Harvard Journal of Law & Technology
Volume 12, Number 2 Winter 1999

THE INTERNET AND ITS CHALLENGES FOR THE FUTURE OF INSIDER TRADING REGULATION

Robert A. Prentice[*]

TABLE OF CONTENTS

---

* University Distinguished Teaching Professor and Ed & Molly Smith Centennial Professor of Business Law, Graduate School of Business, University of Texas at Austin.

I. INTRODUCTION

There is no doubt that the Internet is revolutionizing the securities business.[1] This revolution mandates a reexamination of most aspects of how the Securities and Exchange Commission ("SEC") regulates securities.[2] In an earlier article,[3] I ruminated *generally* about the implications of the Internet revolution for securities fraud jurisprudence under SEC Rule 10b-5[4] and Section 10(b)[5] of the Securities Exchange

---

1. *See* GENE I. ROCHLIN, TRAPPED IN THE NET 75 (1997) ("No other major human activity has moved so quickly to the edge of 'cyberspace' [as the securities business]."); Kenneth W. Brakebill, Note, *The Application of Securities Laws in Cyberspace: Jurisdictional and Regulatory Problems Posed by Internet Securities Transactions*, 18 HASTINGS COMM. & ENT. L.J. 901, 904 (1996) ("Information technology has had a substantial impact on the investment process and the marketplace in general."); Kurt Andersen, *The Digital Bubble*, NEW YORKER, Jan. 19, 1998, at 30 ("The only professional caste as profoundly computer-dependent as the media is Wall Street. Traders and analysts require infusions of fresh data — all day, every day — on earnings and share prices and interest rates.").

2. Professor Langevoort foresaw this need as long ago as 1985. *See* Donald C. Langevoort, *Information Technology and the Structure of Securities Regulation*, 98 HARV. L. REV. 747 (1985); *see also* John C. Coffee, Jr., *Brave New World? The Impact(s) of the Internet on Modern Securities Regulation*, 52 BUS. LAW. 1195 (1997) ("It is now a trite commonplace that the advent of the Internet will in time revolutionize securities regulation."); Erica Clements, Comment, *The Seventh Amendment Right to Jury Trial in Civil Penalty Actions: A Post-*Tull *Examination of the Insider Trading Sanctions Act of 1984*, 43 U. MIAMI L. REV. 361, 398 (1988) ("Since the 1930s, the American system of securities regulation has been based on a set of assumptions, assumptions that recent advances in information technology have rendered invalid."); Bradford P. Weirick, *With the Internet Craze Reaching the Public-Offering Markets, State, Federal and Foreign Regulators Are Scrambling to Catch Up with Technological Advances*, NAT'L L.J., May 6, 1996, at B5, B6 ("More difficult issues, such as the global nature of Internet offerings and the potential impact of conflicting regulations on electronic commerce, raise significant questions that have generated demand for fundamental changes to existing federal, state and foreign securities regulation.").

The SEC has issued scores of new rules and no-action letters in order to respond to changes wrought by the Internet. *See generally* Jane Kaufman Winn, *Regulating the Use of the Internet in Securities Markets*, 54 BUS. LAW. 443 (1998) (summarizing recent SEC actions).

3. *See* Robert A. Prentice, *The Future of Corporate Disclosure: The Internet, Securities Fraud, and Rule 10b-5*, 47 EMORY L.J. 1 (1998) [hereinafter Prentice, *Corporate Disclosure*].

4. 17 C.F.R. § 240.10b-5 (1998).

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
>
> (a) To employ any device, scheme, or artifice to defraud,
>
> (b) To make any untrue statement of a material fact or to

Act of 1934 ("Exchange Act"). In this Article, I examine *specifically* the Internet's implications for insider trading law. Such analysis is critical because most believe that the new technology will increase the opportunities for, and amount of, insider trading,[6] and the SEC has made

---

> omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
>
> (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

Id.

5. 15 U.S.C. § 78j(b) (1994).

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange —
>
> . . . .
>
> (b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors.

Id. § 78j.

6. *See* Caroline A.A. Greene, Note, *International Securities Law Enforcement: Recent Advances in Assistance and Cooperation*, 27 VAND. J. TRANSNAT'L L. 635, 636 (1994) (noting that advances in telecommunications and automated mechanisms for securities transactions globally have "increased the opportunities for securities violations such as insider trading"); Diane Francis, *Lies & Rumors*, TORONTO SUN, Mar. 25, 1997, at 12 ("The Internet is ungovernable . . . . The tipsters and inside traders are beyond the short arms of national securities regulators or police."); Neil Winton, *Internet Share Trading May Slash Dealing Costs*, REUTER EUR. BUS. REP., July 5, 1995 ("Some experts worry that share trading on the Internet . . . will greatly increase the possibility of fraud or insider trading."); Steven Wolowitz & Anthony J. Diana, *Unexpected SEC Issues Are Arising Online*, NAT'L L.J., Feb. 9, 1998, at B7 ("[T]he new electronic technology . . . potentially increases the risk that 'traditional' insider trading will occur . . . .").

These fears are consistent with earlier (justified) concerns about pre-Internet forms of technological advancement exacerbating insider trading problems. *See* John M. Fedders, *Policing Trans-Border Fraud in the United States Securities Markets: The 'Waiver by Conduct' Concept — A Possible Alternative or a Starting Point for Discussions?*, 11 BROOK. J. INT'L L. 477, 477 (1985) (noting that technological advances enabling cross-border trading "have increased the opportunity for trans-border securities fraud"); Roberta Karmel, *Regulatory Aspects of Securities Trading: Can Regulators of International Capital Markets Strike a Balance Between Competing Interests?*, 4 B.U. INT'L L.J. 105, 109 (1986) ("As the global market becomes more developed, fraud or manipulation in multiply-listed securities may adversely affect the market for those

it clear that the "liability provisions of the federal securities laws apply equally to electronic and paper-based media."[7] Such analysis is timely because the SEC continues to emphasize insider trading enforcement as a high priority,[8] and the Supreme Court's recent decision in *United States v. O'Hagan*[9] justifies an entire reconceptualization of current insider trading jurisprudence.

I have selected five issues[10] for extended discussion:

1. What implications does Internet technology have for the concept of "nonpublic" information?[11]
2. Can "hackers" be misappropriators?[12]

---

securities in a variety of different jurisdictions . . . .").

7. Use of Electronic Media for Delivery Purposes, Securities Act Release No. 7233, 60 Fed. Reg. 53,458, 53,459 n.11 (Oct. 6, 1995).

8. *See* Stephen M. Bainbridge, *Incorporating State Law Fiduciary Duties into the Federal Insider Trading Prohibition*, 52 WASH. & LEE L. REV. 1189, 1191 (1995) [hereinafter Bainbridge, *Incorporating*] ("Today . . . insider trading is a major Securities and Exchange Commission . . . enforcement target and carries penalties that can only be described as draconian.").

9. 521 U.S. 642 (1997) (embracing "misappropriation" theory and other tools in SEC's enforcement quiver).

10. Obviously, other important issues could also be discussed, but this Article is long enough as is. One issue I considered examining related to the implications of encryption technology on insider trading rules and enforcement. There is a highly visible, and even more highly controversial, debate regarding encryption technology. *See, e.g.*, John Carey, *The Great Encryption Debate*, BUS. WK., Mar. 9, 1998, at 36; Richard Raysman & Peter Brown, *The Continuing Debate Over Encryption Software*, N.Y. L.J., July 14, 1998, at 3. Promoting encryption technology advances commerce over the Internet, but also may frustrate law enforcement and intelligence gathering activities. *See* William A. Hodkowski, Comment, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 SANTA CLARA COMPUTER & HIGH TECH. L.J. 217, 218–19 (1997) (noting that "the lack of encryption technology to protect sensitive information from data thieves as it travels the Internet has severely hampered the ability to effectively communicate over the Internet"); Richard R. Mainland, *Congress Holds the Key to Encryption Regulation*, NAT'L L.J., Apr. 20, 1998, at B9 (outlining debate between commerce interests on the one hand and law enforcement and intelligence community interests on the other). The SEC, as an enforcement agency, certainly has an interest in the debate because the more that highly sophisticated encryption technology is available, the harder it will be to detect insider trading and other securities laws violations. Still, larger issues of national security should drive this debate, and the SEC would do well to follow the lead of the Australian Securities Commission and decline to take an active role in resolution of the issue. *See* AUSTRALIAN SECURITIES COMMISSION, VIRTUALLY NO LIABILITY? SECURITIES MARKETS IN AN ELECTRONIC AGE (1997), *reprinted in* SECURITIES IN THE ELECTRONIC AGE 187, 215 (Glasser LegalWorks Seminars 1998).

11. *See infra* Part II.

12. *See infra* Part III.

3. What liability might an Internet Service Provider ("ISP") have for insider trading involving the Internet?[13]
4. Can e-mail create insider trading liability for companies that do not adequately control their employees' communications?[14]
5. What implications does Internet technology carry for international enforcement of insider trading rules?[15]

II. WHAT IMPLICATIONS DOES INTERNET TECHNOLOGY HAVE FOR THE CONCEPT OF "NONPUBLIC" INFORMATION?

The essence of insider trading is trading on material, *nonpublic* information.[16] If the information is available to the general investing public, there is no unfair informational advantage to the insider. It is the secret nature of the information that has caused courts to create the "duty to disclose or abstain from trading."[17] Once the information becomes public, abstention from trading is no longer required. But when does information cease to be "nonpublic" and become fair game for trading?[18]

A. Traditional Views

There is no clear rule regarding when information leaves behind its secret status and enters the public domain. The statutes contain no definition. Congress has stated in various reports, more tautologically than helpfully, that "nonpublic" information is information that is "not available to the general public."[19] The SEC has issued no clarifying rules. The courts have sensibly focused the inquiry upon whether the

---

13. *See infra* Part IV.
14. *See infra* Part V.
15. *See infra* Part VI.
16. For a recent discussion of the elements of insider trading liability, see Robert A. Prentice, *Clinical Trial Results, Physicians, and Insider Trading*, 20 J. LEGAL MED. 195, 199–210 (1999) [hereinafter Prentice, *Clinical Trial*].
17. *See* United States v. O'Hagan, 521 U.S. 642, 652 (1997) (citing Chiarella v. United States, 445 U.S. 222, 228–29 (1980)).
18. For excellent discussions of the general issue of when information is considered "nonpublic," see 2 ALAN R. BROMBERG & LEWIS D. LOWENFELS, SECURITIES FRAUD AND COMMODITIES FRAUD §§ 7.4(411) to 7.4(412) (2d ed. 1996); RALPH C. FERRARA ET AL., FERRARA ON INSIDER TRADING AND THE WALL § 2.01[2] (1997) [hereinafter FERRARA]; VII LOUIS LOSS & JOEL SELIGMAN, SECURITIES REGULATION 3505–09 (3d ed. 1991); WILLIAM K.S. WANG & MARC I. STEINBERG, INSIDER TRADING § 4.3 (1996).
19. H.R. REP. NO. 100-910, at 7–8 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6045; H.R. REP. NO. 98-355, at 2 (1983), *reprinted in* 1984 U.S.C.C.A.N. 2274, 2275.

information is available to the *investing* public generally.[20] But when is information generally available to the investing public? Two main views have been espoused.

1. Public Dissemination and Absorption

The courts have produced no blanket rule to determine for all situations whether information has entered the public domain so that it can be the basis for trading without any danger of insider trading liability. Rather, the results "var[y] with the circumstances."[21] Mere disclosure is not enough, for "[t]acking a notice to the loading dock door constitutes disclosure but does not amount to dissemination."[22] Most courts have taken the view that information becomes "public" only after there has been public dissemination of some form *and* the market has had an opportunity to "absorb" the disclosed information.[23]

a. Public Dissemination

The question often arises as to whether an issuer has adequately disseminated information so that the market has had the opportunity to begin absorbing it. What mechanisms of disclosure and distribution are adequate to the task? The SEC's first opportunity to give guidance on this issue came in its initial insider trading action, *Cady, Roberts & Co.*[24] The facts of the case were as follows: J. Cheever Cowdin was both a registered representative of Cady, Roberts and a director of the Curtiss-Wright Corporation. At approximately 11:00 a.m. on November 25, 1959, the Curtiss-Wright board of directors voted to pay a reduced dividend and authorized transmission of information regarding this action to the New York Stock Exchange ("NYSE"). Due to several glitches, this information, although transmitted to Western Union at 11:12 a.m., was not delivered to the NYSE until 12:29 p.m. The Wall Street Journal was not given the information until 11:45 a.m., and the announcement did not appear on the Dow Jones broad tape until

---

20. *See, e.g.*, SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 854 (2d Cir. 1968) (en banc). The SEC concurs. *See, e.g.*, Investors Management Co., 44 S.E.C. 633, 643 n.22 (1971) (focusing on "availability to the investing public" (internal quotation marks omitted) (quoting *Texas Gulf Sulphur*, 401 F.2d at 854)).

21. LOSS & SELIGMAN, *supra* note 18, at 3505.

22. J. ROBERT BROWN, JR., THE REGULATION OF CORPORATE DISCLOSURE § 4.02[3], at 4-7 (3d ed. 1998).

23. *See* LOSS & SELIGMAN, *supra* note 18, at 3505–09.

24. 40 S.E.C. 907 (1961).

11:48 a.m. Soon after the board decision had been made, however, the board recessed and Cowdin slipped out to call Robert M. Gintel, another employee of Cady, Roberts, and told him of the news. Gintel entered two sell orders which were executed at 11:15 a.m. and 11:18 a.m.[25]

The SEC did not take maximum advantage of its opportunity to clarify the rules in this area.[26] On the one hand, the SEC clearly held that Gintel had improperly traded on the basis of nonpublic information. The SEC noted that the NYSE had set up "explicit requirements and recommended procedures for the immediate public release of dividend information" by listed issuers.[27] Indeed, the SEC seemed to approve and thereby to lend a patina of authority to those procedures. On the other hand, the SEC effectively dodged the issue of when the Curtiss-Wright dividend had become public so that trading would have been proper, stating only:

> The practical problems envisaged by respondents in effecting appropriate disclosures in connection with transactions on the Exchange are easily avoided where, as here, all the registered broker-dealer need do is to keep out of the market until the established procedures for public release of the information are carried out instead of hastening to execute transactions in advance of, and in frustration of, the objectives of the release.[28]

In more recent years, SEC pronouncements have tended to be demanding, yet vague. The official SEC position seems to be that "[p]roper and adequate disclosure of significant corporate developments

---

25. *See id.* at 908–10.

26. The SEC has failed to provide rule-based guidance regarding when information becomes public despite Judge Bonsal's invitation for it to do so in *SEC v. Texas Gulf Sulphur Co.*, 258 F. Supp. 262, 289 (S.D.N.Y. 1966), *aff'd in part and rev'd in part*, 401 F.2d 833 (2d Cir. 1968) (en banc), and Justice Blackmun's expression of displeasure several years later in *Dirks v. SEC*, 463 U.S. 646 (1983):

> I agree that disclosure in this case would have been difficult. I also recognize that the SEC seemingly has been less than helpful in its view of the nature of disclosure necessary to satisfy the disclose-or-refrain duty. The [SEC] tells persons with inside information that they cannot trade on that information unless they disclose; it refuses, however, to tell them how to disclose. This seems to be a less than sensible policy, which it is incumbent on the [SEC] to correct.

Id. at 677 (Blackmun, J., dissenting) (citations and footnotes omitted).

27. *Cady, Roberts*, 40 S.E.C. at 915.

28. *Id.*

can only be effected by a public release through the appropriate public media, designed to achieve a broad dissemination to the investing public generally and without favoring any special person or group."[29] But what media meet those criteria of broad dissemination and nonfavoritism? Court rulings provide some guidance.

The first major insider trading case to be litigated in the courts, *SEC v. Texas Gulf Sulphur Co.*,[30] involved a massive ore strike in Canada. The company issued a press release on April 16, 1964, at 10:00 a.m. This press release was carried over the Merrill Lynch internal news wire at 10:29 a.m. and over the Dow Jones broad tape between 10:54 a.m. and 11:02 a.m.[31] One Texas Gulf Sulphur ("TGS") director placed a buy order for TGS stock at 10:20 a.m.[32]

Judge Bonsal, the trial judge, held that the news of the mineral strike was not public *before* 10:00 a.m. on April 16, when the press conference occurred, notwithstanding: (1) circulation of rumors in the press,[33] (2) publication of an inaccurate story in a Canadian newspaper that morning as well as telephone calls and telexes about the Canadian article to American brokers, and (3) delivery of a statement to the press gallery in the Ontario Parliament at 9:40 a.m.[34] However, Judge Bonsal held that the 10:00 a.m. press release did constitute public disclosure and that the director was free to trade at 10:20 a.m., noting "it is the making of the announcement that controls."[35]

The Second Circuit disagreed with Judge Bonsal's view that the information became "public" at 10:00 a.m., when the press release was issued. The court noted initially that the key to whether illicit trading has occurred is when the insider *placed* the order, not when the order was *executed*.[36] In this case, one defendant had called his broker at midnight the night before and asked him to execute his buy order as soon

---

29. Faberge, Inc., 45 S.E.C. 249, 256 (1973), *quoted in* Dirks v. SEC, 463 U.S. 646, 654 n.12 (1983)); *accord* Jack Schaefer, 8 SEC Docket 261, 261 (1975).

30. 258 F. Supp. 262 (S.D.N.Y. 1966), *aff'd in part and rev'd in part*, 401 F.2d 833 (2d Cir. 1968) (en banc).

31. *See Texas Gulf Sulphur*, 401 F.2d at 846–47.

32. *See id.* at 847.

33. Because TGS had issued an April 12 press release denying the rumors, the court was quite sensible to hold that the rumors did not constitute a public disclosure of the ore strike. In a related context, one court held that disclosing *general* information to a limited segment of the public does not render public very *specific* information known to an insider-trading defendant. *See* SEC v. Lund, 570 F. Supp. 1397, 1401 (C.D. Cal. 1983).

34. *See Texas Gulf Sulphur*, 258 F. Supp. at 285–86.

35. *Id.* at 288 (citing *Cady, Roberts*, 40 S.E.C. at 915).

36. *See Texas Gulf Sulphur*, 401 F.2d at 853 n.17.

as the Midwest Stock Exchange opened.[37] This was clearly "beating the news" illicitly.[38] But even the director who traded at 10:20 a.m. was deemed by the Second Circuit to have traded too quickly:

> Before insiders may act upon material information, such information must have been *effectively disclosed in a manner sufficient to insure its availability to the investing public.* Particularly here, where a formal announcement to the entire financial news media had been promised in a prior official release known to the media, all insider activity must await *dissemination* of the promised official announcement.[39]

At a minimum, the court stressed, the insiders "should have waited until the news could reasonably have been expected to appear over the media of widest circulation, the Dow Jones broad tape . . . ."[40]

After *Texas Gulf Sulphur* established the basic rule that no trading should occur until after (and probably not *immediately* after) the information appears on the Dow Jones broad tape,[41] and thereby did

---

37. *See id.* at 847.
38. *See id.* at 853.
39. *Id.* at 854 (emphasis added).
40. *Id.*
41. The *Texas Gulf Sulphur* ruling prompted Professor Bromberg to note:
    > [From] the overriding purpose of eliminating informational inequities in the market, it follows that the best medium for disseminating material information is the one with the widest distribution in the market. This the Second Circuit recognized to be the Dow Jones broad tape. The broad tape is the one preferred by most companies for their releases. But it can hardly be the sole arbiter of when insiders may trade. Quite apart from the legal questions in any such delegations, there are practical problems in the limited capacity of any medium, and its need to choose what it considers most important and interesting to its subscribers. As more companies release more information, partly spurred by court decisions like the Second Circuit rulings in TGS, the odds go down that any particular item will be carried by the Dow Jones tape or other media. Against this nonpublication possibility and in furtherance of a sound policy of maximum dissemination, a company would be wise to issue important news widely, e.g., to Dow Jones, to Reuters, to the AP and UPI, to broker-dealers with their own wires to branches or correspondents, to broker-dealers or analysts known to have particular interest in the company's securities, and to newspapers in the major financial centers and where the company's operations or shareholders concentrate.

much to create the modern information industry that specializes in dissemination of corporate press releases,[42] additional rulings came piecemeal. In *Faberge, Inc.*,[43] the SEC ruled that information communicated over the AutEx wire system, which reported block trades to its subscribers and enabled subscribers to receive market and research information, did *not* constitute public dissemination because disclosure was effective as to only a limited number of institutional subscribers.[44] To be effective, information "must be disseminated in a manner calculated to reach the securities market place in general through *recognized channels of distribution* . . . ."[45]

However, in *duPont Glore Forgan, Inc. v. Arnold Bernhard & Co.*,[46] a court held that distribution via a Reuter Financial Report rendered the information available to the investing public, even though that information was not published in the Wall Street Journal or other newspapers until three days later.[47] Although the plaintiff was not a subscriber to the Reuters service, the court found public dissemination because: (1) the service had 654 subscribers in 38 states; (2) the two market makers[48] in the stock in question other than the plaintiff subscribed to the service;[49] (3) the major stock exchanges subscribed to

---

> Mailing to shareholders, although slower, is good public relations as well as a means of dissemination which is entirely within the company's control.

2 ALAN R. BROMBERG, SECURITIES LAW, FRAUD § 7.4(7)(c), at 190.3–.4 (Supp. 1969).

42. *See* Tom Abate, *Love Him or Hate Him — King of the Business Press Release*, S.F. CHRON., June 30, 1998, at B1 (profiling founder of Business Wire, which disseminates about half of all business press releases in United States).

43. 45 S.E.C. 249 (1973).

44. *See id.* at 255.

45. *Id.* (emphasis added).

46. No. 73 Civ. 3071, 1978 U.S. Dist. LEXIS 20385 (S.D.N.Y. Mar. 6, 1978).

47. *See id.* at *17.

48. A "market maker" is

> any specialist permitted to act as a dealer, any dealer acting in the capacity of block positioner, and any dealer who, with respect to a security, holds himself out (by entering quotations in an inter-dealer communications system or otherwise) as being willing to buy and sell such security for his own account on a regular or continuous basis.

15 U.S.C.A. § 78c(a)(38) (West Supp. 1998).

49. It was sensible for the court to focus upon market makers in the particular stock involved because under the efficient market hypothesis, *see infra* Part II.A.2, if information is disseminated among analysts of the security, market makers of the security, and existing or potential large investors in the security, then it is presumed that the stock price will adjust to reflect the new information. *See, e.g.*, Elkind v. Liggett & Myers, Inc., 635 F.2d 156, 166 (2d Cir. 1980) (holding that information was not

the service, and the NYSE and American Stock Exchange required listed companies to disseminate earnings news through Reuters as well as through Dow Jones; and (4) the plaintiff itself had contracted to install the service, although installation had not yet been accomplished at the time of the incident in question.[50]

As a final point, at an April 8, 1998 conference sponsored by the SEC, representatives of the major stock exchanges and Nasdaq stated that they considered information appearing on the major newswires, such as PR Newswire or Business Newswire, as constituting public dissemination.[51]

b. Absorption Period

May insiders legally wait with their "fingers on the button" and place their orders the instant the information becomes "public" by showing up on the Dow Jones broad tape or some other recognized channel of distribution? In *Texas Gulf Sulphur*, Judge Bonsal noted the SEC's position that trading should not be allowed immediately upon the announcement, but only after the information has been "absorbed by the public."[52] Arguing that such a restriction would lead to uncertainty, Judge Bonsal refused to provide a "reasonable waiting period" in the absence of Congressional or SEC action. In support of his argument, he

---

material, nonpublic information because it was "already common knowledge among the analysts"); SEC v. Bausch & Lomb, Inc., 565 F.2d 8, 17 (2d Cir. 1977) (holding that information was not nonpublic because it was "common knowledge among members of the investment community").

50. *See duPont Glore Forgan*, 1978 U.S. Dist. LEXIS 20385, at *17–*18.

51. *See SEC is Reluctant to Provide Guidance to Companies on Disclosure, Official Says*, BNA SEC. L. DAILY, Apr. 9, 1998 [hereinafter *SEC is Reluctant*].

52. SEC v. Texas Gulf Sulphur Co., 258 F. Supp. 262, 288–89 (S.D.N.Y. 1966), *aff'd in part and rev'd in part*, 401 F.2d 833 (2d Cir. 1968) (en banc).

raised several tricky questions that could arise[53] and cited widely differing views of experts as to what would be a "reasonable time."[54]

However, the Second Circuit again overruled Judge Bonsal, clearly indicating that an insider should not be allowed to sit with her finger on the telephone speed dialer in order to call a stockbroker the second the information appears on the Dow Jones broad tape. Rather, the court indicated, there should be no trading by insiders until a period of time has passed to enable the market to *absorb* the information in order to allow investors a chance to make an informed decision. How long a period is required and who must absorb the information is not clear. With regard to a particular defendant who had traded *after* dissemination over the broad tape, the court stated in dicta[55] that "where the news is of a sort which is not readily translatable into investment action, insiders may not take advantage of their advance opportunity to evaluate the information by acting immediately upon dissemination."[56]

Not surprisingly, there is no clear rule regarding what period of time constitutes a reasonable period for absorption. Again, the issue has been addressed on a case-by-case basis with two of the determinative factors being the nature and complexity of the information. Because the purpose of the absorption period is to provide investors with an opportunity to make an informed decision,[57] if the information is readily

---

53. *See id.* at 289. Judge Bonsal queried:

> What of a representative of the news media who, upon hearing the announcement, calls his broker before he calls his office? What of a wire house which has an inside track in getting the information to its registered representatives and to its customers? (The April 1 announcement went out over Merrill Lynch's news wire to its 145 offices half an hour before it went out over the Dow Jones ticker.) Should the representatives of the news media and the wire houses be subjected to such a rule since they are in possession of material information which the average stockholder has not had an opportunity to absorb?

Id.

54. *See id.* at 289 n.12. Judge Bonsal noted, for example, that the President of the NYSE had suggested a 30-day waiting period, former SEC Commissioner Cary had suggested that a 30-day period was overly generous, and Cary's former assistant Fleischer had concluded that an "an arbitrary twenty-four hour period after news is released to the public" would be appropriate. *Id.* (internal quotation marks omitted).

55. The holding was dicta because the defendant had died, rendering his appeal moot.

56. *Texas Gulf Sulphur*, 401 F.2d at 854 n.18. The court followed the trial judge's example by asking, in vain it turns out, for SEC clarification of an insider's responsibilities. *See id.*

57. *See* WANG & STEINBERG, *supra* note 18, § 4.3, at 153.

translatable into investment action, then the waiting period before insiders can trade apparently is relatively short.

Results in specific cases have varied widely. For example, the court in *duPont Glore Forgan, Inc. v. Arnold Bernhard & Co.*[58] held that six hours was sufficient for absorption.[59] In *Billard v. Rockwell International Corp.*,[60] the court noted various rules of thumb that had been suggested, ranging from "waiting for the morning newspaper to carry the information" to "fifteen minutes after the [Dow Jones broad] tape runs."[61] In *SEC v. Ingoldsby*,[62] the court held that a press release was not fully absorbed by the market until nine days after its release.[63] Other wildly disparate suggestions have been made,[64] and a popular but amorphous formulation is that "a public disclosure of information relieves the duty to disclose if it is reasonable to conclude that the plaintiff should have been made aware of the fact as a result of that disclosure."[65] Most recently, the SEC's director of the Division of Corporate Finance stated at an April 8, 1998 conference that information cannot necessarily be traded upon at the moment that a press release is sent out over the "blast fax" to analysts and the media; rather, public dissemination may require passage of an unspecified amount of time so that those receiving the information may digest it.[66]

---

58. No. 73 Civ. 3071, 1978 U.S. Dist. LEXIS 20385 (S.D.N.Y. Mar. 6, 1978).

59. *See id.* at *20 n.6.

60. 526 F. Supp. 218 (S.D.N.Y. 1981).

61. *Id.* at 220.

62. No. 88-1001-MA, 1990 U.S. Dist. LEXIS 11383 (D. Mass. May 15, 1990).

63. *See id.* at *13–*14. The court noted that the company was small and not well-followed by the media, the stock price and volume of trading did not readily indicate that the information had been incorporated by the market, and only when the news in the press release was carried in a trade publication nine days after the release did the stock price change. *See id.*

64. *Loss & Seligman* notes these various suggestions for absorption periods:

- 24 hours after publication of a release in a national medium (or 48 hours when the publication is not so widespread).
- One week after disclosure by press release, SEC filing, or comparable method, with the burden being on any trader who asserts that a fact was generally available to the public more quickly.
- 24 hours after disclosure.

See VII LOSS & SELIGMAN, *supra* note 18, at 3507 n.132.

65. Powell v. American Bank & Trust Co., 640 F. Supp. 1568, 1579 (N.D. Ind. 1986).

66. *See SEC is Reluctant*, *supra* note 51 (quoting Brian Lane, Director, Division of Corporate Finance).

2. Efficient Market Hypothesis View

Although the SEC and most courts focus upon dissemination and absorption in determining whether information has become public, some courts have adopted an approach based upon the efficient market hypothesis ("EMH").[67] The most widely accepted form of the EMH, the "semi-strong" version, posits that at any given time, share prices in an efficient market will incorporate all publicly available information relating to publicly traded companies (in addition to general information about the economy as a whole).[68] This view condenses the dissemination and absorption elements of the majority approach and simply focuses upon whether the subject company's stock price has adjusted to reflect the new information. After it does so, no benefit remains to be gained from trading on the formerly secret information. If there is no such price reaction, the information must not have been material anyway.

Information can become public, of course, through issuer dissemination to the investing public, but there are many other ways that it might become incorporated into the stock's price. Sometimes public dissemination will occur via means other than a formal announcement by the issuer. For example, various cases have held that information *is* available to the investing public if it is: (1) widely known among investors (however they came to know it),[69] (2) common knowledge among analysts following the particular stock (even if the investing public at large does not yet know the information),[70] or (3) already published in widely distributed magazines.[71] On the other hand,

---

67. *See generally* Ronald J. Gilson & Reinier H. Kraakman, *The Mechanisms of Market Efficiency*, 70 VA. L. REV. 549 (1984) (explaining EMH).

68. *See* John C. Coffee, Jr., *Liquidity Versus Control: The Institutional Investor as Corporate Monitor*, 91 COLUM. L. REV. 1277, 1330 n.206 (1991) (explaining "semi-strong" version of EMH).

69. *See, e.g.*, SEC v. Monarch Fund, 608 F.2d 938, 943 (2d Cir. 1979) (noting that information was "circulating throughout the over-the-counter community").

70. *See, e.g.*, Elkind v. Liggett & Myers, Inc., 635 F.2d 156, 166 (2d Cir. 1980) (information about lower sales of firm's products); SEC v. Bausch & Lomb, Inc., 565 F.2d 8, 17 (2d Cir. 1977) (information about flat sales of company's new contact lens). Because of the potential for insider trading by analysts, a current SEC enforcement priority, it is not at all clear that the SEC would endorse such a view.

71. *See, e.g.*, Catherines v. CopyTele, Inc., 602 F. Supp. 1019, 1024–25 (E.D.N.Y. 1985) (noting that information about company's product had already been published in the Wall Street Journal, Fortune, and similar publications).

information has been held still nonpublic despite general rumors in the market about the company.[72]

Courts adopting the EMH approach are not particularly concerned with broad dissemination to the "investing public," concluding that a more limited distribution to key market players may accomplish all that needs to be done. For example, in *United States v. Libera*,[73] the court noted:

> We agree that information may be considered public for Section 10(b) purposes even though there has been no public announcement and only a small number of people know of it. The issue is not the number of people who possess it but whether their trading has caused the information to be fully impounded into the price of the particular stock. Once the information is fully impounded in price, such information can no longer be misused by trading because no further profit can be made.[74]

It seems apparent that only in the absence of evidence that the information has been incorporated into the issuer's stock price should there be a detailed analysis of whether there has been adequate dissemination and time for absorption. If the market price has fully incorporated the information and reflected it in a change in the company's stock price, the information should be viewed as "public" — end of inquiry.[75] The failure of Congress and the SEC to fully and clearly explicate guidelines for dissemination and absorption makes it even more imperative that the EMH approach be recognized as a valuable supplement in determining whether information has become "public."

---

72. *See* SEC v. Peters, 735 F. Supp. 1505, 1514–15 (D. Kan. 1990), *rev'd on other grounds*, 978 F.2d 1162 (10th Cir. 1992).

73. 989 F.2d 596 (2d Cir. 1993).

74. *Id.* at 601; *see also* SEC v. Mayhew, 121 F.3d 44, 50 (2d Cir. 1997) (holding that information becomes public either when it has been broadly disseminated or when, although not widely known, it has become fully impounded into market price).

75. Similarly, when insiders are trading in efficient markets before the stock price has fully incorporated the new information, there should be a legal presumption that adequate time for absorption has not yet passed.

B. The New Technology and Its Implications

Under the traditional view, news was fully disseminated once it was carried by either the Dow Jones broad tape (now known as the Dow Jones News Service) or another accepted news ticker. The length of the required absorption period remained unclear. Today, the Internet and other new technologies have further roiled these murky waters. These technologies create new means of making disclosures and thereby create new situations where it is unclear whether the information has been made "public."[76] These new developments create two sets of problems. One set arises when it is fairly clear that public dissemination has functionally occurred via new electronic means, but the SEC has not fully and officially embraced that fact.[77] A second set arises when it is unclear whether public dissemination has functionally occurred.

1. SEC Recalcitrance

As noted earlier, the SEC has consistently refused to issue definitive criteria to establish when information has been adequately disseminated or absorbed such that it can be treated as "public."[78] For many years this was not overly problematic because courts made it fairly clear that the appearance of information on the Dow Jones broad tape or Reuters news service would suffice for dissemination. However, due to new technology, specific SEC guidance is now needed. As has recently been observed:

---

76. Recent events have highlighted the complex problems that technology brings to the area of public disclosure of sensitive data. For example, in early 1999, an electronic news outlet accidentally released Xerox Corporation's earnings data in advance of a prescheduled time. *See* Greg Ip & Raju Narisetti, *First Call Reviews Earnings Policy After Error*, WALL ST. J., Jan. 27, 1999, at C1. And in late 1998, the Bureau of Labor Statistics prematurely released data via its website that "briefly roiled financial markets." Alejandro Bodipo-Memba, *Labor Department Temporarily Suspends Postings on Web of Supplemental Data*, WALL ST. J., Nov. 9, 1998, at A2; *see also* Thomas E. Weber et al., *Oops. In Cyberspace, News Often Jumps the Gun*, WALL ST. J., Nov. 6, 1998, at B1 ("The mistake was just the latest cautionary tale about the Internet's awesome power to disperse information in the blink of an eye without any hope of calling it back.").

77. *See Roundtable Participants Call on SEC to Continue to Address Technological Issues*, BNA SEC. L. DAILY, Apr. 15, 1998 [hereinafter *Roundtable Participants*] (quoting SEC Commissioner Norman Johnson as saying that the SEC "will probably [continue to] lag behind this brave new world" of the Internet).

78. *See supra* note 26 and accompanying text.

> Bloomberg News is now recognized as a third "full disclosure medium" by the stock exchanges and Nasdaq, and the S.E.C. appears to tacitly concur. Moreover, the big commercial news transmission services, PR Newswire and Business Wire, now routinely guarantee any company, for a modest fee, that its news release will not only be transmitted to but also carried by the Bloomberg and Reuters financial screens, Dow Jones News Retrieval, Nexis, America Online, Compuserve and on PR Newswire's or Business Wire's own sites on the World Wide Web. Companies are further assured that their announcements will appear automatically on these data bases and on-line services as soon as 15 minutes after their transmission to the primary news media.
>
> . . . .
>
> Today, companies can carefully select a release time, and be confident that not long after that moment, the news will be legitimately "public" and can be freely disclosed elsewhere. Technology has enabled companies to simultaneously fax-broadcast the full text to 100, 300, 500 or more of the company's closest followers among investment analysts and money managers worldwide.
>
> The text can then be posted on the company's [website] and through a toll-free number for an instant fax. Finally, often within the hour, the company conducts a prearranged teleconference at which the chief financial officer can discuss the news with those same hundreds of professionals.[79]

If a particular issuer uses all (or most) of these mechanisms, it seems clear that the information has been publicly disseminated, even if it has not yet appeared on the Dow Jones broad tape or Reuters news ticker.[80]

---

79. Ted Pincus, *When News is in the Timing*, N.Y. TIMES, Sept. 7, 1997, at F12.

80. Several companies vigorously compete to provide instant financial news and data to the public. Reuters, which specializes in newsgathering and foreign-currency exchange information, currently delivers its information to approximately 386,000 desktops. Bridge/Telerate, which specializes in treasury bond prices, delivers its information to approximately 169,000 desktops. And Bloomberg, which offers sophisticated financial analysis, delivers its information to approximately 92,000 desktops. *See* I. Jeanne Dugan, *A Feverish Battle Breaks Out on Your Desk*, BUS. WK.,

However, the SEC has not yet officially recognized this fact, motivating some companies needlessly and inefficiently to delay discussing the news until it appears on Dow Jones or Reuters.[81] The SEC's refusal to recognize officially that these new channels can result in effective public dissemination creates a "two-tier system of distribution" that results in "uncertainty for those disseminating the information and inequities for those who want to trade on it."[82] The SEC should draw new rules to recognize and accommodate the new technological reality.[83]

2. Difficult Situations

The SEC's reluctance to recognize officially public dissemination via new electronic media is a product of caution and a laudable desire to ensure that individual investors are not unfairly disadvantaged. Faster dissemination via electronic media does not guarantee fair access to all.[84] After all, unless information has become impounded in the securities market price, such information becomes public when it has achieved broad dissemination to the general investing public "without favoring any special person or group."[85] When a company uses the full panoply of media discussed in the previous Section, it seems that the SEC is being unduly cautious. However, when only one (or a few) of the new

---

Apr. 13, 1998, at 98.

81. *See* Pincus, *supra* note 79, at F12 ("Just to be on the safe side, for example, a company treasurer might end up waiting two or more hours after the release is issued, making sure it has been carried on the accepted media [i.e., Dow Jones and Reuters], before discussing the information publicly.").

82. *Id.*

83. *Cf., e.g.*, Checkosky v. SEC, 139 F.3d 221, 222 (D.C. Cir. 1998) (chastising SEC for not articulating an "intelligible standard" of what is "improper professional conduct" for purposes of Rule 2(e), 17 C.F.R. § 201.102(e) (1998)); SEC v. Adler, 137 F.3d 1325, 1337 & n.33 (11th Cir. 1998) (declining to apply liability based only on possession because SEC had not issued rule clarifying its position on whether inside traders in possession of inside information could be liable for insider trading even if they had not used the information in making their trading decision); Paul Beckett, *SEC's Lack of Some Clear Rules Irks Appeals Courts*, WALL ST. J., Apr. 14, 1998, at B7 ("In decisions on a range of topics in recent months, the courts have frowned on the agency's efforts to hold alleged violators responsible in the absence of an SEC rule.").

84. *See* Paul G. Mahoney, *Technology, Property Rights in Information, and Securities Regulation*, 75 WASH. U. L.Q. 815, 816 (1997) ("[T]echnology will not change the relative proportions of public and private information in securities markets, but it will increase the speed with which prices adjust to private information. Regulatory change cannot, therefore, be premised on the notion that technology will make traders more nearly homogeneously informed.").

85. Dirks v. SEC, 463 U.S. 646, 653 n.12 (1983); SEC v. Mayhew, 121 F.3d 44, 50 (2d Cir. 1997); Faberge, Inc., 45 S.E.C. 249, 256 (1973).

means of electronic dissemination is (are) used, the question is more difficult.

On the one hand, the disclosure power of the Internet is astounding. "Combine the circulation of the Wall Street Journal (1.8 million) and the USA Today (1.6 million) and you still fall short of the 'self-publishing' reach available to someone who joins a few commercial bulletin board services."[86] Information is coming to the market through e-mail, chat rooms, bulletin boards, corporate websites, and numerous other mechanisms unheard of just a few short years ago. For this reason, information disseminated over the Internet is arguably "public." As the Seventh Circuit noted in a recent Rule 10b-5 case:

> In today's society, with the advent of the "information superhighway," federal and state legislation and regulations, as well as information regarding industry trends, are easily accessed. A reasonable investor is presumed to have information available in the public domain, and therefore [plaintiff investor] is imputed with constructive knowledge of this information.[87]

On the other hand, because much of the investing public is not "plugged in" and there is no established "duty to browse," it is legitimate to question whether dissemination via the Internet can truly be

---

86. North American Securities Administrators Association, *Cyberspace Fraud and Abuse* (visited Mar. 10, 1999) <http://www.nasaa.org/investoredu/investoralerts/cyberspa.html>.

87. Whirlpool Fin. Corp. v. GN Holdings, Inc., 67 F.3d 605, 610 (7th Cir. 1995). Although this passage can be read as indicating that information that is on the Internet is necessarily public information, it is unlikely that the Seventh Circuit intended to go that far. The case involved the defendant's alleged failure to disclose information about pending legislation and industry-wide trends. The court merely held that that information was present in a number of sources — as one example, the court cited a print journal, the *Journal of the American Medical Association* — and that those sources were easily available, in part because of the information superhighway. *See id.* at 608–10. The Seventh Circuit did not directly address the question of whether information disclosed solely on the Internet should be treated as public information.

Still, *Whirlpool* has many interesting implications. *See generally* Will Morrow, Comment, *Is the Internet Participating in Securities Fraud? Harsh Realities in the Public Domain*, 72 TUL. L. REV. 2203, 2210–25 (1998) (asking, for example, whether postings on the Internet constitute "inquiry notice," thus commencing Section 10(b)'s statute of limitations).

"public."[88] Is it fair to disseminate information only over selective and arguably discriminatory media and yet treat it as generally available?[89]

Consider, for example, that concern over insider trading practices[90] prompted Japan's Ministry of Finance to impose a rule that companies cannot legally post announcements of material information on the Internet until twelve hours after that information has been released via a press release aimed at nationally circulating newspapers.[91] Thus, in Japan, "[a]lert Internet surfers who grab such data as newly released earnings reports [appearing on the Internet] and call their stock broker are technically violating Japan's insider-trading regulations."[92] This rule has the effect of putting Japanese companies even further behind U.S. companies in electronic data dissemination, thus arguably hurting their chances of attracting foreign investors.[93] At last report, the Ministry of

---

88. One commentator has noted several important differences between the Internet and traditional sources of information in the public domain:

> Limitations on the Internet's value within the public domain include [1] the limited nature of information distribution, [2] novelty and limited use of the technology, [3] reliability issues resulting from a lack of controls on the information published, and [4] the temporary and transient nature of postings.

Morrow, *supra* note 87, at 2216 (footnotes omitted).

89. Because the universe of potential investors is not fully plugged-in to the Internet, any disclosure using only the Internet is arguably selective. In a letter to the editor of Business Week, attorney Maryann A. Waryjas of Jenner & Block noted that "although the Internet audience is presumably infinite, the courts and the Securities & Exchange Commission may view disclosures made here as 'selective' because they are available only to the 'wired' elite." Maryann A. Waryjas, *Wrong Turn on the I-Way?*, BUS. WK., June 26, 1995, at 12 (letter to the editor); *see also* NATIONAL TELECOMMS. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, FALLING THROUGH THE NET II: NEW DATA ON THE DIGITAL DIVIDE (1998), *available at* <http://www.ntia.doc.gov/ntiahome/net2/falling.html> [hereinafter FALLING THROUGH THE NET] (finding continued "digital divide" based on race, income, and other demographic characteristics).

90. *See Murata Mfg. to Delay Disclosure on Internet*, JIJI PRESS TICKER SERVICE, Nov. 20, 1995; *Tokyo SE Hits Out at News Distribution*, INTERNET BUS. NEWS, Feb. 1, 1996.

91. *See* Yoshiharu Ohi, *For Corporate Data, It's Plug In or Lose Out*, NIKKEI WEEKLY, Oct. 28, 1996, at 7.

92. Tatsuya Inoue, *Internet: Convenient Medium or Unfair Trading Edge? Immediate Release of Corporate Data May Lead to Insider Trading, Authorities Warn*, NIKKEI WEEKLY, Dec. 11, 1995, at 12.

93. *See* Ohi, *supra* note 91, at 7 (expressing this concern); *Tokyo Assails Results on Internet*, FIN. TIMES, Dec. 5, 1995, at 6 ("The Tokyo Stock Exchange does not want companies to send their earnings results to individual investors over the Internet shortly after the results are announced in news conferences . . . [as s]uch data transfers could go against the companies' self-imposed ban on insider trading.").

Finance was considering shortening the waiting period from twelve hours to three hours.[94]

In the United States, with so much disclosure currently occurring electronically,[95] similar concerns have been voiced.[96] One observer has noted the dichotomy between the "traditional [Securities and Exchange] Commission," which makes insider trading enforcement a top priority, and the "modern [Securities and Exchange] Commission," which through a plethora of releases and rules has authorized corporate disclosures via new electronic media that are necessarily selective given the current state of technology adoption.[97] At some level, the dilemma traces back to *Dirks*: the SEC was concerned about enforcing insider trading laws out of concerns for fairness, but the Supreme Court rebuffed the agency out of concerns that such enforcement would unduly stifle analysts' legitimate efforts to gather market information.[98] The Internet has the potential to be the "leveler of the playing field," allowing individual investors the chance to trade on an even footing with

---

94. *See MOF to Ease Internet Data Disclosure Rule*, JIJI PRESS TICKER SERVICE, Sept. 4, 1996.

95. As noted earlier, *see supra* notes 1–2, the Internet is revolutionizing the securities industry. Internet-savvy firms are attempting to use the Internet to replace traditional stock exchanges, circumvent underwriters during initial public offerings, and undercut broker-dealer fees, including those of discount brokers. *See, e.g.*, ANDREW D. KLEIN, WALLSTREET.COM (1998) (describing many of these developments and recounting author's own experience as founder of Wit Capital); *see also* Daniel M. Gallagher, Comment, *Move Over Tickertape, Here Comes the Cyber-Exchange: The Rise of Internet-Based Securities Trading Systems*, 47 CATH. U. L. REV. 1009 (1998) (describing revolution and criticizing SEC's ad hoc approach to regulation as insufficient).

96. *See* Melissa Bane, *The Virtual Exchange: Who Needs Wall Street? Some Contend that the Internet Will Become the Place to Trade*, COMPUTERWORLD, June 17, 1996, at 125 (quoting financial analyst Bert Hochfeld as saying, "Somebody's got to guarantee that there's a free and equal flow of information with an online system. Otherwise, you get some investors with an advantage over others and possible insider trading.").

97. Saul Cohen, *The Deadly Coupling of Public and Inside Information*, WALLSTREETLAWYER.COM, Oct. 1997, at 17.

98. *See* Dirks v. SEC, 463 U.S. 646, 657–58 (1983). The SEC chose poorly in deciding to make an example of investment adviser Raymond Dirks. He received a tip from a former employee of Equity Funding of America that the corporation had perpetrated a huge fraud. Dirks's actions led to the fraud being uncovered, yet the SEC pursued insider trading charges against him because in addition to tipping the SEC, insurance regulators, and others, he had also tipped his clients. *See id.* at 649 & n.2, 650. The Supreme Court noted that "[i]mposing a duty to disclose or abstain solely because a person knowingly receives material nonpublic information . . . could have an inhibiting influence on the role of market analysts, which the SEC itself recognizes is necessary to the preservation of a healthy market." *Id.* at 658.

institutional investors,[99] but that goal is far from being accomplished. Consider the following three scenarios:

a. E-mailing Corporate Developments to All Current Shareholders with E-mail Access

A strong argument can be made that e-mailing developments to current shareholders, by itself, would not constitute public disclosure. Again, "public" usually means generally available to the investing public. Under the traditional approach, one could claim that when a company e-mails corporate developments, such as annual earnings, to current shareholders, it omits two important constituencies: all current shareholders without e-mail, and all nonshareholders. The first group is fairly substantial, given that only about 15% of Americans currently "do e-mail."[100] The second group, all nonshareholders, is even larger. One might argue that although only a relatively small percentage of individual investors have access to the Dow Jones broad tape, investors who want access can obtain it more easily than access to other persons' e-mail.

However, if it is shown in a given case that the market price has reacted and impounded the information, then, as explained earlier,[101] the EMH approach mandates a conclusion that the information has become "public."

b. Posting Corporate Developments on a Passive Corporate Website

Many corporations are now posting substantial amounts of information important to investors on corporate websites.[102] This

---

99. *See Roundtable Participants*, *supra* note 77 (quoting David Pottruck, president of Charles Schwab, Inc., urging SEC to demand more level playing field for institutional and individual investors and to use the Internet to that end); *see also* Karen Damato, *Different Players, Different Access*, WALL ST. J., Apr. 24, 1998, at C1 (noting that institutional investors have better access to mutual fund advisers, but that Internet resources are helping to equalize access for small investors).

100. *See* FALLING THROUGH THE NET, *supra* note 89. On the other hand, this percentage of e-mail users is predicted by some to grow to 50% by 2001. *See* Diedtra Henderson, *High-Wire Act*, SACRAMENTO BEE, Mar. 12, 1997, at E1.

101. *See supra* Part II.A.2.

102. *See* Robert Prentice et al., *Corporate Web Site Disclosure and Rule 10b-5: An Empirical Evaluation*, 36 AM. BUS. L.J. (forthcoming Summer 1999) (containing empirical survey of current corporate website disclosure practices); *Technology is Making Big Changes in Investor Relations, Survey Finds*, BNA CORP. COUNS. DAILY, May 7, 1998 (noting increase in use of e-mail and websites to communicate with

information can include such market-moving information as recent financial results, press releases involving litigation, product development, and other matters. Do these postings constitute publication and dissemination so that insiders may then trade? Or must insiders post, wait a reasonable period of time for "absorption," and then trade?

These questions will soon be of even more pressing importance. Soon investors may not have to wait from quarter to quarter for the filing of 10-Qs[103] with the occasional 8-K[104] thrown in. Rather, the technology now largely exists for real-time financial reporting year-round. The American Institute of Certified Public Accountants and the Financial Accounting Standards Board are currently analyzing the matter and the SEC is closely following the debate.[105]

A strong argument can be made that information available only on a corporate website is not "public."[106] The Internet has been termed simply a "research tool" rather than being coextensive with the public domain.[107] Only about 45% of U.S. households contain computers;[108] in late 1998, 27% of U.S. homes had online access, up from 17% in 1997, but substantially lower than the 98% figure for televisions.[109] On the

---

investors); John C. Wilcox, *Electronic Communications and Proxy Voting: The Governance Implications of Shareholders in Cyberspace*, INSIGHTS, Mar. 1997, at 8 (noting substantial use of company websites to disclose important information in order to better serve numerous corporate constituencies).

103. A Form 10-Q, 17 C.F.R. § 249.308a (1998), must be filed within 45 days after the end of a company's first three quarters. The report consists primarily of financial data and material developments within the company. *See generally* BROWN, *supra* note 22, § 2.02[1][c], at 2-11.

104. A Form 8-K, 17 C.F.R. § 249.308 (1998), must be filed with the SEC within 15 days after a triggering event occurs, such as a change of control, sale of substantial assets, bankruptcy, or auditor change. *See generally* BROWN, *supra* note 22, § 2.02[1][b], at 2-9.

105. *See* Dominic Bencivenga, *Investors Push for Real-Time Data on Internet*, N.Y. L.J., May 7, 1998, at 5 (summarizing recent developments).

106. *Cf. supra* Part II.B.2.a. The SEC is apparently concerned about the adequacy of posting notices on websites. For example, under current guidelines, issuers must send out a schedule describing when information will be posted to websites. Thus, when unscheduled matters occur, the information must be sent to investors in paper form. Investment companies, among others, have complained about this rule. *See Roundtable Participants*, *supra* note 77.

107. *See* Morrow, *supra* note 87, at 2224 ("[I]n a legal context, the Internet is treated as a research tool, not public notice.").

108. *See* Walter S. Mossberg, *Computing Got Easier Last Year, but It Still Has a Long Way to Go*, WALL ST. J., Oct. 8, 1998, at B1 (noting that "only about 45% of U.S. homes have a PC, and that relatively few PCs are being sold to new households.").

109. *See id.* (doubting that computer use will rise until computers are made easier to

other hand, the percentage of Internet users among the *investing* public is probably much higher than that among the general public; the huge amount of financial information available on the Internet reflects this view.[110] However, even those who are active Internet users can scarcely be expected to check the websites of all public corporations several times a day to determine if anything new and material has been posted.

At a recent conference sponsored by the SEC, participants disagreed as to the proper approach to resolving the issues presented by this scenario. Some took the position that because an investor must "pull" the information, displaying releases on a corporate home page is not the full dissemination of information that is "pushed" at the media or others via a fax transmission. Others, including Harvey Pitt, argued that a posting on the Internet is equivalent to a Form 8-K filing or disclosure in a leading newspaper; investors must search for those as well.[111]

---

use).

110. *See, e.g.*, Edward H. Baker, *Tools of the Trade*, FIN. WORLD, Feb. 18, 1997, at 80 (describing for Web neophytes how they can use the Internet to research companies in which they are interested); Amy Dunkin, *For Investors of All Stripes, A Cornucopia on the Net*, BUS. WK., Dec. 22, 1997, at 104 (describing "wealth of Web material" aimed at investors); *Microsoft Investor Gives Access to Financial Reports from Off the Record Research*, M2 PRESSWIRE, Dec. 18, 1997 (noting that "cutting-edge research reports from Off the Record (OTR) Research that have never before been available to noninstitutional investors" now are at the Microsoft Investor site, <http://investor.msn.com/>); Colleen Neumann, *A Guide to Business-Related Web Sites*, STAR TRIB. (Minneapolis), Feb. 23, 1998, at 13 ("There is virtually no end to the business and investment resource material available on the World Wide Web."); Deb Price, *Internet Opens Investing to the Masses*, DETROIT NEWS, Jan. 10, 1998, at C1 ("Today, a cyber-investor has access — free — to about 80 percent of the information that once was the exclusive property of professional brokers. For an additional $200, that same investor could narrow the gap to 95 percent, says Douglas Gerlach, a cyber-investing guru who runs the popular Invest-o-rama site (http://investorama.com/)."); Joseph Szadkowski, *Investors Needn't Worry About a Lack of Information*, WASH. TIMES, Apr. 28, 1997, at D7 (summarizing numerous services providing information for online investors).

One site alone — Microsoft Investor — has 1.6 million unique visitors each month. That site contains tremendous amounts of helpful information to investors. *See Microsoft Investor Previews New Version with Breakthrough Tools*, M2 PRESSWIRE, Mar. 5, 1998 [hereinafter *Microsoft Investor*]. This service also has at least 37,000 regular subscribers who pay extra to access information that mere surfers cannot access. *See Profile: Chris Payne*, FIN. NETNEWS, Feb. 1, 1998, at 10.

111. *See SEC is Reluctant*, *supra* note 51. A key premise of the SEC's adoption of its integrated disclosure system in 1982 was that "information for certain types of companies is as accessible if on file with the SEC as it would be if physically delivered to prospective investors." James D. Cox, *The Fundamentals of an Electronic-Based Federal Securities Act*, 75 WASH. U. L.Q. 857, 872 (1997). "EDGAR" (the Electronic Data Gathering, Analysis, and Retrieval system) and the SEC's website

Which side has the better argument? Pitt's 8-K analogy is undermined by the fact that although an 8-K is a public document in a general sense, it arguably does not become public the moment it is filed. First, it is not accessible to the public for twenty-four to seventy-two hours.[112] Rather, the 8-K is made immediately available to a commercial firm which then feeds the information to other firms that sell the information to subscribers.[113] Second, filing an 8-K electronically with the SEC arguably satisfies the dissemination part of the test (or soon will) as to investors who have access to the Internet,[114] but perhaps not as to those without access. The SEC itself has characterized an 8-K disclosure as "an unusually clear case of burial disclosure" because the issuer is not required to send the information to security holders or to issue its contents in press release form.[115] Finally, electronic filing of the 8-K does not satisfy the absorption requirement. Again, it is improper for insiders to push one button on their keyboards to send the 8-K on its way to the SEC and then a second later push another button to execute a stock trade.[116]

It is reasonable for Pitt's opponents to argue that posting information on a passive corporate website, by itself, does not make for adequate public dissemination.[117] It is reasonable to expect an investor to read the *Wall Street Journal* every day. It is not as reasonable to expect an

---

<http://www.sec.gov/> come close to realizing that premise.

112. *See* Neumann, *supra* note 110, at 13.

113. *See* Marcia Vickers, *Rich, If Not Famous, in 15 Minutes*, N.Y. TIMES, July 14, 1996, at D7.

114. The SEC has made its EDGAR archive of all securities filings available on the Internet at <http://www.sec.gov/edgarhp.htm>.

115. BROWN, *supra* note 22, § 4.02[3][c], at 4–10 n.39 (internal quotation marks omitted) (quoting REPORT OF SEC ADVISORY COMMITTEE ON CORPORATE DISCLOSURE 181 (1983)).

116. In an interesting recent article, Professor Jesse Fried suggested that the profitability of corporate insider trading can be reduced by requiring insiders to predisclose their trades. *See* Jesse M. Fried, *Reducing the Profitability of Corporate Insider Trading Through Pretrading Disclosure*, 71 S. CAL. L. REV. 303 (1998). Essentially, he argues that we should put information regarding such trades in the public domain before the trades occur. He wishes to require that notice be given to the SEC and then suggests an absorption period — for the information to go from EDGAR to subscriber and news services such as Reuters, AP, and Bloomberg — of one, two, or three days, depending on "the speed with which the market can react to the announcement of a trade and the cost that delay would impose on insiders." *Id.* at 392 n.182.

117. *See* Mark A. Metz, *Don't Get Too Comfy with that Home Page*, BUS. L. TODAY, July–Aug. 1998, at 61 ("The mere inclusion of the information in the home page probably does not sufficiently disseminate the information to the extent necessary for it to be considered 'public' as the term is used in the securities law context.").

investor — especially one without Internet access — to search on a daily basis the websites of the companies in which she has invested.

On the other hand, the average investor has more reasonable access to the Internet than to the Dow Jones broad tape. True, access to the Internet in general does not necessarily give one access to information that is "hot off the presses" regarding particular companies, but Pitt's position is bolstered by the fact that investors can subscribe to services that will send them e-mail alerts on companies or entire industries of interest, which seems to be roughly equivalent to having a subscription to the Dow Jones broad tape.[118] Most individual investors may not subscribe to such services, but most will also choose not to subscribe to the Dow Jones broad tape. Access to either is available to diligent investors.

Ultimately, I deem Pitt's position to be slightly more persuasive. Even individual investors should be nudged in the direction of taking advantage of what the Internet has to offer. If adequate time for absorption is required, and this could vary from company to company depending on their profile in the investment community, no substantial unfairness should result from accepting Pitt's position. Furthermore, any evidence that the information has been incorporated into the company's stock price, pursuant to the EMH, should create a nearly conclusive presumption that the information is no longer nonpublic.

c. Authorizing a CEO's Meeting with Analysts to be Broadcast in Real Time on the Internet

As one observer recently noted:

> Thanks to the rapid spread of faster and faster computers, e-mail, high speed modems, and the information superhighway . . . , today's corporate management is provided with reports of sales and other business items as they occur. Companies are pressed by analysts and institutions to provide this information as quickly as it is reported, not just quarter by quarter as in the past. Take, for example, a current advertisement for a site on the World Wide Web, which promises to anyone "audio and video coverage

---

118. *See* Dunkin, *supra* note 110, at 105 (noting e-mail and other services available on the Internet); *Thomson Investors Network, AT&T to Build AT&T WorldNet Investors Network*, M2 PRESSWIRE, July 29, 1997 (describing similar services).

> of market-moving events — as they happen . . . . CEO interviews, brokerage conferences, corporate presentations."[119]

All of these means of disclosure can raise similar questions, but to focus the discussion, assume that an investor subscribes to the described service and is given access to the site on the World Wide Web. A high-tech company's CEO is meeting with a small group of analysts to answer their questions about rumors that have been circulating about the company.

The meeting with the analysts, in and of itself, raises sensitive issues regarding insider trading law. In a speech in March of 1998, SEC Chairman Arthur Levitt noted that he had seen an increase in trading-volume jumps occurring between analysts' conferences and the issuance of general news releases, and warned that the SEC was looking closely at trading by analysts.[120] Yet at the same time, some lawyers argued that a teleconference with dozens of analysts would be the equivalent of a public disclosure, especially because small investors "can get on the Internet and get the releases fairly quickly now."[121] However, the SEC seems to be of the view that such a meeting would not by itself constitute public disclosure.[122] For that reason, it has been suggested that companies begin their teleconferences with analysts by warning the analysts that what they hear may constitute material, nonpublic information that they use at their own peril.[123] Such warnings certainly take out much of the fun for the analysts.

Would a simulcast of that meeting, broadcast over the Internet to hundreds or perhaps thousands of investors subscribing to the aforementioned service, constitute public dissemination so that the right to trade would promptly follow (after some minimal time for absorption)? If so, the subscription service seems well worth the price: subscribers have the chance to trade upon information known only to a few other investors — not to the 1.8 million who read the *Wall Street*

---

119. Cohen, *supra* note 97, at 17 (alteration in original).

120. *See* Paul Beckett & Rebecca Buckman, *SEC's Levitt Warns Analysts on Certain Trades*, WALL ST. J., Mar. 9, 1998, at B7B.

121. *Id.* (quoting Peter Davis, a consultant with Booz Allen & Hamilton) (internal quotation marks omitted).

122. *See* Baruch Lev, *Disclosure and Litigation*, CAL. MGMT. REV., Spring 1995, at 8, 22 ("The relationship between corporate executives and financial analysts is sensitive and fraught with legal pitfalls.").

123. *See* Beckett & Buckman, *supra* note 120, at B7B (citing former SEC Commissioner Edward Fleischman).

Journal each day. If not, the subscription service is much less valuable in that it grants investors access to information that they cannot legally trade upon. They must wait to trade until the same information is disseminated via a broader medium and the time for absorption passes.

Which approach is the law? Cases point both ways. The hypothetical bears strong resemblance to the SEC proceeding in *Faberge, Inc.*,[124] discussed earlier,[125] where subscribers to the AutEx wire system received advance information about block trades. The SEC held that dissemination to only a limited number of institutional subscribers did not constitute public disclosure.[126] In contrast, in *du Pont Glore Forgan, Inc. v. Arnold Bernhard & Co.*,[127] the court found dissemination through the Reuter's Financial Service Report to be "public" even though the service had only 654 subscribers in 38 states. As noted above,[128] two of the three market makers in the subject stock subscribed to the Reuters service, the third (the plaintiff) had already contracted to do so, and the NYSE and American Stock Exchanges required their listed companies to disseminate earnings through Reuters as well as through the Dow Jones broad tape.

Today, the outcome of such a case should revolve around a fact-specific determination of whether the number and type of subscribers to the service more closely resemble the relatively few institutional investors in *Faberge* or the more numerous subscribers in *duPont*. Although the market for information is clearly going to become more and more efficient, equality of access is a value that should not be ignored. Again, defendants should escape liability by proving that the information was incorporated into the issuer's stock price by the efficient market before they traded, and an issuer should be able to avoid any controversy by coupling disclosure of the CEO's simulcast meeting with analysts with the other forms of disclosure mentioned in Part II.B.1.

Because of the potential value that these various forms of Internet communications embody,[129] it seems clear that companies will continue to push the envelope. A single posting on an obscure website does not put information in the public domain for insider trading purposes,

---

124. 45 S.E.C. 249 (1973).

125. *See supra* notes 43–45 and accompanying text.

126. *See Faberge*, 45 S.E.C. at 255. The number of subscribers was not specified.

127. No. 73 Civ. 3071, 1978 U.S. Dist. LEXIS 20385 (S.D.N.Y. Mar. 6, 1978).

128. *See supra* notes 46–50 and accompanying text.

129. *See Investor Relations: The Delicate Job of Chatting with Investors Online*, WALLSTREETLAWYER.COM, Jan. 1998, at 18–19 (noting advantages stemming from company's ongoing dialogue with individual investors through message boards on America Online's Motley Fool and Silicon Investor).

although it might conceivably do so for other securities law[130] and nonsecurities law purposes.[131] The SEC announced in early 1999 that within two years it would probably issue new rules addressing what constitutes effective public disclosure.[132] Given the amount of information currently available to investors on the Internet,[133] and, more importantly, the speed with which that information is becoming available,[134] it seems that the SEC (and the courts) should in close cases err on the side of recognizing disclosure over the Internet as "public."[135]

---

130. For example, the SEC has taken the position that posting information about a securities offering on an issuer's website is sufficient to constitute a "general solicitation," thus disqualifying the offering for certain 1933 Securities Act exemptions. However, there are different policy considerations in determining whether there has been a "public" disclosure for insider trading purposes. *See* Use of Electronic Media for Delivery Purposes, Securities Act Release No. 7233, 60 Fed. Reg. 53,458, 53,458 n.9, 53,463 n.40 (Oct. 6, 1995).

131. For example, a trade secret holder might forfeit the "secrecy" of its information and thus lose intellectual property protection by posting the information on a publicly-accessible website, and for purposes of copyright law, items are often viewed as "published" once they appear on the Internet. *See, e.g.*, Religious Tech. Ctr. v. NetCom On-line Communications Serv., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (holding that information published on the Internet can thereby pass into public domain). However, the issue in these trade secret and copyright cases is different than that in an insider trading case. In the former, the question is whether there was sufficient public exposure to compromise the intellectual property owner's rights. In the latter, the question is whether there was sufficient exposure to alert the general public. Two different levels of exposure are involved. *See* Morrow, *supra* note 87, at 2216–17.

132. *See Insider Trading: Goldschmid Says SEC Considering Rulemaking in Insider Trading Cases*, BNA SEC. L. DAILY, Feb. 10, 1999 (citing SEC General Counsel as saying that rules may also address use versus possession of inside information and fiduciary relationships for misappropriation theory purposes).

133. *See supra* note 110.

134. *See Microsoft Investor*, *supra* note 110 (quoting Craig Gordon, founder of Off the Record Research, as saying that "[t]he Internet is accelerating the pace at which individual investors can receive information and is truly beginning to rival the information available to professional money managers").

For this reason, Langevoort has noted that informational efficiency of the securities markets will expand with the new technology, although the fundamental efficiency of the markets may be another matter. *See* Donald C. Langevoort, *Toward More Effective Risk Disclosure for Technology-Enhanced Investing*, 75 WASH. U.L.Q. 753, 758 (1997).

135. This bias would also be consistent with Roberta Karmel's excellent suggestion that the SEC reformulate insider trading policy to encourage more rapid disclosure of corporate information rather than to suppress the use of nonpublic information. *See* Roberta S. Karmel, *Outsider Trading on Confidential Information—A Breach in Search of a Duty*, 20 CARDOZO L. REV. 83, 84 (1998) [hereinafter Karmel, *Outsider Trading*].

III. CAN "HACKERS" BE MISAPPROPRIATORS?

A. The Problem

Computer "hacking" is a serious problem of epidemic proportions.[136] Computer hackers have broken into and altered the home pages of major corporations,[137] the Department of Defense,[138] and even the Central Intelligence Agency.[139] These hackers can cause many different kinds of damage,[140] costing billions of dollars annually in theft of information

---

136. *See* Richard Behar, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 59 (noting that estimated financial losses from computer crime amount to $10 billion a year, but that this number is unreliable because as many as 95% of attacks go undetected and 85% of those that are detected go unreported, and quoting the Federal Bureau of Investigation as stating, "The hackers are driving us nuts. Everyone is getting hacked. It's out of control."); David M. Remnitz & Ryan Breed, *Network Security Audits Keep the Hackers at Bay*, NAT'L L.J., Feb. 2, 1998, at C9 (noting that Ernst & Young survey on information security found that 38% of all U.S. respondents had been victims of industrial espionage in previous year).

137. *See* Tim Wilson, *Profits Embolden Hackers*, INTERNETWEEK, Mar. 23, 1998 (discussing Internet hackers' attacks on corporate home pages).

138. *See* Andrew J. Glass, *Hackers Hit Computers at Defense Department*, AUSTIN AM.-STATESMAN, Feb. 26, 1998, at A4 (noting that the Pentagon logged more than 250,000 attempted attacks on its nonclassified computer systems in 1995, 60% of which had some success).

139. *See* Erik Sherman, *Secure Internet Commerce Means Upfront Precautions*, MACWEEK, Mar. 3, 1997, at 29 (mentioning hacker attack on Central Intelligence Agency website).

140. *See* Jared Sandberg, *Hackers Prey on AOL Users with Array of Dirty Tricks*, WALL ST. J., Jan. 5, 1998, at B1 [hereinafter Sandberg, *Hackers*] (describing "phishing," "carding," "pinting," "instant message bombing," "e-mail bombing," "tossing," "proggies," and "Trojan horses"); Jared Sandberg, *Internet Vandals Pose Threat by Using New Mode of Attack Called "Smurfing,"* WALL ST. J., Jan. 9, 1998, at B18. *See generally* DAVID H. FREEDMAN & CHARLES C. MANN, AT LARGE: THE STRANGE CASE OF THE WORLD'S BIGGEST INTERNET INVASION (1997) (painting frightening picture of damage hackers can inflict); Arnaud de Borchgrave, *Electronic Bank Robbers Flourish*, WASH. TIMES, Apr. 21, 1997, at A12 (describing extensive plague of computer crime).

alone.[141] In addition, as use of the Internet rises, exposure to break-ins increases dramatically.[142]

Often, hackers act solely to be mischievous. But they frequently hack for a commercial motive. As one hacker said: "When I was a child, I hacked as a child, . . . [t]hen it was time to make some money."[143] One way that hackers might make money is to plant false information on corporate websites or investor electronic bulletin boards

---

141. *See* Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 216 (1995) (noting serious problem of theft of information by hackers); Heather Brewer, *Online Losses*, BUS. LAW. TODAY, May–June 1998, at 6 (citing study finding that 88% of reporting Fortune 500 companies had suffered security breaches, 75% had suffered financial losses, and 44% had been hacked by outsiders); Jack Nelson, *Grappling with Crime Wave on the Web*, L.A. TIMES, Nov. 30, 1997, at A10 (noting that computer hackers committing commercial espionage cost $100 billion annually in United States alone); Clinton Wilder & Bob Violino, *Data Security: Online Theft — Trade in Black Market Data is a Growing Problem for Both Business and the Law*, INFORMATIONWEEK, Aug. 28, 1995, at 30 (noting that $10 billion in information is stolen from U.S. industry annually).

There are many different ways of causing damage. *See, e.g.*, Kate Button, *Hacking Off the Hackers*, COMPUTER WEEKLY, Jan. 16, 1997, at 40 (noting examples of $12 million stolen from Citibank Corporation in New York by Russian hackers and $50 million in goods charged to credit card numbers stolen from MCI); Wilder & Violino, *supra*, at 30 (noting estimates that U.S. cellular-phone industry loses $1.5 million per day to fraud and that combined cellular and long-distance fraud, stemming largely from computer hacking, totals $4–$5 billion annually). *See generally* David L. Gripman, Comment, *The Doors Are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167 (1997) (containing extensive description of computer security problems in United States).

142. *See* Behar, *supra* note 136, at 58 ("The more the computers of the business world become interconnected — via the Internet and private networks — the more exposed they are to break-ins."); Wilder & Violino, *supra* note 141, at 30 ("[T]he increasing use of online commerce among major corporations could substantially increase the risk of electronic theft for all industries.").

143. David Holthouse, *Hacker, Cracker, Watchman, Spy*, PHOENIX NEW TIMES, June 12, 1997; *see also* Button, *supra* note 141, at 40 (quoting computer consultant who believes that as hackers get older "their harmless or often irritating antics take on a more sinister aspect: as they get cars and mortgages their intent is based on financial gain rather than exploration"); S.J. Ross, *Hack Attack: While the Rest of Us Sleep, a Subculture of Hackers, Phreakers, Thieves, Pirates and Pranksters Goes About Its Business in Cyberspace*, TORONTO STAR, Jan. 15, 1998, at J1 (describing hacker subculture and its occasional commercial motivation).

for purposes of manipulating the company's stock.[144] I have addressed the legal implications of such activity elsewhere.[145]

Another commonly expressed fear is that hackers will break into issuers' computer systems for purposes of obtaining confidential information that could be used for insider trading or sold to those who intend to engage in insider trading.[146] One computer security expert has noted that biotech companies, because they have so much data in computers and flowing over the Internet, are particularly vulnerable to hackers stealing information for insider trading purposes.[147] Several different methods could be successfully employed for such crimes.[148] This danger has led some firms to contact computer security experts regarding means of safeguarding information so that it cannot be stolen and used for insider trading.[149]

To combat theft of inside information by hackers and their allies who might use that information for insider trading or other improper

---

144. *See* Robert A. Robertson, *Personal Investing in Cyberspace and the Federal Securities Laws*, 23 SEC. REG. L.J. 347, 406–09 (1996) ("The potential for market manipulation using the Internet and the on-line services is substantial and may present new challenges for state and federal regulatory agencies."); Edward Wyatt, *Fake News Account on Web Site Sends Stock Price Soaring*, N.Y. TIMES, Apr. 8, 1999, at A1.

145. *See* Prentice, *Corporate Disclosure*, *supra* note 3, at 44–58. A hacker can accomplish the same manipulative purpose by sending out an e-mail to investors that appears to come from the issuer itself. For a discussion of how such a scheme could be accomplished, see Joseph E. Cella III & John Reed Stark, *SEC Enforcement and the Internet: Meeting the Challenge of the Next Millennium — A Program for the Eagle and the Internet*, 52 BUS. LAW. 815, 826–27 (1997).

146. *See, e.g.*, Ingrid Meyer, *Security Spending Rises — Businesses Support Electronic Commerce Despite Hacker Threats*, COMMUNICATIONSWEEK, Sept. 30, 1996, at 45 ("[M]any [hackers] have a profit motive — obtaining company information that can be used for insider trading and sold at a premium . . . .").

147. *See* Mara Bovsun, *Spies Who Came in from the Cold War Find Hot Target in Biotechnology*, BIOTECHNOLOGY NEWSWATCH, Jan. 2, 1995, at 1 ("Computer hackers pose a huge threat, said [security expert Alan E.] Brill. With so much data in computers and speeding along the Internet, biotechs are particularly vulnerable to both insider trading and trade secret theft.").

148. *See* Behar, *supra* note 136, at 66 (describing "sniffers," which are "programs that, planted in a computer that is connected to a network, work like hidden recorders, capturing E-mail messages and passwords as they flow by. 'You can get inside information on everything flowing through a company,' says Daniel Kozin, a Boston computer-networking expert.").

149. *See Encryption, Key Recovery, and Privacy Protection in the Information Age: Hearings on S. 376 and S. 909 Before the Senate Comm. on the Judiciary*, 105th Cong. 81 (1997) (statement of Raymond Ozzie, Chairman, Iris Associates) ("[Firms] are looking to cryptography in products from vendors such as myself to help them reduce their exposure to break-ins, to disclosure of trade secrets, *insider trading*, corporate espionage, covert transactions." (emphasis added)).

purposes, companies are spending untold sums on security procedures like firewalls.[150] However, it seems likely that determined hackers will be able to overcome even the most sophisticated and expensive security precautions for the foreseeable future.[151] When a hacker is caught trading on stolen nonpublic information, an interesting question that goes to the very heart of insider trading law arises: Can a hacker be liable for insider trading? More specifically, can a hacker be a "misappropriator" within the definition of the federal securities laws?

B. Hackers as Misappropriators

1. The Traditional View

Hackers who steal inside information and trade on it are essentially thieves. But are they also liable as inside traders? The answer to this question from a traditional point of view is "no."[152] There are essentially four categories of persons who owe a duty to "disclose or abstain" and incur liability for insider trading if they breach that duty: (1) company insiders, (2) temporary insiders, (3) misappropriators, and (4) tippees of the previous three categories or of other tippees.[153] The hacker is neither a company insider, a temporary insider, nor a tippee.[154] If a hacker is to be plugged into one of the four traditional categories of insider trading defendant, the most promising candidate is that of misappropriator. Yet

---

150. *See* Behar, *supra* note 136, at 58 (noting that U.S. corporations spent $6 billion on network security in 1996); Meyer, *supra* note 146, at 45 (discussing firewalls and other security procedures).

151. *See* Behar, *supra* note 136, at 57, 59, 70 (noting that 30% of all break-ins involving the Internet occur despite the presence of firewalls; WheelGroup, a security firm, seems to be able to hack into the website of any company; and recent tests by *LAN Times* (a trade magazine) of seven leading commercial firewalls found all to be lacking).

152. *See* Barbara Bader Aldave, *Misappropriation: A General Theory of Liability for Trading on Nonpublic Information*, 13 HOFSTRA L. REV. 101, 122 (1984); Corey J. Smith, Note, *Extraterritorial Enforcement of Rule 10b-5: Insider Trading in the International Equities Market*, 12 SUFFOLK TRANSNAT'L L.J. 83, 97 (1988) (noting that "under [the misappropriation] theory parties who obtain inside information by theft are free to use it to their advantage while parties who obtain information through a 'confidential relationship' are not").

153. *See* Robert A. Prentice, *The Impact of* Dirks *on Outsider Trading*, 13 SEC. REG. L.J. 38, 54–57 (1985).

154. The underlying assumption is that the hacker does not independently have the status of a proper insider trading defendant. If, for example, a company employee hacked into files that she had no proper access to, she could be liable for insider trading as a company insider who breached a fiduciary duty to current and potential shareholders.

the general view has been that misappropriation does not encompass illegal acquisition of information. Rather, its essence is lawful possession, but illicit application.[155]

This traditional view is bolstered by the language of the *O'Hagan* opinion, which, while not explicitly ruling out liability based on criminal acts, definitely implies that misappropriation liability can be based only upon a breach of fiduciary duty.[156] Justice Ginsburg's introduction to the misappropriation theory stated clearly that the theory applies when a defendant "misappropriates confidential information for securities trading purposes, *in breach of a duty owed to the source of the information.*"[157] She elaborated:

> Under this theory, a fiduciary's undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information . . . . [T]he misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information.[158]

To the extent that misappropriation liability is based solely on a breach of fiduciary duty, thieves unrelated to the source of the information could steal the information without being in violation of

---

155. *See* Jeffrey P. Strickler, Comment, *Inside Information and Outside Traders: Corporate Recovery of the Outsider's Unfair Gain*, 73 CAL. L. REV. 483, 512 n.160 (1985) ("Misappropriation can be distinguished from illegal acquisition. A party misappropriating information has been given lawful possession of the information subsequently used for an unlawful purpose, while the thief has never had a lawful right to possess the information.").

156. *See* Richard W. Painter et al., *Don't Ask, Just Tell: Insider Trading After* United States v. O'Hagan, 84 VA. L. REV. 153, 181 (1998) (noting that Government conceded during *O'Hagan* oral arguments that misappropriation theory would not cover thieves, industrial spies, and other nonfiduciaries); Joel Seligman, *A Mature Synthesis: O'Hagan Resolves "Insider" Trading's Most Vexing Problems*, 23 DEL. J. CORP. L. 1, 14 (1998) (noting that *O'Hagan's* fiduciary duty requirement "would preclude Rule 10b-5 liability for those who engage in industrial espionage or the outright thief").

157. United States v. O'Hagan, 521 U.S. 642, 652 (1997) (emphasis added).

158. *Id.* The *O'Hagan* facts presented a nearly prototypical scenario of misappropriation — an attorney who worked for a law firm hired by a would-be acquirer took information (the identity of the target corporation) that the law firm's client would have wished to keep confidential and converted it to his own benefit by trading on it. *See id.* at 647–48.

existing federal securities laws.[159] Under the traditional view, they would have to be punished for their misdeeds via mail fraud, wire fraud, simple theft, or other comparable statutes.

2. A Nontraditional Argument

I find uncomfortable the received wisdom that someone who obtains inside information via hacking, physical breaking and entering, bribery, extortion, espionage, or similar means is not liable for insider trading when such trading was the entire motivation behind the initial criminal act. In this Section, I argue that "misappropriation" should be construed broadly enough to embrace these other physical acts, which tend to be at least as morally blameworthy as the breach of a fiduciary duty.

First, it seems clear that hackers who steal nonpublic information and trade on it are "misappropriators" by any standard dictionary definition.[160] After all, "steal" and "misappropriate" are synonyms.[161]

Second, Chief Justice Burger, the original Supreme Court proponent of the misappropriation theory, clearly seemed to believe, in his *Chiarella* dissent, that misappropriation covered theft.[162]

Third, holding such thieves liable as misappropriators would bolster the legislative purposes of the Exchange Act, which are to advance the ethical standards in every aspect of the securities industry[163] and to encourage and reward the production of information.[164] In addition, it

---

159. *See* Wolowitz & Diana, *supra* note 6, at B12 ("Thus, a third party who intercepts confidential information about a business through Internet communications or e-mails of corporate officers and subsequently trades on such information may not be in violation of existing federal securities laws.").

160. *See, e.g.*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 838 (New College ed. 1982) (defining "misappropriate" as meaning "[t]o appropriate wrongly," "[t]o appropriate wrongly for one's own use; embezzle," and "[t]o use for illegal purposes").

161. *See, e.g.*, WEBSTER'S NEW WORLD THESAURUS 750 (3d ed. 1997).

162. In his *Chiarella* dissent, Chief Justice Burger sought to pin liability upon the defendant because he had "misappropriated — *stole* to put it bluntly — valuable nonpublic information . . . ." Chiarella v. United States, 445 U.S. 222, 245 (1980) (Burger, C.J., dissenting) (emphasis added). His theory rested on the notion that obtaining information illicitly serves no useful purpose and does not involve the type of skill and foresight that should be protected. *See id.* at 241–42.

163. *See* Bateman Eichler, Hill Richards, Inc. v. Berner, 472 U.S. 299, 315 (1985); SEC v. Capital Gains Research Bureau, 375 U.S. 180, 186–87 (1963).

164. *See* Paula J. Dalley, *From Horse Trading to Insider Trading: The Historical Antecedents of the Insider Trading Debate*, 39 WM. & MARY L. REV. 1289, 1329 (1998) ("Because one of the goals of the law is to encourage and reward both diligence and the production of information, a rule that distinguishes between information acquired by

would also advance the most fundamental policies underlying the misappropriation theory. As Justice Ginsburg noted in *O'Hagan*, the theory is aimed at protecting "the integrity of the securities markets against abuses by 'outsiders' to a corporation who have access to confidential information that will affect th[e] corporation's security price when revealed, but who owe no fiduciary or other duty to that corporation's shareholders."[165] The hacker fits precisely within that definition: an outsider with access to confidential information who, owing no duty to the corporation's shareholders, undermines the integrity of the securities markets by trading on purloined nonpublic information.

Fourth, although Justice Ginsburg's opinion clearly implies that application of the misappropriation theory may be premised solely on the breach of a fiduciary duty of confidentiality, nowhere does she explicitly say that misappropriation liability could not be based on hacking or some other form of theft.[166] Any such statement would have been dicta anyway; the point was not at issue in *O'Hagan*.

Fifth, it seems to be the near-consensus that Justice Ginsburg's opinion is not entirely satisfying. Its logic fails to tie up all the loose ends of the misappropriation theory.[167] Given its limitations, it is doubtful that Justice Ginsburg's opinion constitutes the last word on the misappropriation theory. Therefore, it is reasonable to try to come up with an approach that is either seamless, or at least more comprehensive.

---

lawful effort and information acquired by theft or accident makes a great deal of sense.").

165. *O'Hagan*, 521 U.S. at 653 (alteration in original) (internal quotation marks omitted).

166. *See* Painter et al., *supra* note 156, at 181 ("The Court's opinion in *O'Hagan* does not explicitly concede [that thieves cannot be covered by the misappropriation theory], but it does so impliedly by emphatically stating that the misappropriation theory requires both a prior fiduciary relationship and deception of the principal by the fiduciary.").

167. *See, e.g.*, *id.* at 155 (noting that *O'Hagan* "left many questions unresolved"); Carol M. Swanson, *Reinventing Insider Trading: The Supreme Court Misappropriates the Misappropriation Theory*, 32 WAKE FOREST L. REV. 1157, 1212 (1997) ("Before *O'Hagan*, insider trading law was in confused disarray . . . . After *O'Hagan*, the world looks very much the same."); Holman W. Jenkins, Jr., *Knowing Naughty Information from Nice*, WALL ST. J., July 22, 1997, at A15 (criticizing *O'Hagan*'s lack of clarity); Harvey L. Pitt & Karl A. Groskaufmanis, *The Supreme Court Has Upheld the Misappropriation Theory, but How Far the SEC Will Take the Ruling is Anything but Clear*, NAT'L L.J., Aug. 4, 1997, at B4 [hereinafter Pitt & Groskaufmanis, *Upheld Misappropriation Theory*] (same criticism). *But see* Seligman, *supra* note 156, at 24 (arguing that after *O'Hagan*, "[t]here may be fuzziness at the exotic extremes, but for the overwhelming majority, there should be little doubt when [defendants] have violated Rule 10b-5").

The opinion itself admits that the misappropriation theory as explicated is only "a *partial* antidote" to insider trading abuses.[168] While courts tinker, they should remember the Second Circuit's opinion in *United States v. Carpenter*,[169] which stated that "trading on the basis of improperly obtained information is fundamentally unfair, and that distinctions premised on the source of the information undermine the prophylactic intent of the securities laws."[170] The same may be said of distinctions that find a violation of the insider trading rules when a lawyer like O'Hagan snoops around her partners' offices to steal inside information but do not find a violation when a hacker cracks the same law firm's computer system to copy the same information.[171]

Sixth, to hold that hackers are misappropriators is consistent with the pre-1934 common law upon which Section 10(b) was based,[172] is consonant with the underlying policy of Section 10(b) — investor protection,[173] and is consistent with more recent congressional actions. By refusing to enact a statutory definition of "insider trading," Congress has delegated to the courts the task of fleshing out the rules in this area. Yet, when Congress recently addressed insider trading issues, by enacting both the Insider Trading Sanctions Act of 1984 ("ITSA")[174] and the Insider Trading Securities Fraud and Enforcement Act of 1988 ("ITSFEA"),[175] it did so to *expand* the scope of liability delineated by the

---

168. *O'Hagan*, 521 U.S. at 659 n.9 (emphasis added).

169. 791 F.2d 1024 (2d Cir. 1986), *aff'd by an equally divided court*, 484 U.S. 19 (1987).

170. *Id.* at 1029 (internal quotation marks omitted) (quoting SEC v. Musella, 578 F. Supp. 425, 438 (S.D.N.Y. 1984)).

171. *See* Dalley, *supra* note 164, at 1314 ("[T]here is no reason why fraud . . . should be limited to breach of fiduciary duty.").

172. Back in 1936, Professor Keeton wrote that "[a]ny time information is acquired by an illegal act it would seem that there should be a duty to disclose that information . . . ." W. Page Keeton, *Fraud-Concealment and Non-Disclosure*, 15 TEX. L. REV. 1, 25–26 (1936).

173. *See* Bateman Eichler, Hill Richards, Inc. v. Berner, 472 U.S. 299, 315 (1985) (noting that the main policy underlying passage of the Exchange Act was "protection of the investing public and national economy through promotion of 'a high standard of business ethics'" (quoting SEC v. Capital Gains Research Bureau, Inc., 375 U.S. 180, 186 (1963))); *see also* Karmel, *Outsider Trading*, *supra* note 135, at 113 ("[W]hen Congress passed and subsequently amended the Exchange Act, it was concerned about fairness and the protection of investors . . . .").

174. Pub. L. No. 98-376, 98 Stat. 1264 (codified as amended in scattered sections of 15 U.S.C.).

175. Pub. L. No. 100-704, 102 Stat. 4677 (codified as amended in scattered sections of 15 U.S.C.). Among other things, ITSFEA expanded the scope of civil penalties for those who fail to take adequate steps to prevent their agents from engaging in insider trading, created a bounty system to aid detection of wrongdoers, increased criminal

courts, not to restrict it.[176] Congress has completely accepted the rationale of those who would broadly prohibit insider trading[177] and it has sought to fight all forms of fraud caused by insider trading.[178]

ITSA's legislative history suggests that the important inquiry is whether "the informational advantage [was] improperly obtained, that is, one which others cannot obtain through lawful means or competition?"[179] This question, in the hacker context, leads to an affirmative answer despite the lack of a fiduciary duty owed by the hackers to corporate shareholders. ITSA, by extending the coverage of insider trading rules to options traders, went beyond the scope of fiduciary duty to impose liability, laying the groundwork for a similar extension regarding hackers trading on stolen information.[180]

---

penalties for insider trading, created a new cause of action for "contemporaneous traders," and enhanced the SEC's authority to cooperate with foreign authorities in investigating international securities law violations. *See* H.R. REP. NO. 100-910, at 7 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6044.

176. Taken together, the thrust of ITSA and ITSFEA was to support a broad and flexible view of what activity constitutes insider trading, to boost sanctions against the activity, to increase the powers of both the SEC and private plaintiffs to sue wrongdoers, and to facilitate SEC enforcement efforts.

177. In the House Report accompanying passage of ITSFEA in 1988, the House made its position clear in the debate over the wisdom of regulating insider trading:

> A modest number of economists and academics defend the practice of insider trading as promoting an efficient market. Some free market economists even favor legalizing insider trading . . . . But the far greater number of commentators support efforts to curb insider trading, viewing such efforts as crucial to the capital formation process that depends on investor confidence in the fairness and integrity of our securities markets. Insider trading damages the legitimacy of the capital market and diminishes the public's faith. The investing public has a legitimate expectation that the prices of actively traded securities reflect publicly available information about the issuer of such securities. According to this view, the small investor will be — and has been — reluctant to invest in the market if he feels it is rigged against him.

H.R. REP. NO. 100-910, at 8 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6045.

178. *See* United States v. Carpenter, 791 F.2d 1024, 1030 (2d Cir. 1986) (referring to ITSA and quoting H.R. REP. NO. 98-376, at 4 (1983), *reprinted in* 1984 U.S.C.C.A.N. 2274, 2277), *aff'd by an equally divided court*, 484 U.S. 19 (1987).

179. Robert B. Titus & Peter G. Carroll, *Netting the Outsider: The Need for a Broader Restatement of Insider Trading Doctrine*, 8 W. NEW ENG. L. REV. 127, 151 (1986).

180. In adding section 20(d) to the Exchange Act, Congress provided that wherever tipping or trading would violate the insider trading proscriptions, such activity in connection with derivative securities would result in comparable liability to purchasers

ITSFEA, by enacting a right to sue on behalf of "contemporaneous traders," to whom defendants owe no fiduciary duty, clearly bolsters the misappropriation theory as later explicated by Justice Ginsburg and goes beyond it.[181] Indeed, in drafting ITSFEA, Congress expressly stated its support for then-existing theories of liability, including the misappropriation theory (as explicated by the courts and enforced by the SEC, if undefined by statute) and Rule 14e-3.[182]

---

or sellers in the derivative market. *See* Insider Trading Sanctions Act § 5. *See generally* Daniel L. Goelzer et al., *Insider Trading Legislation: A Review and a Preview, in* INSIDER TRADING: COPING WITH THE USE AND ABUSE OF MARKET SENSITIVE INFORMATION 239, 251 (Law & Business 1985) (describing ITSA's provisions on derivative securities).

Because option holders are not shareholders of the issuer, it had been argued that insiders of the issuer did not owe any duty to disclose or abstain before trading in standardized options. By enacting ITSA, Congress clearly rejected that notion, extending insider trading liability to the options market. *See* Steve Thel, *Section 20(d) of the Securities Exchange Act: Congress, the Supreme Court, the SEC, and the Process of Defining Insider Trading*, 69 N.C. L. REV. 1261, 1267 (1991) ("With section 20(d), Congress provided very explicit evidence that corporate insiders' duty to disclose information is broader than the duty the [Supreme] Court was prepared to recognize in *Chiarella*.").

181. This cause of action, which overruled a restrictive holding in *Moss v. Morgan Stanley, Inc.*, 719 F.2d 5 (2d Cir. 1983), could be premised only upon the misappropriation theory. *See* H.R. REP. NO. 100-910, at 26 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6063. The House Report described various acts of misappropriation and stated that "this type of security fraud should be encompassed within Section 10(b) and Rule 10b-5." *Id.* at 10, *reprinted in* 1988 U.S.C.C.A.N. at 6047.

182. *See* Howard M. Friedman, *The Insider Trading and Securities Fraud Enforcement Act of 1988*, 68 N.C. L. REV. 465, 472–75 (1990) (discussing Rule 14e-3); *id.* at 481–83 (discussing misappropriation theory).

Section 2 of ITSFEA provides:

> The Congress finds that —
>
> (1) the rules and regulations of the Securities and Exchange Commission under the Securities Exchange Act of 1934 governing trading while in possession of material, non-public information are, as required by such Act, necessary and appropriate in the public interest and for the protection of investors;
>
> (2) the [SEC] has, within the limits of accepted administrative and judicial construction of such rules and regulations, enforced such rules and regulations vigorously, effectively, and fairly; and
>
> (3) nonetheless, additional methods are appropriate to deter and prosecute violations of such rules and regulations.

Insider Trading and Securities Fraud Enforcement Act of 1988, Pub. L. No. 100-704, § 2, 102 Stat. 4677, 4677 (codified at 15 U.S.C. § 78u-1 note (1994)).

Congress explicitly stated that its "findings" were "intended as an expression of

When drafting ITSFEA, Congress considered enacting an explicit definition of insider trading that would have outlawed all "wrongful" use of inside information. The term "wrongful" was defined to include breach of the various relationships — personal, contractual, fiduciary, and employment — that the courts have used to support the misappropriation theory and such acts as theft, conversion, or misappropriation.[183] Had that definition been adopted, it clearly would have ensnared hackers caught stealing and trading on nonpublic information. Congress ultimately failed to enact this definition, but not because it did not wish to outlaw theft, conversion, or misappropriation of inside information as forms of insider trading. It simply chose not to enact a fixed definition in order to avoid limiting SEC flexibility and allowing wrongdoers to find loopholes in the law.[184]

Recognizing hackers and other thieves as misappropriators rectifies a few of the more obvious shortcomings of the misappropriation theory. A theory tied solely to the breach of a fiduciary duty to the source of the

---

congressional support for these regulations." H.R. REP. NO. 100-910, at 35 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6072; *see also* Bainbridge, *Incorporating*, *supra* note 8, at 1232–33 (concluding that in enacting ITSFEA, and perhaps even ITSA, Congress clearly endorsed both misappropriation theory and Rule 14e-3); Steve Thel, *Statutory Findings and Insider Trading Regulation*, 50 VAND. L. REV. 1091, 1134 (1997) (noting that "on careful examination [the Congressional findings regarding ITSFEA] appear[] extremely well-constructed to establish the validity of the misappropriation theory and rule 14e-3").

183. *See* Reconciliation Draft of Insider Trading Proscriptions Act of 1987, S. 1380, *reprinted in The Insider Trading Proscriptions Act of 1987: Hearings Before the Subcomm. on Securities of the Senate Comm. on Banking, Housing and Urban Affairs*, 100th Cong., lst Sess. 28–30 (1987).

There were several bills attempting to define insider trading that were considered in the 1987–88 period which eventually led to the passage of ITSFEA. All of them focused on the "wrongful" obtaining of information and all defined theft and similar acts as "wrongful." *See generally* Robert D. Rosenbaum & Stephen M. Bainbridge, *The Corporate Takeover Game and Recent Legislative Attempts to Define Insider Trading*, 26 AM. CRIM. L. REV. 229, 233–34 (1988) (summarizing various approaches).

184. *See* H.R. REP. NO. 100-910, at 8 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6048. The problem was not that Congress thought the proposed definition was too broad, but that it "might be under-inclusive and constitute what many have called a 'roadmap for fraud.'" Stuart J. Kaswell, *An Insider's View of the Insider Trading and Securities Fraud Enforcement Act of 1988*, 45 BUS. LAW. 145, 150 (1989); *see also* Stephen Bainbridge, Note, *A Critique of the Insider Trading Sanctions Act of 1984*, 71 VA. L. REV. 457, 473 (1985) (noting that Congress omitted statutory definition of insider trading when passing ITSA because any statutory definition might contain holes "large enough to drive a truck through"); Karmel, *Outsider Trading*, *supra* note 135, at 100 (noting that definition of insider trading that included espionage through electronic or other means was deleted by Congress on grounds "that a statutory definition could have a potentially narrowing effect").

information leads to dissonant results by letting morally blameworthy thieves of information off the hook, relatively speaking.[185] Such a theory similarly fails to protect the integrity of the market against outsiders who trade on the basis of material, nonpublic information. The source of the information can consent to the trading and thereby absolve the trader from liability, even though damage is done to the market at large.[186] Furthermore, a fiduciary can trade even without her principal's permission if she discloses the trade.[187] Thus, a narrow view of the misappropriation theory is underinclusive.[188]

---

185. Such a theory absolves hackers and thieves of insider trading liability. Even though they face other penalties, those alternative penalties may be relatively light. A hacker who traded on stolen information to the tune of $1 million in profit could face insider trading penalties of (1) disgorgement of the $1 million, (2) a civil fine of up to $3 million, (3) a criminal fine of up to $1 million, *and* (4) up to 10 years in jail. *See* 15 U.S.C. §§ 78u-1(a)(2), 78ff(a) (1994). By comparison, the maximum criminal penalty for mail fraud is only five years in jail and/or a more modest fine, unless the "violation affects a financial institution," in which case much more severe penalties (fine up to $1 million and/or jail sentence up to 30 years) apply. 18 U.S.C. § 1341 (1994). Of course, given the multiple theories that will often apply and the indeterminacies of the federal sentencing guidelines, *see, e.g.*, Jeffrey Standen, *Plea Bargaining in the Shadow of the Guidelines*, 81 CAL. L. REV. 1471, 1506–08 (1993), it is difficult to generalize about punishments for wrongdoing. However, hackers who misappropriate nonpublic information and trade for a profit should be punished as inside traders because insider trading is the essence of their wrong, and an insider trading charge stacked on top of other potential charges (such as mail and wire fraud, extortion, or blackmail) is more likely to lead to an appropriate punishment than if those other charges stand alone.

186. *See* Painter et al., *supra* note 156, at 179; David M. Zornow & Keith D. Krakaur, *Insider Trading After 'O'Hagan': Questions Remain About Scope of Conduct Falling Within Misappropriation Theory*, N.Y. L.J., Feb. 2, 1998, at 7. An unsettling example of such trading involved a scientist conducting clinical trials of a medical product. He received the permission of his employer to purchase the stock of the company that made the tested product before the public announcement of the positive results of the test. *See* Kathleen Day, *Cold Researcher Made Profit on Quigley Shares: Stock Soared After Release of Study Favorable to Lozenges*, WASH. POST, Jan. 31, 1997, at G1; Philip J. Hilts, *Researcher Made Profit After Study*, N.Y. TIMES, Feb. 1, 1997, at 6. For an article critical of medical ethics in this area, see Prentice, *Clinical Trial*, *supra* note 16.

Even before *O'Hagan*, many commentators recognized the defense of consent as a potential weakness in the misappropriation theory. *See, e.g.*, Dennis S. Karjala, *Federalism, Full Disclosure, and the National Markets in the Interpretation of Federal Securities Law*, 80 NW. U. L. REV. 1473, 1521–22 (1986); Mark A. Clayton, Comment, *The Misappropriation Theory in Light of* Carpenter *and the Insider Trading and Securities Fraud Enforcement Act of 1988*, 17 PEPP. L. REV. 185, 212 (1989).

187. *See* Painter et al., *supra* note 156, at 180.

188. For an analysis of other gaps in insider trading law, see Steven R. Salbu, *Tipper Credibility, Noninformational Tippee Trading, and Abstention from Trading: An Analysis of Gaps in the Insider Trading Laws*, 68 WASH. L. REV. 307 (1993).

Philosophically, it is more satisfying to include theft via hacking and other means as insider trading when *trading* is the sole purpose of the theft. There are two major philosophical approaches to examining the ethics of insider trading. First, there is the teleological/utilitarian approach, which tends to reduce to a debate over efficiency versus fairness.[189] This Article has too much ground to cover to review the long debate over the merits of insider trading regulation.[190] It is clear that Congress, in passing ITSA and ITSFEA, has taken the position that the intrinsic unfairness of insider trading justifies its regulation. The more unfair the activity, the more justification there is for regulation. Second, there is the deontological, rule-based approach. Certainly a regime which condemns theft of inside information for the purpose of trading on that information is more consonant with our basic rule-based concepts of morality (e.g., "Thou shalt not steal") than one that does not. Even property-rights theorists should not disapprove of this broad view of the misappropriation theory because "[p]roperty rights theorists, whether of a Lockean or social-efficiency bent, have a means of identifying at least one major class of transaction deserving of moral disapproval: trading on stolen goods."[191]

---

189. *See* David A. Wilson, Note and Comment, *Outsider Trading—Morality and the Law of Securities Fraud*, 77 GEO. L.J. 181, 195–98 (1988) (discussing various approaches to gauging morality of insider trading).

190. Similarly, this Article will not consider the "efficiency" of insider trading, except to make the blanket but deeply believed statement that any claim that insider trading is an efficient means of compensating corporate insiders is silly. Indeed, a recent study indicates that the market believes that securities fraud remedies (not just insider trading remedies in particular) as they currently stand are efficient. *See* Ashiq Ali & Sanjay Kallapur, *Shareholders' Perception of the Securities Litigation Regime in the United States: Stock Price Impact of the Presidential Veto of the Private Securities Litigation Reform Bill of 1995* (1998), *available at* <http://www.ssrn.com/papers/9802/98022602.pdf> (finding evidence that market believed that Private Securities Litigation Reform Bill, by cutting back on plaintiffs' ability to sue, would reduce deterrent effects of securities litigation and weaken financial disclosure system).

191. Gary Lawson, *The Ethics of Insider Trading*, 11 HARV. J.L. & PUB. POL'Y 727, 783 (1988). In criticizing Lawson's article, Professor Macey argues that "the attempt to critique insider trading using ethical philosophy — divorced from economic analysis — is something of a non-starter, because ethical analysis does not have much to add to the work that has already been done by economists." Jonathan R. Macey, Comment, *Ethics, Economics, and Insider Trading: Ayn Rand Meets the Theory of the Firm*, 11 HARV. J.L. & PUB. POL'Y 785, 786 (1988) (replying to Lawson's article). Macey goes on to argue that "[i]t is clear that lying and stealing are wrong, but it's not clear that insider trading is synonymous with these practices. In some cases it may be, but in others clearly it is not." *Id.* at 802. Presumably, even Professor Macey would support prohibiting insider trading by hackers, because that activity clearly involves stealing.

It has been argued that theft via hacking would not satisfy the deception requirement of a Rule 10b-5 violation.[192] However, if the hacker avoids detection and then fails to disclose the information but trades on it instead, there is at least as much "deception" as exists in a misappropriation case as envisioned by Justice Ginsburg in *O'Hagan*. The misappropriation theory has been similarly criticized as based more on a nondeceptive state law breach of fiduciary duty than on the type of deception that typifies a Section 10(b)/Rule 10b-5 violation.[193] However, Justice Ginsburg in *O'Hagan* found sufficient deception in the misappropriator's "feigning fidelity to the source of the information . . . ."[194] Unless the hacker advertises the stolen information before trading on it, which would defeat the purpose of her crime, the hacker is similarly deceiving market participants who do not know of her theft of the inside information.[195]

David Phillips has also made an ethical case against insider trading in general and most certainly against insider trading in the hacking situation, based on the ethical imperative of reciprocal treatment ("Do Unto Others"). He notes that "if the party with the inside information has unlawfully gained access to that information, the other investor's expectations [of fair reciprocal treatment] have been violated because he simply would not expect the other party's access or use of the information." David M. Phillips, *An Essay: Six Competing Currents of Rule 10b-5 Jurisprudence*, 21 IND. L. REV. 625, 636 n.61 (1988).

192. *See* Manning Gilbert Warren III, *Who's Suing Who? A Commentary on Investment Bankers and the Misappropriation Theory*, 46 MD. L. REV. 1222, 1239–40 (1987).

> While it is true that theft may be accomplished by deception, it is also true that not all theft is deceptive. If the theft [by an employee, say, of an investment bank hired by a takeover artist] were fully disclosed to [both the takeover firm and the investment bank] . . . , it is difficult to pinpoint the deception. If [the employee] had stolen [a target firm's] securities from [the investment bank and the takeover firm] in an armed robbery, criminal theft would have occurred but not the deceptive conduct proscribed by [S]ection 10(b).

Id.

193. *See* Jill E. Fisch, *Start Making Sense: An Analysis and Proposal for Insider Trading Regulation*, 26 GA. L. REV. 179, 204 (1991) ("Although it may be wrong to violate a relationship of trust and confidence by breaching an employer confidentiality policy . . . these wrongs are not fraudulent or deceptive."); Warren, *supra* note 192, at 1248.

194. United States v. O'Hagan, 521 U.S. 642, 655 (1997).

195. Although the essence of a misappropriation claim is that the defendant breached a fiduciary duty to the source of the information, even if a hacker breaches no such duty, there are sufficient elements of deception to satisfy the requirements of Section 10(b): (1) not disclosing to the source of the information that it is being stolen, (2) not disclosing to the opposite party in the trading transaction that material, nonpublic

Finally, it should be noted that hacking meets the "in connection with" requirement[196] of Section 10(b). It is obviously a stretch to frame the robbery of money from a bank and subsequent use of the funds for securities trading as a securities law violation,[197] but stealing information that can be of use to the thief only if the thief trades securities on the basis of the information, or sells the information to others who plan on doing so, is another matter. The latter offense is tied inextricably to the securities laws, satisfying the "in connection with" requirement. Thus, a hacker who steals inside information for the purpose of trading on it commits an insider trading violation.

IV. WHAT LIABILITY MIGHT ISPS HAVE FOR INSIDER TRADING INVOLVING THE INTERNET?

A. Theft by Hackers

1. The Problem

Firms worried about intrusion through the Internet by hackers may well access the Internet via an Internet Service Provider ("ISP"),[198] because the risk of being invaded by hackers is less for such firms than for firms whose computers access the Internet directly.[199] Nonetheless,

---

information is being used, and (3) not disclosing to the marketplace the use of material information but not abstaining either.

196. *See generally* WANG & STEINBERG, *supra* note 18, § 4.5 (discussing "in connection with" requirement in insider trading cases).

197. *See O'Hagan*, 521 U.S. at 656 ("The misappropriation theory would not . . . apply to a case in which a person defrauded a bank into giving him a loan or embezzled cash from another, and then used the proceeds of the misdeed to purchase securities." (alteration in original) (internal quotation marks omitted) (quoting Government's brief)).

Notwithstanding this limiting statement, Justice Ginsburg's holding clearly rejects the narrow view of the Fourth Circuit in *United States v. Bryan*, 58 F.3d 933, 949–50 (4th Cir. 1995), that the "in connection with" requirement could not be met in a misappropriation case. Earlier cases from other circuits holding to the contrary have a better argument. *See, e.g.*, SEC v. Clark, 915 F.2d 439, 449 (9th Cir. 1990); United States v. Newman, 664 F.2d 12, 18 (2d Cir. 1981), *aff'd after remand*, 722 F.2d 729 (2d Cir. 1983).

198. This Article uses the term "Internet Service Provider" to cover both "Internet Access Providers" and "Online Service Providers."

199. *See* Rustad & Eisenschmidt, *supra* note 141, at 220.

ISPs are also vulnerable to hacking[200] and may be used as portals for entry by hackers into the ISP's clients' computers.[201]

Assume that a hacker breaks into XYZ Company's computer, entering via XYZ's ISP. Assume further that the hacker steals inside information about an upcoming takeover and trades on that information in such volume that the target's stock price rises. Instead of buying the target for $13.3 billion as originally planned, XYZ must pay $14.3 billion.[202] Finally, assume that XYZ can plausibly argue that the ISP's security procedures were inadequate. Can XYZ recover from the ISP the extra $1 billion it paid to purchase the target?

Takeover firms such as XYZ have already filed similar damage actions against the actual traders who were engaged in insider trading.[203] Although these lawsuits have produced mixed results,[204] they do provide

---

200. *See, e.g.*, Kenneth Li, *They're Hacking Away at the Net*, N.Y. DAILY NEWS, Mar. 15, 1998, at 50 (noting reports that America Online alone had suffered 28 documented security breaches in previous 10 months); Sandberg, *Hackers*, *supra* note 140, at B1 (describing successful hacker attacks against America Online).

201. *See* Rustad & Eisenschmidt, *supra* note 141, at 221 ("The ISP's server computer is 'on' the Internet twenty-four hours a day. Any computer 'on' the Internet may be potentially 'hacked into' from elsewhere on the Internet . . . ."); Deborah Radcliff, *Enterprise Computing: Is Your ISP Secure? As Web Sites Proliferate, Companies Hosting Sensitive Information Should Inquire About an ISP's Security*, INFOWORLD, Mar. 2, 1998, at 97 ("If your company stores any valuable information on your Web servers and those servers are housed at an ISP or Web hosting center, you should pay close attention to your ISP's security policy.").

202. This number is extremely plausible, for a recent study shows that takeovers accompanied by illegal insider trading typically involve premiums of 43% versus only 33% premiums for takeovers unaccompanied by illicit trading. *See* Gene Koretz, *The Injury from Insider Trading*, BUS. WK., Nov. 24, 1997, at 32 (citing study in *European Finance Review* by Lisa K. Meulbroek and Carolyn Hart).

203. *See, e.g.*, *In re* Ivan F. Boesky Sec. Litig., 36 F.3d 255 (2d Cir. 1994) (suit by would-be suitor against its investment banker); Litton Indus., Inc. v. Lehman Bros. Kuhn Loeb, Inc., 967 F.2d 742 (2d Cir. 1992) (suit by corporate raider against its investment bank, individual traders, and their tippees); SEC v. Marcus Schloss & Co., 714 F. Supp. 100 (S.D.N.Y. 1989). *See generally* Ralph C. Ferrara & Robert K. Gordon, *Inside Traders Face Wave of Litigation*, NAT'L L.J., Sept. 19, 1988, at 25 (summarizing proceedings against traders).

204. In *Litton*, plaintiff Litton claimed, essentially, that it retained investment bank Lehman Brothers Kuhn Loeb to assist it in acquiring Itek Corporation. However, employees of Lehman passed the information on to famed inside trader Dennis Levine who began buying large amounts of Itek stock. Others tipped by Levine or piggybacking on his trades also helped raise the price of Itek stock, thereby boosting the premium Litton ultimately had to pay to complete the takeover. The Second Circuit overturned the trial court's summary judgment ruling that the increased market price had not affected the premium that Litton paid, *see* 967 F.2d at 748–51, paving the way for settlement of the case.

plausible precedent for a lawsuit against hackers who stole the information and traded it, or against any tippees to whom the hackers sold or otherwise conveyed the information.

But the ISP did not engage in insider trading. The question presented by the hypothetical factual scenario is whether the ISP can be liable for the damage done by the hacker's trading. Most of the attention regarding ISP liability thus far has focused on matters of pornography,[205] defamation,[206] and copyright,[207] but answering this particular question

---

Two other cases resulted in substantial settlements for injured tender offerors. In *Kidder, Peabody & Co. v. Maxus Energy Corp.*, 925 F.2d 556 (2d Cir. 1991), Ivan Boesky was involved in insider trading which jacked up the market price of Natomas Company to the detriment of Maxus Energy's predecessor corporation, Diamond Shamrock Corporation. Kidder, Peabody settled the case for $165 million. *See Litigation: Big Suits*, AM. LAW., Dec. 1992, at 70 (reporting settlement). And in *Anheuser-Busch Cos. v. Thayer*, No. CA3-85-0794-R (N.D. Tex. filed Apr. 26, 1985), *cited in* J. Robert Brown, Jr., *Corporate Secrecy, the Federal Securities Laws, and the Disclosure of Ongoing Negotiations*, 36 CATH. U. L. REV 93, 145 n.197 (1986), a director of Anheuser-Busch paid $600,000 to settle a suit claiming that his tips to others had raised the market price of a firm, Campbell Taggart, Inc., that Anheuser-Busch was trying to acquire.

On the other hand, in *In re Boesky*, FMC Corporation was looking to restructure itself with a view toward becoming a less attractive takeover target. *See* 36 F.3d at 257. After consultation with the investment bank Goldman Sachs, FMC decided to reorganize in such a manner as to place a higher percentage of shares in the hands of management shareholders. In the planned reorganization, more cash would go to public shareholders and more shares would go to management shareholders. An employee of Goldman Sachs tipped confidential information about the deal to Ivan Boesky whose trading boosted FMC's market price, *see id.* at 258, leading Goldman Sachs to suggest to FMC that it boost the planned payments to public shareholders by $10 per share to ensure that the deal go through. FMC agreed, paying $220 million more than originally planned to repurchase the shares from public shareholders. *See id.* at 259. FMC sued Goldman Sachs, but lost, in part, because the court noted that the overpayment went to FMC's own (public) shareholders. "[B]ecause the excess amounts inured to the benefit of FMC's shareholders, FMC cannot claim that it was injured thereby." *Id.* at 261.

205. *See generally* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51 (1996) (discussing liability of ISPs and others for pornography after passage of Communications Decency Act, which was later declared unconstitutional in part); Sean Adam Shiff, Comment, *The Good, the Bad and the Ugly: Criminal Liability for Obscene and Indecent Speech on the Internet*, 22 WM. MITCHELL L. REV. 731 (1996) (discussing liability of ISPs and others for obscenity).

206. *See generally* Douglas B. Luftman, Note, *Defamation Liability for On-line Services: The Sky is Not Falling*, 65 GEO. WASH. L. REV. 1071 (1997).

207. *See, e.g.*, INFORMATION INFRASTRUCTURE TASK FORCE, U.S. DEP'T OF COMMERCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (1995), *available at* <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>

involves examining the elements of common law negligence.[208] Any answers are necessarily tentative, for there currently is no clear body of law regarding ISP liability.[209]

2. Elements of Common Law Negligence Examined

Prosser and Keeton spells out the most accepted formulation of the four elements of a common law negligence cause of action that might be pursued by a takeover firm against an ISP.[210] Each deserves individual analysis, however brief.

a. Existence of a Duty

Do ISPs owe a duty of due care to their subscribers? Almost certainly they do. Under the precepts of common law negligence, each actor owes a duty of care to the foreseeable victims of the actor's

---

(discussing ISP copyright infringement liability); Patrick J. Glynn, *Cyber Copyrights: Internet Provider Liability*, 60 TEX. B.J. 634 (1997) (same).

208. Epstein and Tancer note that "[f]rom what little law exists, and in the absence of legislative solutions, it appears as if jurists will attempt to apply 'off-line' legal concepts to online torts . . . ." Keith J. Epstein & Bill Tancer, *Enforcement of Use Limitations by Internet Services Providers: "How to Stop that Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber,"* 19 HAST. COMM. & ENT. L.J. 661, 671 (1997).

Rustad and Eisenschmidt, in discussing ISP tort liability, *see supra* note 141, at 244, note that section 6 of the Restatement (Second) of Torts provides that any invasion of a legally protected interest should be compensable under tort law, whether the claim is based on negligence, strict liability, or intentional misconduct. The most plausible claim by a client against an ISP would appear to be based on negligence: strict products liability does not appear to apply because the ISP provides a service rather than a good, *see, e.g.*, Dennis v. Allison, 698 S.W.2d 94 (Tex. 1985) (holding that implied warranty not available to doctor's patient injured by improper treatment), and it is extremely unlikely that any ISP would *intentionally* facilitate a hacker's invasion into a client's computers.

209. *See* Epstein & Tancer, *supra* note 208, at 663 (noting that in absence of clear body of law, ISPs will be forced to resort to self-help to minimize Internet abuses).

210. The elements of a negligence cause of action are:

> 1. A duty, or obligation, recognized by the law, requiring the person to conform to a certain standard of conduct, for the protection of others against unreasonable risks.
> 2. A failure on the person's part to conform to the standard required . . . .
> 3. A reasonably close causal connection between the conduct and the resulting injury . . . .
> 4. Actual loss or damage resulting to the interests of another.

W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 30, at 164–65 (5th ed. 1984) [hereinafter PROSSER AND KEETON] (footnotes omitted).

carelessness.[211] Commentators believe that ISPs should be held liable to customers whose data they carelessly lose or damage,[212] as well as to customers damaged by an ISP's careless failure to anticipate technical problems and provide backup.[213] Lawsuits have already been filed against ISPs for carelessly failing to correct inaccurate data that they transmitted to the detriment of third parties.[214] To the extent that their logic obtains, these lawsuits provide support for imposing liability on ISPs for carelessly allowing security breaches.[215]

b. Breach of the Duty

In determining whether the ISP has breached its duty of care, a court must establish an appropriate standard of care. Absent the adoption of a legislative standard addressing due care,[216] the courts will have to

---

211. *See* RESTATEMENT (SECOND) OF TORTS § 281 (1965).

212. *See* HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY § 4.8, at 173 (1996); Allen S. Hammond, *Private Networks, Public Speech: Constitutional Speech Dimensions of Access to Private Networks*, 55 U. PITT. L. REV. 1085, 1136 (1996) ("[S]hould the network owner lose or damage customer information in storage, manipulation or transmission of customer information entrusted to its care, it is reasonable to require that the owner compensate the customer to the extent of its legally recognized tort damages.").

213. *See* JONATHAN ROSENOER, CYBERLAW: THE LAW OF THE INTERNET 163 (1996).

214. America Online ("AOL") was reporting the share price of software firm Ben Ezra, Weinstein, Inc. at $0.17 when it was really $1.84. Such a misreporting can cause investors to panic. When the misreporting persisted for two days, the firm sued AOL for carelessly failing to correct the error. AOL's defense was predicated, in part, upon the arguments that (1) the information was transmitted from a provider, S&P Comstock, and went unedited and untouched into AOL's system, and (2) AOL runs a disclaimer to investors warning them to double-check stock quotes. *See generally AOL Sued for Allegedly Erroneous Information*, CYBERSPACE LAW., Apr. 1997, at 32; Kimberly Weisul, *Quote Vendor Glitches Create Lawsuit Headaches for AOL: On-line Investors React Swiftly to Inaccurate Stock Quotes*, INV. DEALERS' DIG., Mar. 31, 1997, at 19.

215. Although it may be a close call, it appears that such carelessness would constitute a basis for a negligence lawsuit and not simply a breach of contract action. For example, in *Southwestern Bell Tel. Co. v. DeLanney*, 809 S.W.2d 493 (Tex. 1991), the court held that the defendant phone company's failure to print the plaintiff's yellow-pages advertisement was simply a breach of contract. The majority, over a strong dissent, reversed a negligence judgment and held that the plaintiff's only remedy was breach of contract. *See id.* at 495. However, the ISP hypothetical is different because the plaintiff claims more than a simple failure to perform on the part of the defendant. *See* PROSSER AND KEETON, *supra* note 210, § 92, at 656. Still, it is arguable that the "economic loss doctrine," where recognized, might bar such a lawsuit in negligence and relegate the plaintiff to a breach of contract claim. *See infra* notes 230–37 and accompanying text.

216. Rustad and Eisenschmidt have speculated about the legislative adoption of a

invoke common law standards. The appropriate standard is that of the reasonably careful ISP. Evidence that the defendant ISP did not have some of the security measures typically found in the industry would certainly be evidence of a breach of the duty of due care.[217] Conversely, evidence that the defendant *did* have the same level of security measures as other ISPs raises the inference that the defendant did act with due care.[218] Current industry custom includes such security devices as firewalls,[219] routers, switches at each port of the ISP, filtering, intrusion detection software, and, perhaps, encryption.[220] There is substantial evidence that many ISPs are not meeting industry custom: some large ISPs say they are providing security but are actually not, and many small ISPs cannot afford the more sophisticated filtering switches and other security devices.[221]

Furthermore, although meeting industry custom raises the inference of due care, it is not *conclusive* on the issue of liability.[222] Learned Hand

---

related standard:

> The National Computer Security Center of the [National Security Agency] administers the process for C2 certification of computer security. Assuming that a federal certificate of authority were widely adopted, an Internet security firm that, for example, failed to obtain necessary "trusted certificate" authority for validating digital signatures might be found negligent per se for any loss resulting from such failure.

Rustad & Eisenschmidt, *supra* note 141, at 251 (footnotes omitted). Of course, no such federal standard currently exists.

217. *See* William Laurie Co. v. McCullough, 90 N.E. 1014, 1017 (Ind. 1910); Roberts v. Indiana Gas & Water Co., 221 N.E.2d 693, 694–95 (Ind. Ct. App. 1966).

218. *See* King v. National Spa & Pool Inst., 570 So.2d 612, 616 (Ala. 1990) (stating that conformance with professional standards is indicative, but not conclusive, of due care); Advincula v. United Blood Servs., 678 N.E.2d 1009, 1027 (Ill. 1996) (same); Cerretti v. Flint Hills Rural Elec. Coop. Ass'n, 837 P.2d 330, 336 (Kan. 1992) (same).

219. *See* Hodkowski, *supra* note 10, at 223–224:

> A network-level firewall, or packet filter, examines data traffic as it attempts to pass between the local network and the Internet. It filters out the packets that are coming from an "unsecure" machine (most likely a computer that is not owned by the company or not authorized to have access to the local network).

Id. (footnotes omitted).

220. *See* Radcliff, *supra* note 201, at 97 (describing these various devices and what they do).

221. *See id.*

222. *See* Doe v. American Nat'l, 848 F. Supp. 1228, 1233 (S.D.W.Va. 1994); Hanover Ins. Co. v. Brotherhood State Bank, 482 F. Supp. 501, 506 (D. Kan. 1979); Grisham v. Transamerica Ins. Group, 1977 U.S. Dist. LEXIS 16962, at *8 (D. Idaho Mar. 10, 1977) ("[I]t has become hornbook law that the custom and practices of an industry, while relevant to the question of negligence, are not conclusive."); Northern

wrote in *The T.J. Hooper*,[223] a case involving radio sets for ocean-going tugs, that "a whole calling may have unduly lagged in the adoption of new and available devices."[224] Thus, if a plaintiff can demonstrate that security devices were available and effective, the breach of duty element can be established notwithstanding the fact that the defendant ISP's failure to adopt the new devices conformed to industry custom.[225] Given the rapid pace of technological evolution in this area, difficult questions will likely arise regarding the relative presence or absence of care in the adoption of technological breakthroughs.

Another aspect of the duty of care is the well-known rule that an actor may raise its duty of care by voluntarily assuming a higher standard. For example, if an ISP advertised that customers should subscribe to it because of its superior security devices and procedures, that ISP has automatically raised its legal duty of care above the industry norm.[226]

c. Proximate Causation

Causation is a key element of negligence recovery[227] and may be a problem in this context. Although as noted earlier there have been recoveries in similar cases, some plaintiffs have been derailed by the causation requirement. For example, in *SEC v. Marcus Schloss*,[228] the occurrence of too many other events — including the public announcement of the inside information and the launching of three other competing tender offer bids — prevented the plaintiff takeover artist from proving that the defendant's illicit insider trading had caused the price to rise.[229] If issuers cannot prove that the higher acquisition prices they paid were proximately caused by the illicit insider trading, then they cannot prove that their losses were caused by the negligence of the ISP whose security lapses allowed the insider trading to occur.

Lights Motel, Inc. v. Sweaney, 561 P.2d 1176, 1191–92 (Alaska 1977).

223. 60 F.2d 737 (2d Cir. 1932).

224. *Id.* at 740.

225. *See* PROSSER AND KEETON, *supra* note 210, § 33, at 193–95 ("Even an entire industry, by adopting such careless methods to save time, effort, or money, cannot be permitted to set its own uncontrolled standard.").

226. *See* RESTATEMENT (SECOND) OF TORTS § 299A (1965) (providing that one who represents that she has greater skill or knowledge than others in her profession may be held to higher standard of care).

227. *See, e.g.*, Davis v. Bell, 705 So.2d 108, 109 (Fla. Dist. Ct. App. 1998); *In re* Estate of Brandecker, 963 S.W.2d 461, 465 (Mo. Ct. App. 1998).

228. 714 F. Supp. 100 (S.D.N.Y. 1989).

229. *See id.* at 102–03.

d. Damages

It is the damages element that will present the biggest roadblock to recovery from ISPs for issuers whose confidential information was stolen by hackers due to the ISPs' negligence. Many jurisdictions follow the rule that a negligence theory cannot be the basis for a recovery of only monetary damages. Rather, these jurisdictions hold, negligence liability is primarily an avenue of recovery for personal injuries, absent a special relationship between the defendant and the plaintiff. Although the trend seems to be toward scrapping this barrier to recovery known as the Economic Loss Doctrine ("ELD"),[230] in perhaps a majority of jurisdictions, plaintiffs will not be able to recover from ISPs absent proof of a special relationship.

Modern commentators have generally criticized the ELD,[231] and many jurisdictions follow a more modern trend. For example, in *Congregation of the Passion v. Touche Ross*,[232] the Illinois Supreme Court held that the economic loss doctrine should apply "only where the duty of the party performing the service is defined by the contract that he executes with his client. Where a duty arises outside of the contract, the economic loss doctrine does not prohibit recovery in tort for the negligent breach of that duty."[233] Numerous exceptions have been

---

230. The ELD traces from Justice Traynor's opinion in *Seely v. White Motor Co.*, 403 P.2d 145 (Cal. 1965). Fearful that the rapidly expanding tort law of products liability would completely swallow contract law unless checked, the court held that to preserve the law of warranty, no tort liability should be allowed in cases where a defective product caused purely economic loss. *See id.* at 150.

231. *See, e.g.*, Amanda K. Esquibel, *The Economic Loss Rule and Fiduciary Duty Claims: Nothing Stricter than the Morals of the Marketplace?*, 42 VILL. L. REV. 789 (1997) (criticizing ELD's application in arena of breach of fiduciary duty claims); Paul J. Schwiep, *The Economic Loss Rule Outbreak: The Monster that Ate Commercial Torts*, 69 FLA. B.J. 34 (1995) (criticizing ELD's broad application); Kelly M. Hnatt, Note, *Purely Economic Loss: A Standard for Recovery*, 73 IOWA L. REV. 1181 (1988) (arguing for imposition of severe limitations on ELD); Raul Jauregui, Comment, *Rembrandt Portraits: Economic Negligence in Art Attribution*, 44 UCLA L. REV. 1947 (1997) (criticizing ELD in context of negligence by art dealers); William Way, Note, *The Problem of Economic Damages: Reconceptualizing the* Moorman *Doctrine*, 1991 U. ILL. L. REV. 1169 (1991) (criticizing ELD in context of malpractice actions). *But see* Edward T. O'Donnell et al., *On the Differences Between Blood and Red Ink: A Second Look at the Policy Arguments for the Abrogation of the Economic Loss Rule in Consumer Litigation*, 19 NOVA L. REV. 923 (1995) (evaluating arguments on both sides and generally defending ELD).

232. 636 N.E.2d 503 (Ill. 1994).

233. *Id.* at 514; *see also* J'Aire Corp. v. Gregory, 598 P.2d 60, 61 (Cal. 1979) (allowing negligence recovery even for losses to prospective economic advantage).

developed to the ELD,[234] and the hypothetical situation above is similar to some of those exceptions.[235] Thus, in jurisdictions that do not still embrace the strictest versions of the ELD, a plaintiff might recover in negligence if its contract with the ISP does not directly address this security issue. If the contract *does* address the issue, then plaintiffs may well have a legitimate breach of contract suit.[236] Under either theory, however, $1 billion in relatively unforeseeable damages might provide a court with a strong motivation to block recovery on the basis of either the ELD in a negligence suit, or the unforeseeability doctrine of *Hadley v. Baxendale*[237] in a contract action.

3. Defenses

a. Comparative Negligence

Any firm that files a negligence suit against its ISP is certainly subject to a comparative negligence defense,[238] for a hacker using an ISP's facilities to invade the ISP's client's computers must also overcome the client's security defenses.[239] A firm without firewalls,[240]

---

234. *See* Hnatt, *supra* note 231, at 1194–1201.

235. *See, e.g.*, Western Union Tel. Co. v. Mathis, 110 So. 399, 401–02 (Ala. 1926) (holding telegraph company liable when its negligent transmission caused plaintiff to lose contract).

236. The scope of compensatory damages in breach of contract suits is limited by reasonable foreseeability as spelled out in *Hadley v. Baxendale*, 156 Eng. Rep. 145 (1854). *See generally* JOHN D. CALAMARI & JOSEPH M. PERILLO, CONTRACTS § 14.5, at 546 (4th ed. 1998). Given the widespread problem of insider trading and the well-known price effects that it can have in takeover cases, it is certainly arguable that the foreseeability requirement is met. On the other hand, defendant ISPs might reasonably claim that they did not know of the planned takeover (such matters usually being kept top secret) and therefore could not have reasonably foreseen such tremendous damages flowing from a careless failure to provide adequate security.

237. 156 Eng. Rep. 145 (1854), discussed *supra* note 236.

238. Only a few states still adhere to the traditional contributory negligence system in which a plaintiff's carelessness that contributes to her own injuries, no matter how small the contribution, will totally bar her recovery. Most states have adopted comparative negligence or comparative fault regimes ranging from "pure" systems in which a plaintiff's 99% fault would still allow her to recover 1% of her damages from a careless defendant, to less pure systems that typically allow a plaintiff proportional recovery up to and including situations where she is 49% or 50% at fault but bar recovery totally if the plaintiff's contributory fault is 50% or 51%. *See generally* PROSSER AND KEETON, *supra* note 210, § 67.

239. Because "[t]he subscriber shares in the obligation to protect his or her account from access by unauthorized persons," experts suggest that ISPs provide in their contracts with subscribers that subscribers be prohibited from attempting to break into

proxy servers, or other well-planned and effectively-implemented security procedures is contributing to its own losses, and its recovery may be reduced accordingly, if not barred altogether.[241]

b. Communications Decency Act

Any ISP sued on the negligence theory articulated above might try to raise the Communications Decency Act ("CDA") in defense.[242] In *Zeran v. America Online, Inc.*,[243] the plaintiff claimed that America Online ("AOL") had carelessly failed immediately to remove, retract, and screen defamatory messages posted by an unknown user.[244] However, the Fourth Circuit held that the CDA preempted the plaintiff's negligence claim.[245] There are some obvious parallels between *Zeran* and the insider trading hacker scenario. In *Zeran*, the plaintiff claimed that AOL was careless in not removing a third party's message from its server; in the insider trading case, the plaintiff is claiming that the ISP is careless in not preventing a third party from accessing the plaintiff's computer system. However, neither the language nor the purpose of the CDA will protect an ISP in the insider trading scenario.

The relevant provision of the CDA, § 230, states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information

---

the accounts of other subscribers, and subscribers acknowledge their obligation to safeguard their accounts against unauthorized access. Epstein & Tancer, *supra* note 208, at 681.

240. *See generally* D. BRENT CHAPMAN & ELIZABETH D. ZWICKY, BUILDING INTERNET FIREWALLS (1995); WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER (1994); Marius Nacht, *The Spectrum of Modern Firewalls*, 16 COMPUTERS & SECURITY 54 (1997) (describing fundamental features and requirements of Internet and intranet firewalls); John Herron, *Law Firms Can Reduce Internet Security Risks*, NAT'L L.J., Mar. 25, 1996, at C6 (describing various Internet security devices).

241. Indeed, some believe that hacking is often caused by careless subscribers who leave passwords lying around or are too lazy to change them regularly. *See* Epstein & Tancer, *supra* note 208, at 81.

242. *See* 47 U.S.C. § 230 (Supp. II 1996).

243. 129 F.3d 327 (4th Cir. 1997).

244. In *Zeran*, an unknown party posted a message on AOL that made it appear that plaintiff Zeran was selling tasteless T-shirts and other items related to the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. The posting was so sleazy that Zeran received many harassing, derogatory, and threatening phone calls from persons who had seen it. *See id.* at 329.

245. *See id.* at 330–31; *see also* Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998) (citing *Zeran* in using CDA to dismiss high-profile claim against AOL).

content provider."[246] The plaintiff in the insider trading scenario is not suing the ISP on grounds that it was the speaker of any information. Therefore, the First Amendment concerns that might be relevant in *Zeran* are irrelevant to the insider trading claim. Additionally, the two main purposes of this portion of the CDA were (1) to encourage free online speech by shielding ISPs from liability and therefore removing their incentive to unduly censor online communications, and (2) to encourage ISPs to censor materials without worrying about being held liable to the strict liability standards usually applied to publishers.[247] Neither of those concerns is relevant to the insider trading scenario.[248]

B. Theft by ISP Employees

Another scenario that has been envisioned is theft of confidential information and subsequent insider trading by an employee of an ISP.[249] Assume that the hacker who broke into the corporation's computers to steal inside information via the ISP was an employee of the ISP. The inquiry now changes slightly.

1. The ISP Hacker's Liability

Numerous cases, including three in the Supreme Court, have involved employee theft of information and claims of misappropriation.[250] Twice the Supreme Court failed to determine the employee's liability,[251] but in *O'Hagan*, the Court clearly embraced the misappropriation theory.[252] Thus, an ISP employer/hacker who steals information from one of her ISP's subscribers breaches a fiduciary duty owed to her employer and, in turn, a duty owed to the subscriber.

---

246. 47 U.S.C. § 230(c)(1) (Supp. II 1996).

247. *See Zeran*, 129 F.3d at 331.

248. *See generally* Blake A. Bell, *E-Broker Chat Rooms and Federal Securities Laws*, WALLSTREETLAWYER.COM, Aug. 1998, at 1 (discussing CDA's potential application to electronic brokers who set up "e-broker chat rooms").

249. *See* Wolowitz & Diana, *supra* note 6, at B12.

250. *See, e.g.*, United States v. Libera, 989 F.2d 596 (2d Cir. 1993) (employee of financial printer purloined advance copies of *Business Week*); SEC v. Cherif, 933 F.2d 403 (7th Cir. 1991) (former employee pierced bank's security to steal clients' secrets).

251. *See* Carpenter v. United States, 484 U.S. 19 (1987) (splitting 4-4 on validity of misappropriation theory); Chiarella v. United States, 445 U.S. 222 (1980) (declining to address misappropriation theory because it had not been presented to jury).

252. *See* United States v. O'Hagan, 521 U.S. 642, 652 (1997).

2. The ISP's Liability

The ISP would probably not have any vicarious tort liability for the hacker's theft. Such liability, based upon the agency doctrine of respondeat superior, does not exist when the employee's wrongful act is outside the scope of authority and does not serve the master in any way.[253] Theft by an ISP employee of a customer's information so that the employee can engage in the act of insider trading is clearly outside the normal scope of employment in the ISP context, so imposition of vicarious liability seems unlikely.[254] However, this does not completely rule out the possibility of liability, which might exist under the provisions of ITSFEA, as discussed below in another context.[255]

---

253. *See* HAROLD GILL REUSCHLEIN & WILLIAM A. GREGORY, THE LAW OF AGENCY AND PARTNERSHIP § 52 (2d ed. 1990) (explaining vicarious liability and its limitations).

254. Stock brokerage firms have been held liable for their employees' insider trading on grounds that they put the wrongdoers in a position to engage in the illicit trading. *See, e.g.*, SEC v. Management Dynamics, Inc., 515 F.2d 801, 812–13 (2d Cir. 1975). A similar argument — that the employer put the hacker in a position to hack — can be made against ISPs, but seems a bit more of a stretch. Trading by the securities professional is plausibly within the scope of authority absent use of the inside information, but hacking by the ISP professional seems totally beyond the pale.

Still, even in the context of brokerage firms, most courts and commentators have taken the view that illicit insider trading is not within the scope of employment for purposes of vicarious tort liability. *See, e.g.*, Energy Factors, Inc. v. Nuevo Energy Co., 1992 U.S. Dist. LEXIS 10208, at *18 (S.D.N.Y. July 7, 1992) (holding that employee who trades on or tips nonpublic information is normally on frolic of her own); O'Connor & Assoc. v. Dean Witter Reynolds, Inc., 529 F. Supp. 1179, 1194 (S.D.N.Y. 1981) (same); *see also* Helen A. Garten, *Insider Trading in the Corporate Interest*, 1987 WIS. L. REV. 573, 636 n.279 ("[W]ithout clear evidence to the contrary, insider trading is presumed to occur outside the scope of the firm's business . . . ."); Patrick Diaz & Rosemary Maxwell, Note, *Insider Trading and the Corporate Acquirer: Private Actions Under Rule 10b-5 Against Agents Who Trade on Misappropriated Information*, 56 GEO. WASH. L. REV. 600, 656 (1988) (noting that only rarely could employer be liable on vicarious liability basis for employees' insider trading); Jeanne M. Hauch, Note, *Insider Trading by Intermediaries: A Contract Remedy for Acquirers' Increased Costs of Takeovers*, 97 YALE L.J. 115, 122 (1987) ("Under respondeat superior, an employee's act must be within the scope of her employment — a difficult standard to meet in cases of well-hidden inside trading or tipping."); Bruce A. Teeters, Comment, *Insider Trading and Securities Fraud Enforcement Act of 1988: Just How Much Are Employers Going to Pay?*, 59 U. CIN. L. REV. 587, 612 (1990) ("[I]nside trading will rarely be within the scope of an employee's duties.").

255. The discussion of ITSFEA in the next Part will make it clear that imposition of liability upon an ISP for one of its employee's thefts of inside information is unlikely. *See infra* notes 264–72 and accompanying text. Regarding primary liability, ITSFEA would impose liability on an ISP for an employee's insider trading only if the ISP "knew or recklessly disregarded the fact that such controlled person was likely to engage in the

V. CAN E-MAIL CREATE INSIDER TRADING LIABILITY FOR COMPANIES THAT DO NOT ADEQUATELY CONTROL THEIR EMPLOYEES' COMMUNICATIONS?

As I discussed in an earlier article,[256] new technology creates new means of information dissemination and concomitant new opportunities for leaks of inside information. Because many corporations and firms are potentially legally responsible for the insider trading misdeeds of their employees, they must adjust their compliance programs to consider these new threats to security.

A. Current Considerations

Public corporations, law firms, accounting firms, and particularly firms engaged in the securities business must pay serious attention to potential insider trading activity by their employees. Such trading may not only tarnish the reputation of these firms and cost them business, it may also exact a substantial toll on them in terms of liability.

First, such firms could conceivably be liable for their employees' insider trading under the theory of respondeat superior. Although there is an ongoing debate about the continued viability of respondeat superior under Section 10(b)/Rule 10b-5 in light of the Supreme Court's decision in *Central Bank*,[257] several courts continue to recognize this route to imposing vicarious liability,[258] and many reasonable arguments can be made for its continued existence in the general context of Rule 10b-5 cases.[259] Nonetheless, although such liability should theoretically be

---

act or acts constituting the violation and failed to take appropriate steps to prevent such act or acts before they occurred." 15 U.S.C. § 78u-1(b)(1)(A) (1994). Regarding secondary liability, ITSFEA provides that at least in causes of action by injured contemporaneous traders, there is to be no respondeat superior liability. *See* 15 U.S.C. § 78u-1(b)(2) (1994).

256. *See* Prentice, *Corporate Disclosure*, *supra* note 3, at 76–87.

257. Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164 (1994) (holding that aiding and abetting is not viable theory under Section 10(b)/Rule 10b-5).

258. *See, e.g.*, Seolas v. Bilzerian, 951 F. Supp. 978, 981–84 (D. Utah 1997); Pollack v. Laidlaw Holdings, Inc., No. 90 Civ. 5788, 1995 U.S. Dist. LEXIS 5909, at *17 (S.D.N.Y. May 3, 1995). *But see In re* Prudential Ins. Co. of Am. Sales Practices Litig., 975 F. Supp. 584, 612–13 (D.N.J. 1996) (holding that *Central Bank*'s reasoning eliminates aiding and abetting liability); ESI Montgomery County, Inc. v. Montenay Int'l Corp., No. 94 Civ. 0119, 1996 U.S. Dist. LEXIS 592, at *3 (S.D.N.Y. Jan. 23, 1996) (same).

259. Many of these arguments are contained in Robert A. Prentice, *Conceiving the Inconceivable and Judicially Implementing the Preposterous: The Premature Demise*

available generally, it should not be applied in this context because, as explained in the previous Part, one must possess a vivid imagination to come up with a scenario under which illicit insider trading is within the scope of an employee's job.[260]

Second, firms can also be held liable under the "controlling person" provisions of section 20(a) of the Exchange Act.[261] Once a plaintiff under section 20(a) proves that an insider trading violation has occurred and that the defendant firm "controlled" the violator, the burden of proof shifts to the defendant to prove that it acted in good faith and did not directly induce or cause the violation. The rules regarding who is considered a "controlling person" are quite vague,[262] and there are cases indicating that controlling person liability is broader than respondeat superior liability.[263] Still, it seems that only in the exceptionally rare cases of true rogue firms would the criteria of controlling person liability be met.

Third, and most plausibly, firms face liability for their employees' insider trading under ITSFEA.[264] When passage of ITSA in 1984 did

---

of Respondeat Superior Liability Under Section 10(b), 58 OHIO ST. L.J. 1325 (1997).

260. *See supra* note 254 and accompanying text.

261. *See* 15 U.S.C. § 78t(a) (1994). Based upon a parallel "controlling person" provision in section 15 of the 1933 Securities Act, *see* 15 U.S.C. § 77o (1994), section 20(a) provides:

> Every person who, directly or indirectly, controls any person liable under any provision of this chapter or of any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable, unless the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the violation or cause of action.

15 U.S.C. § 78t(a).

262. *See* Lewis D. Lowenfels & Alan R. Bromberg, *Controlling Person Liability Under Section 20(a) of the Securities Exchange Act and Section 15 of the Securities Act*, 53 BUS. LAW. 1, 32 (1997) ("[T]he law with respect to controlling persons . . . is complex and confusing."). The courts are split on various fundamental questions, including whether to be a "controlling person" one must simply be capable of exercising control over the primary violator or must actually have done so. *See* Maher v. Durango Metals, Inc., 144 F.3d 1302, 1305 n.8 (10th Cir. 1998) (citing cases on both sides of dispute); Brown v. Enstar Group, Inc., 84 F.3d 393, 395–97 (11th Cir. 1996) (same), *cert. denied*, 519 U.S. 1112 (1997).

263. *See, e.g.*, Harrison v. Dean Witter Reynolds, Inc., 79 F.3d 609 (7th Cir. 1996) (upholding jury verdict against employer for crooked scheme of employees that had been held outside scope of employment for respondeat superior purposes); *see also* Harrison v. Dean Witter Reynolds, Inc., 974 F.2d 873, 881 (7th Cir. 1992) (earlier opinion in case).

264. *See supra* note 175.

not seem even to slow down the rising tide of insider trading cases occurring during the mergers-and-acquisitions boom of the mid-1980s, Congress decided to give the SEC some assistance. Hoping to "provide greater deterrence, detection, and punishment,"[265] Congress decided to impose "institutional, rather than merely individual,"[266] responsibility for insider trading.

ITSFEA focuses upon the securities industry and imposes its greatest burdens there. However, it also imposes liability for the insider trading activity of subordinates upon all "controlling persons," including public corporations and perhaps their officers and directors. The Act extends this liability to tipping, even when the tipping employees and their tippees do not trade, but instead act as conduits for others (remote tippees) who trade. Fortunately, firms are not strictly liable under ITSFEA for the inside trading of their employees. Under ITSFEA, liability for the insider trading of controlled persons cannot be based solely on the fact that a defendant employed a violator.[267] It should not be so based, because, as noted above,[268] insider trading is typically not within the scope of an employee's work activities.

Although it does not impose strict vicarious liability, ITSFEA does place substantial burdens upon firms in the securities industry. Firms such as brokerages and investment advisers can be held liable for failing to establish, maintain, or enforce procedures and policies designed to prevent insider trading by employees.[269] Public companies in general are not subjected to such a high standard, but neither are they ignored. Their ITSFEA liability for the insider trading activity of an employee arises only when they, as controlling persons, "knew or recklessly disregarded

---

265. H.R. REP. NO. 100-910, at 7 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6044.

266. *Id.* at 14–15, *reprinted in* 1988 U.S.C.C.A.N. at 6051–52. Congress's rationale for imposing such liability was spelled out in the report:

> The Committee intends through the broadening of controlling person civil penalty liability to increase the economic incentives for such persons to supervise vigorously their employees. Effective supervision of securities firms of their employees and agents is a foundation of the federal regulatory scheme of investor protection. With respect to insider trading in particular, the necessity for appropriate supervision to prevent violations is evident in view of the special opportunities for abuse in this area.

Id. at 17, *reprinted in* 1988 U.S.C.C.A.N. at 6054.

267. *See* 15 U.S.C. § 78u-1(b)(2) (1994).

268. *See supra* note 254 and accompanying text.

269. *See* 15 U.S.C. § 78u-1(b)(1)(B). Thus, whereas all companies can be liable for knowingly or recklessly disregarding the fact that their subordinates were likely to engage in insider trading, securities firms can also be liable for knowingly or recklessly failing to institute control procedures.

the fact that such controlled person was likely to engage in the act or acts constituting the violation and failed to take appropriate steps to prevent such act or acts before they occurred."[270] The penalties for violation are substantial.[271]

ITSFEA and other considerations, such as the federal sentencing guidelines for corporations,[272] caused firms and companies around the country to install compliance programs to monitor and prevent insider trading. Such programs must keep pace with technological developments.

B. Complications Created by Technology

Increased securities trading and other securities-related activity occurring across the Internet necessitate reevaluation of insider trading compliance programs. For example, employees increasingly are using e-mail as a major means of communication in securities-related transactions.[273] They often use websites as well. There is no particular reason that these new avenues of communication should cause the SEC to alter the content of its policies regarding insider trading. However, on the enforcement end, the SEC should alter its investigation procedures

---

270. 15 U.S.C. § 78u-1(b)(1)(A).

271. The basic civil liability of a controlling person "shall not exceed the greater of $1,000,000, or three times the amount of the profit gained or loss avoided as a result of such controlled person's violation." 15 U.S.C. § 78u-1(a)(3). Additionally, criminal liability can be imposed. ITSFEA increased the criminal penalties to a maximum of 10 years in jail and/or a $1,000,000 fine for individuals and up to a maximum fine of $2,500,000 for non-natural persons. *See* 15 U.S.C. § 78ff(a) (1994).

272. Under the federal sentencing guidelines, corporations whose employees commit crimes within the scope of their employment may receive substantial breaks in sentencing when they have effective compliance programs in place. *See generally* Pamela H. Bucy, *Organizational Sentencing Guidelines: The Cart Before the Horse*, 71 WASH. U. L.Q. 329 (1993) (explaining operation of guidelines); Charles J. Walsh & Alissa Pyrich, *Corporate Compliance Programs as a Defense to Criminal Liability: Can a Corporation Save Its Soul?*, 47 RUTGERS L. REV. 605 (1995) (suggesting that juries be allowed to consider evidence of corporate compliance programs); Kevin B. Huff, Note, *The Role of Corporate Compliance Programs in Determining Corporate Criminal Liability: A Suggested Approach*, 96 COLUM. L. REV. 1252 (1996) (same).

273. *See SEC Will Not Make Firms Pre-Review E-mail*, FIN. NETNEWS, Jan. 12, 1998, at 2 (noting that new SEC rules will encourage more e-mail use by brokers).

to consider these sources as possible mechanisms for illicit disclosure of inside information.[274]

Securities firms and public companies faced with the responsibility of controlling their employees' insider trading under ITSFEA must be extra vigilant with respect to this new form of potential disclosure. At least three areas deserve extended attention:

1. Policing Intentional and Inadvertent Tipping

Some observers have worried that as seemingly innocuous a practice as posting personal web pages creates a potential avenue for disclosure of material, nonpublic information.[275] As I noted in an earlier article, "[i]n addition to the normal mixture of boring reports of Junior's soccer games and innocuous braggadocio, an employee might talk about the stirring success she and the other engineers down at the plant are having with the development of a new product."[276]

The opportunity to use e-mail is made particularly problematic by the fact that this new medium tends to cause employees, who are generally aware of the need to keep sensitive company information secure, to speak more freely than they would in other media[277] and to make disclosures that they might not otherwise make.[278] The relative

---

274. Although the SEC has altered many investigation and enforcement practices to account for Internet-related activity, e.g., by having some of its employees surf the Internet on a regular basis looking for fraudulent activity, *see* Sarah Stirland, *News and Trends: Securities Regulators Prowl the Net, Looking for Lawbreakers*, BOND BUYER, Nov. 13, 1996, at 34, it has yet to take other important steps. For example, the SEC is not yet authorized to have its employees pose as investors in stock chat rooms in order to gather information on suspected frauds. *See With 3 Million Trading Securities On Line, Regulatory Issues Multiply, Panelist Says*, BNA SEC. L. DAILY, May 6, 1998 [hereinafter *Regulatory Issues Multiply*] (quoting congressional staffer Jeff Duncan).

275. *See generally* Harvey L. Pitt & Dixie L. Johnson, *Avoiding Spiders on the Web: Rules of Thumb for Issuers Using Web Sites and E-mail*, WALLSTREETLAWYER.COM, June 1997, at 6.

276. Prentice, *Corporate Disclosure*, *supra* note 3, at 81.

277. *See* Maryann Waryjas, *Cyberspace Offers a New Medium for SEC Filings*, NAT'L L.J., Dec. 18, 1995, at B10 ("[T]he presumed anonymity of voiceless and faceless participants can foster a false sense of being 'off the record' and may result in users discussing and disclosing information more freely than they would in other circumstances.").

278. *See* Parry Aftab, *Monitoring Communications on the Internet: Big Brother or Responsible Business?*, N.Y. L.J., Sept. 30, 1996, at S2.

> [F]or some reason, people "say" things in E-mail and on-line which they might not otherwise feel comfortable communicating to others. A combination of the informality with the lack of inhibitions often demonstrated in on-line communications creates

"feeling of anonymity" one has while communicating over the Internet is definitely misleading. Commentators have worried about loyal employees disclosing too much in online chatrooms in misguided attempts to defend their employers,[279] and it turns out the worries have been justified. In one recent situation, an employee of Texas Instruments who belonged to an investment club posted to an Internet chat room nonpublic financial information about the company in an apparently innocent attempt to be "helpful."[280]

Disclosure concerns are exacerbated by the fact that an employee's disclosure of sensitive information over the Internet usually leaves a trail that can be traced.[281] However informal an e-mail seems to be, it "creates a document, and depending upon internal e-mail policies and procedures, that document may or may not be handled as confidential, deemed 'published,' or be discoverable in connection with litigation and/or investigations by agencies."[282]

Although inadvertent tipping may well present the biggest potential problem, observers have suggested that the new technologies create several new avenues for intentional tipping as well.[283] Thus, these

---

> a dangerous situation for employees and their employers, to which the statements may be attributed.

Id.; *see also* Matthew R. Burnstein, Note, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 83 (1996) ("[T]he caution ordinarily exercised in face-to-face real space tends to recede in the world of anonymity and solitude that one finds in front of computer terminals.").

279. *See* Morgan Molthrop, *Chat Rooms — Investor Relations Latest Migraine*, WALLSTREETLAWYER.COM, Sept. 1998, at 16.

280. *See* Del Jones, *Balancing Ethics and Technology: Companies Grapple with Limiting Employee Abuse*, USA TODAY, Apr. 27, 1998, at 1A.

281. *See, e.g.*, Patrick Mitchell, *Following the E-mail Trail*, COMPUTER SHOPPER, Apr. 1, 1997, at 92 (noting that e-mail is often fruitful source of evidence in litigation); Victoria Sonshine Pasher, *Cos. Urged to Set Up E-mail Plans*, NAT'L UNDERWRITER, Apr. 14, 1997, at 11 (noting situation where employees were fired after inappropriate e-mail messages were traced to them).

282. Micalyn S. Harris, *E-mail Ethics on Intranets*, WALLSTREETLAWYER.COM, July 1997, at 6.

283. *See* Wolowitz & Diana, *supra* note 6, at B7.

> Posting information on a corporation's [website] could increase the risk of traditional insider trading, as corporate insiders may attempt to mask inside information known only to co-conspirators. The relative anonymity and ease of online communication may hamper efforts to connect an illegal trader with the source of the information. Furthermore, the use of chat rooms, bulletin boards or e-mail to provide inside information to potential tippees is easier than setting up clandestine meetings and is harder to trace than are traditional means of communication,

relatively new mechanisms for disclosure heighten the need for firms to develop, install, and enforce policies aimed at minimizing illicit insider trading and tipping. Whether the tipping is inadvertent or intentional, firms involved in the securities industry must be particularly concerned because they are responsible for creating policies and procedures to prevent illicit insider trading by their employees.[284] Worries about insider trading and other related activity have prompted some brokerage firms to prohibit employees from using e-mail to contact customers[285] or from setting up their own websites.[286]

Because of its heightened liability for insider trading by employees,[287] the securities industry generally stays on top of such matters. For example, Nasdaq has introduced a surveillance device designed to detect the use of nonpublic, market-sensitive information on the Internet.[288] Both the NYSE and National Association of Securities

---

such as phone calls or paper memorandums.

Id. at B12.

284. Firms seeking guidance for formulation and implementation of such policies can productively consult several resources. *See generally* BROWN, *supra* note 22, ch. 12; Marc I. Steinberg & John Fletcher, *Compliance Programs for Insider Trading*, 47 SMU L. REV. 1783, 1828–35 (1994); Alan M. Weinberger, *Preventing Insider Trading Violations: A Survey of Corporate Compliance Programs*, 18 SEC. REG. L.J. 180 (1990).

285. *See* Adam Rombel, *OPCO Will Limit E-mail to Brokers with Clean Slates*, FIN. NETNEWS, May 5, 1997 ("Oppenheimer & Co. plans to limit the use of e-mail to senior brokers with clean disciplinary records.").

286. *See Regulatory Talk: Allen Meyer*, FIN. NETNEWS, July 28, 1997 (interview with Allen Meyer, Director of Compliance for Paine Webber, who notes that Paine Webber prohibited brokers from creating personal websites or e-mailing customers but planned to loosen e-mail rules soon).

287. *See* Tim Wilson, *E-Mail Eavesdropping — New Regulations, Software Enforce Content Restrictions*, COMMUNICATIONSWEEK, Apr. 7, 1997 ("[I]n the securities industry — where a trader's fraudulent claim or 'insider' tip could lead to censure, fines, lawsuits or jail time — new rules recently have been passed that outline requirements for the systematic monitoring and screening of E-mail between stockbrokers and their customers.").

288. *See* Jane Martinson, *NASDAQ Steps Up Fight Against Internet Fraud: U.S. Stock Market to Launch Surveillance Device*, FIN. TIMES, Sept. 5, 1997, at 12 (describing such device to be launched by end of 1997).

One such system, developed by the Integralis-Sequel-SRA partnership, automatically opens and searches e-mail for suspicious words, phrases, or concepts, and would work something like this:

> A broker posts an E-mail message to a customer. The message is then stored in an archive and logged by Sequel's Net Access Manager, a Windows NT-based tool that tracks transmissions to and from IP networks.
>
> The message is then opened by Integralis' MIMEsweeper, which turns E-mail messages and attached files into ASCII code

Dealers ("NASD") attained SEC approval for programs that require members either (1) to develop written policies and procedures for reviewing electronic correspondence before it is sent, or (2) to educate and train employees regarding firm procedures for electronic correspondence, to document such education and training, and to monitor and test implementation and compliance with the firm's policies.[289] Employees are generally prohibited from e-mailing the public unless their communications are subject to these supervisory and review procedures.[290] Furthermore, members are to prohibit communications with the public via employees' home computers or other non-firm computers unless the firm is capable of monitoring those transmissions.[291] The new rules also address retention of e-mail communications for recordkeeping purposes.[292] These new policies are

---

> that can be searched for keywords. The message is handed over to SRA's NameTag, an advanced language analysis application that can search for phrases and concepts that indicate a potential securities-law violation, such as "guaranteed to double your money," or "the next Microsoft."
>
> If the message does not contain such red-flag language, it can be immediately sent to the customer. If it does, it can be kicked out to a queue for examination by a person.

Wilson, *supra* note 287.

289. *See* Order Approving Proposed Rule Change, Exchange Act Release No. 39,511, 63 Fed. Reg. 1135 (Dec. 31, 1997) [hereinafter NYSE Procedures] (approving NYSE procedures); Order Approving Proposed Rule Change, Exchange Act Release No. 39,510, 63 Fed. Reg. 1131 (Dec. 31, 1997) [hereinafter NASD Procedures] (approving NASD procedures).

290. The SEC later approved rule changes that allowed broker-dealers to substitute a system of random spot checks in place of the requirement of prior approval of all written and electronic correspondence. *See* NYSE Procedures, *supra* note 289, at 1136; NASD Procedures, *supra* note 289, at 1132.

291. *See* NYSE Procedures, *supra* note 289, at 1136; NASD Procedures, *supra* note 289, at 1132.

292. *See* NYSE Procedures, *supra* note 289, at 1136; NASD Procedures, *supra* note 289, at 1132. The basic issue had been whether an e-mail communication should be treated as a memo which, if it were on paper, would be retained in hard copy, or as a substitute for a phone call, retention of which would typically be impossible and therefore not required. *See generally* Ben Pappas, *SEC, NASDR, NYSE to Fine Tune E-mail Requirements*, COMPLIANCE REP., July 22, 1996, at 1.

The SEC has recently approved rules requiring brokerage firms that have hired more than a certain percentage of employees who have been guilty of industry violations to tape all telephone calls those brokers have with investors. Firm policies should similarly address e-mail correspondence. *See* Order Granting Approval of Proposed Rule Change, Exchange Act Release No. 39,883, 63 Fed. Reg. 20,232 (Apr. 17, 1998). *See generally SEC Allows Rule Requiring Taping of Conversations*, WALL ST. J., Apr. 21, 1998, at C20.

being drafted by interdisciplinary in-house task forces, gaining input from many departments — compliance, marketing, trading, technology, product development, and others.[293] Enforcement of the policies will likely result in the formation of special Internet compliance groups within large securities firms.[294]

Law firms, accounting firms, and public companies registered under the Exchange Act should also seriously consider new policies to deal with the new technologies, even though their liability under ITSFEA is more limited than that of securities firms.[295] Implementation of such policies will help prevent insider trading by employees and help convince the SEC that the firm is acting in good faith to uphold its responsibilities under ITSFEA even if the occasional employee does violate the rules. For example, given the extensive potential liability for employee tipping, designated company officials should vet responses to inquiries from outside a public corporation, even if communicated in the informal medium of e-mail.[296]

2. Selective Disclosure Problems

Part II of this Article addressed the question of what is considered "public" information. Generally, trading by insiders is permissible only after there has been public dissemination of information and time for absorption. As noted earlier,[297] one problem area is the potential for selective disclosure to analysts who are following a company's stock. Use of e-mail is likely to exacerbate the SEC's concern over selective disclosure.

---

293. *See Regulatory Talk: Mark Egert*, FIN. NETNEWS, June 16, 1997 (interview with Mark Egert, associate general counsel for the Securities Industry Association).

294. *See Regulatory Talk: Allen Meyer*, *supra* note 286.

295. *See* Howard M. Friedman, *The Insider Trading and Securities Fraud Enforcement Act of 1988*, 68 N.C. L. Rev. 465, 478 (1990) ("Thus, law firms, banks, accounting firms, financial publishers, and indeed issuers themselves now face the risk of civil penalties unless these firms adopt measures to control the risk of information misuse by employees."); *see also* Barbara Bader Aldave, *The Insider Trading and Securities Fraud Enforcement Act of 1988: An Analysis and Appraisal*, 52 ALB. L. REV. 893, 909–10 (1988) ("If the threat of civil penalties . . . inspires . . . employers to improve their systems for controlling access to sensitive information and educating their employees about the consequences of misusing such information, the new penalty statute may well achieve its purpose of reducing the incidence of unlawful trading and tipping." (footnote omitted)).

296. *See* Steinberg & Fletcher, *supra* note 284, at 1831–32 (explaining benefits of such procedure).

297. *See supra* Part II.B.2.c.

Consider the situation where a persuasive analyst e-mails an issuer's manager with a query. Of course, the manager should be aware of the danger of selective disclosure. As long ago as 1977, Judge Kaufman noted the dilemma facing managers:

> [One] may analogize [a manager's] encounter with a financial analyst to a fencing match conducted on a tightrope; he is compelled to parry often incisive questioning while teetering on the fine line between data properly conveyed and material inside information that may not be revealed without simultaneously disclosing it to the public.[298]

The SEC has taken a dim view of such selective disclosures and has launched enforcement actions in several cases.[299] Currently there is

---

298. SEC v. Bausch & Lomb, Inc., 565 F.2d 8, 9 (2d Cir. 1977). *See generally* James H. Fogelson, *Disclosure Laws Retain Teeth Despite Recent Court Limitations*, NAT'L L.J., Feb. 22, 1982, at 30 ("There clearly is no question that an issuer is not permitted to make selective disclosure of material inside information to a securities analyst."); Harvey L. Pitt & Karl A. Groskaufmanis, *For the Issuer, It's Sometimes Tempting to Provide Analysts with Non-Public Information*, NAT'L L.J., Apr. 18, 1994, at B4 [hereinafter Pitt & Groskaufmanis, *Tempting*] (noting legal perils of selective disclosure).

299. *See* SEC v. Rosenberg, Litig. Release No. 12,986, 49 SEC Docket 1373 (Sept. 24, 1991) (SEC insider trading action against analyst who received selective disclosure and traded personally thereon); SEC v. Stevens, Litig. Release No. 12,813, 48 SEC Docket 739 (Mar. 19, 1991) (SEC injunctive action against CEO of small company who had telephoned corporate developments to several analysts); State Teachers Retirement Bd. v. Fluor Corp., 566 F. Supp. 945 (S.D.N.Y. 1983) (Rule 10b-5 suit alleging selective disclosure by manager of public relations to analyst in meeting that was part of firm's regular investor-relations program).

The SEC argues that when insiders selectively disclose to analysts and others, they are doing so to enhance their reputations. *See* Bruce A. Hiler, *The SEC and the Insider/Tipper*, N.Y. L.J., Aug. 29, 1991, at 5 (explaining SEC view). *Dirks v. SEC*, 463 U.S. 646 (1983), held that tippee insider trading liability arises if a tipper wrongfully tips information. Information is wrongfully tipped when the tipper acts out of motives of "personal benefit," such as "a pecuniary gain or a *reputational benefit* that will translate into future earnings." *Id.* at 663 (emphasis added).

Some commentators believe that the SEC's victory in *United States v. O'Hagan*, 521 U.S. 642 (1997), will encourage it to continue pressing its theory vigorously. *See* Pitt & Groskaufmanis, *Upheld Misappropriation Theory*, *supra* note 167, at B6 ("[T]he breadth of the court's *O'Hagan* ruling will inspire the [SEC's] watch-dogs to cast a sharper eye at the quarterly dance between issuers and analysts."). There is some evidence of this. In a February 27, 1998 speech, SEC Chairman Arthur Levitt specifically condemned communications from issuers to analysts (or even groups of analysts) before a press release of new material information. *See SEC Watching for*

widespread belief that the SEC is looking for the proper opportunity to "make an example of someone." Yet, there is a strong incentive for an issuer to disclose to an analyst, given the good that analysts can do for a company's stock price.[300] But if the answer to an analyst's e-mail request contains more details than have been made publicly available, then the response arguably is actionable "selective disclosure." Furthermore, the incentive to disclose selectively is increased by the anonymous feel of the e-mail medium of communication noted earlier.[301] Thus, use of the Internet as a disclosure mechanism, whether via e-mail, chat rooms, or home pages, creates additional opportunities for selective disclosure and thereby multiplies the chances of creating liability.[302]

Harvey Pitt and Karl Groskaufmanis have helpfully suggested six guidelines[303] to aid firms facing these difficulties: (1) limit the number of spokespersons in order to limit sources of potential liability, (2) brief the corporate spokesperson to guard against inadvertent errors, (3) debrief the spokesperson in order to determine if too much was said, (4) avoid enmeshing the company in analysts' reports so as to avoid "entanglement" liability,[304] (5) maintain disclosure binders to provide a paper record of disclosures, and (not just as an afterthought) (6) tell the truth.

In a recent article, I expanded upon two of these rules of thumb:

> First, companies should limit the number of spokespeople. With the advent of e-mail and the Internet, the difficulty of limiting the number of outlets for corporate disclosure became even more difficult,

---

Possible Insider Trading by Analysts with Advance Word of Big News, BNA SEC. L. DAILY, Mar. 2, 1998.

300. *See* Lev, *supra* note 122, at 22 ("Managers are generally interested in having a large and sympathetic analyst following, since it attracts investors (particularly institutional ones) and enhances the demand for the stock."). The SEC permits such disclosures, *see* Public Statements by Corporate Representatives, Securities Act Release No. 6504, 49 Fed. Reg. 2468 (Jan. 13, 1984), and they are encouraged by the American Stock Exchange and NYSE. *See* AMERICAN STOCK EXCHANGE GUIDE ¶ 10,122 (1984); NEW YORK STOCK EXCHANGE MANUAL § 202.02 (1983).

301. *See supra* notes 277–80 and accompanying text.

302. *See* Prentice, *Corporate Disclosure*, *supra* note 3, at 26–87; *see also* Jeffrey B. Rudman et al., *Disclosure in Cyberspace* (Sept. 17, 1996) <http://www.haledorr.com/publications/seclit/Disclose.html> ("There is no case law expressly addressing how the securities laws play out with these forms of communication.").

303. *See* Pitt & Groskaufmanis, *Tempting*, *supra* note 298, at B6.

304. For a quick, recent summary of entanglement liability, see William O. Fisher, *The Analyst-Added Premium as a Defense in Open Market Securities Fraud Cases*, 53 BUS. LAW. 35, 45–50 (1997).

> but this remains important advice. "All employees should understand that all inquiries from investors, analysts, financial reports and others outside the company should be directed to the spokesperson." . . . [A] "company must train its people not to talk" (or to answer their e-mails or to post to newsgroups) unless they do so in compliance with well-established company disclosure procedures.
>
> . . . . In making th[e] recommendation [to tell the truth], Pitt and Groskaufmanis are not simply suggesting that as a strategic decision it may be wise to tell the truth rather than to lie. They are also emphasizing that "[a] spokesperson should understand that even casual Friday afternoon contacts may be memorialized in some file." This is the case regarding e-mails as well. There is no such thing as a "casual Friday afternoon e-mail" and every corporate employee who might be contacted by outsiders must understand that fact.[305]

The good news for the securities industry is that if technology causes a revisiting of the issue of selective disclosure to analysts, the SEC will be afforded an opportunity to alter its approach, which will probably be for the better. Professor Coffee has labeled as "doubtful" the SEC's apparent theory that selective disclosure to analysts should automatically be equated with insider trading. He believes that fewer disclosures to analysts will cause more surprises in the market which will lead, in turn, to greater market volatility that will injure investors.[306] The Internet affords an opportunity for distributing corporate information more quickly to more investors than ever before and a concomitant chance to increase the transparency of the market, to reduce the number and magnitude of "bombshell" announcements, and thereby to reduce market volatility.[307] Just as corporate officers must walk a

---

305. Prentice, *Corporate Disclosure*, *supra* note 3, at 86–87 (footnotes omitted) (quoting Pitt & Groskaufmanis, *Tempting*, *supra* note 298, at B6, *and* Jere Thomson & John Chrisman, *Beware of Forward Statements and Disclosure*, INT'L FIN. L. REV., Apr. 1996, at 20).

306. *See* John C. Coffee, Jr., *Disclosures to Analysts Are Risky*, NAT'L L.J., Feb. 1, 1993, at 20.

307. On the other hand, the SEC's actions attacking selective disclosure to analysts that were criticized in Coffee's article, *see id.*, were strongly defended by Hiler, *The SEC and the Insider/Tipper*, *supra* note 299, at 5. I have enough sympathy for Hiler's views

tightwire when they discuss issues with analysts, so must the SEC walk a tightwire in balancing the important role that analysts play in the market with the need for equal treatment of average investors.

3. Technology and the "Chinese Wall"

Most large securities firms today engage in multiple activities, some of which have the potential to create problems related to insider trading rules.[308] For example, if the mergers-and-acquisitions department of an investment banking firm is hired to assist in a highly-secret takeover of XYZ Company, problems arise if that information is passed on to the firm's investment advisers, who will wish to alert their clients regarding the takeover. Such conflicts[309] have led to the creation of the well-known concept of a "Chinese Wall," "the term given to procedures and policies restricting the flow of material, nonpublic information among the potentially conflicting departments of [a firm in the securities business] and in effect isolating the information within the department to which it has been entrusted."[310] Congress passed ITSFEA's

---

and for the value of equal access that I hope the SEC does not completely ignore that value in reassessing its policies.

308. *See* Charles W. Wolfram, *Screening*, *in* CONFLICTS OF INTEREST IN CLINICAL PRACTICE AND RESEARCH 137, 145 (Roy G. Spece et al. eds. 1996) ("At bottom, the conflict issue is based on the fact that modern securities business is multifarious. Modern securities firms encounter most of their conflict-of-interest problems because they structure and market themselves as multi-service or integrated capital-transfer firms.").

309. For an explanation of the dilemma that this conflict poses for broker-dealers, see SHELDON M. JAFFE, BROKER-DEALERS AND SECURITIES § 7.10, at 148–53 (1977).

310. FERRARA, *supra* note 18, § 9.01, at 9-2. Ferrara traces the origin of Chinese Walls to the SEC's proceeding against Merrill Lynch in 1968 for events arising out of a famous incident involving Douglas Aircraft. *See* Merrill Lynch, Pierce, Fenner & Smith, Inc., 43 S.E.C. 933 (1968). Merrill Lynch's underwriting arm was involved in preparing an offering for Douglas Aircraft, and in that role its underwriters learned of adverse financial news about Douglas. This information was leaked to Merrill Lynch's retail sales side, and several of Merrill Lynch's institutional customers were advised to sell their Douglas shares before the adverse financial information became public. *See id.* at 935. Merrill Lynch settled the case by agreeing to establish a Chinese Wall to prohibit members of its underwriting department from disclosing material, nonpublic information they learned during the course of their duties to other Merrill Lynch employees outside the underwriting department. *See id.* at 938.

The SEC formalized its position on Chinese Walls by providing an institutional defense in Rule 14e-3. Firms whose employees engage in trading securities when other members of the firm are in possession of inside information regarding a relevant takeover may escape liability by showing (1) that the employee who made the actual trading decision did not know the material, nonpublic information, and (2) that the firm

provisions regarding compliance procedures in large part to encourage the strengthening of Chinese Walls,[311] and the Act had that effect.[312]

As Ferrara explains:

> The specific policies and procedures relied upon [to erect and maintain a Chinese Wall] will vary from firm to firm. Firms can turn to code names or numbers to disguise the identity of target corporations, elaborate paper shredding procedures, physical separation of the trading department from those departments that regularly receive confidential information, education of all employees handling material, nonpublic information about firm procedures, and so on. Whatever the procedure relied upon, however, the basic principle of containment remains the same.[313]

To ensure containment today, any firm desiring to convince the SEC that it has an effective Chinese Wall[314] will have to consider technological developments. Now that so much financial information can flow through a firm electronically across its intranets,[315] insider trading possibilities multiply. They cannot be safely ignored. This Article has already discussed the danger of theft of inside information by outside hackers.[316] However, it is well known that a large majority of illicit computer intrusions are by insiders, and that they cause massive losses to companies each year.[317] No matter how effective a firm's

---

had implemented a Chinese Wall policy designed either (a) to prevent trading regarding such securities ("restricted lists") or (b) to prevent the person involved in potential trading from learning of inside information. *See* 17 C.F.R. § 240.14e-3(b)(2) (1998).

311. *See* 134 CONG. REC. 23,598 (1988) (statement of Rep. Markey); *id.* at 23,601 (statement of Rep. Cooper).

312. *See* Steinberg & Fletcher, *supra* note 284, at 1825 ("[S]ince ITSFEA's passage in 1988, firms have formalized their procedures that address the minimum elements of Chinese Walls.").

313. FERRARA, *supra* note 18, § 9.01, at 9-2.

314. Some commentators have argued that the Supreme Court's stressing in *O'Hagan* of the *use* (not mere possession) of nonpublic information redoubles the importance of Chinese Wall procedures. *See* Pitt & Groskaufmanis, *Upheld Misappropriation Theory*, *supra* note 167, at B6.

315. "An intranet is an internal on-line information highway, a mini Internet if you like. It's a closed system used by companies for the distribution of information within their own firms." Annabel Kennedy, *Intranets Keep It In-House*, THE HERALD (Glasgow), Oct. 24, 1996, at 12.

316. *See supra* Parts III–IV.

317. *See* Rustad & Eisenschmidt, *supra* note 141, at 221 ("The greatest threat to the

firewalls are in thwarting outside hackers, there is emerging a large online market for corporate data that is stolen by the firm's own employees.[318] Theft of trade secrets seems to be the most prominent problem, but theft of information for purposes of insider trading is just as plausible.

In the face of information flowing across intranets, the key tools to maintaining a Chinese Wall are switches and routers.[319] Switches are not "intelligent" tools but can be used to segment intranets into subnetworks and thereby localize traffic while optimizing bandwidth. Switches can be used to ensure that data packets are not sent out of the local subnetwork of the intranet.[320] Routers are "intelligent" tools in that they examine packets of data to determine their destination. Routers have the capacity to permit or deny packets to proceed on particular routes based on packet-header information such as the Internet Protocol source and destination addresses, the encapsulated protocol, and the message type.[321] Various vendors are selling routers with security capabilities that can maintain security and data privacy and thereby bring Chinese Walls into the twenty-first century.[322] Without such high-tech tools, a securities firm's Chinese Wall is arguably inadequate today.[323]

---

security of client computers is not the Internet hacker, but rather the enemy within, the in-house hacker."); William J. Cook, *Industrial Espionage and the Internet*, CHI. LAW., Feb. 1997, at 57. Cook's article reports the results of two surveys of corporate security managers. In a 1996 *Information Systems Security* survey of 236 security managers, 46% of the companies reported insider abuse of computer systems, with 22% indicating losses between $50,000 and $200,000 and an additional 20% placing losses at between $200,000 and $500,000. An October 1995 Michigan State survey of 150 corporate security directors revealed that 98.6% of their companies had suffered a computer-related crime, 75–80% caused by insiders. *See id.* An earlier study by the National Institute of Justice had shown that 79% of the thefts of inside information were by insiders or persons working with insiders. *See id.*

318. *See* Wilder & Violino, *supra* note 141, at 30.

319. *See* Emily Kay, *Safeguarding Intranets — Routers, Switches Help Secure Sensitive Data and Boost Reliability*, INFORMATIONWEEK, Sept. 16, 1996, at 124 (describing bank that uses computer hardware to segregate information in securities unit from other units in company).

320. *See id.*

321. *See id.*

322. *See id.*

323. As one senior manager has said, "Sure, we'll put policy barriers in place so we're not allowed to pass information between internal units, but it's also wise to put physical network barriers in place." *Id.* (internal quotation marks omitted) (quoting John Donovan).

Installation of firewalls has the added benefit of potentially qualifying the corporate installer to sue under the Economic Espionage Act of 1996 ("EEA") to protect their trade secrets. *See* Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831–1839

VI. WHAT IMPLICATIONS DOES INTERNET TECHNOLOGY CARRY FOR INTERNATIONAL ENFORCEMENT OF INSIDER TRADING RULES?

A. Introduction

Over the past decade or so, the globalization of securities markets has proceeded at a formidable pace.[324] Many factors have contributed to this trend, but the one cited most often is the rapid progress in computer telecommunications technology.[325] This technological revolution has been accelerated by Internet technology, and many predict that securities trading on physical exchanges will increasingly give way to computerized trading.[326] In the United States alone, sixty or so alternative trading systems existing on the Web now account for

---

(Supp. III 1997)). A prerequisite to suit under the EEA is that the plaintiff has taken "reasonable measures," such as installing a firewall, to protect its trade secrets. *See* David O. Stephens, *Document Security and International Records Management*, RECORDS MGMT. Q., Oct. 1997, at 69.

324. *See, e.g.*, Kellye Y. Testy, *Comity and Cooperation: Securities Regulation in a Global Marketplace*, 45 ALA. L. REV. 927, 931 (1994) ("Securities trading has become an 'around-the-clock' and 'around-the-globe' affair since investment portfolios have become increasingly global in scope."); James A. Kehoe, Note, *Exporting Insider Trading Laws: The Enforcement of U.S. Insider Trading Laws Internationally*, 9 EMORY INT'L L. REV. 345, 345 (1995) ("Internationalization of the world's securities markets is taking place at an increasingly rapid rate.").

325. *See, e.g.*, Michael A. Gerstenzang, Note, *Insider Trading and the Internationalization of the Securities Markets*, 27 COLUM. J. TRANSNAT'L L. 409, 410 (1989) ("The *sine qua non* of market internationalization . . . has been the use of advanced technology in the securities industry."); John Thornell Thomas, Note, *Icarus and His Waxen Wings: Congress Attempts to Address the Challenges of Insider Trading in a Globalized Securities Market*, 23 VAND. J. TRANSNAT'L L. 99, 105 (1990) (citing several sources).

326. *See, e.g.*, Therese H. Maynard, *What is an "Exchange" — Proprietary Electronic Securities Trading Systems and the Definition of an Exchange*, 49 WASH. & LEE L. REV. 833, 862–63 (1992); Lewis D. Solomon & Louise Corso, *The Impact of Technology on the Trading of Securities: The Emerging Global Market and the Implications for Regulation*, 24 J. MARSHALL L. REV. 299, 318–19 (1991).

These predictions have been borne out, prompting even more aggressive predictions. *See* Dominic Bencivenga, *SEC Takes Solomonic Approach to Regulation*, N.Y. L.J., Apr. 30, 1998, at 5 [hereinafter Bencivenga, *Solomonic Approach*] (noting a "dramatic growth in alternate [trading] systems and the increasing volume of securities traded there" as well as describing the SEC's proposed regulatory response); Deb Price, *Internet Opens Investing to the Masses*, DETROIT NEWS, Jan. 10, 1998, at C1 ("Online investing accounts will hit 3 million by the end of [1998], according to Forrester Research, and zoom to 14.4 million in 2002.").

about 20% of the transactions in Nasdaq securities and about 5% of exchange-listed securities.[327] As many as 14 million online securities accounts are predicted for the U.S. market by 2002.[328] In addition, an English company recently announced that investors will soon be able to buy and sell shares using the Internet global network and do so at only a tenth of the cost of going through a traditional broker.[329]

Unfortunately, as noted at the beginning of this Article,[330] many believe that use of the Internet for these trades, especially across national boundaries, will increase the possibility of insider trading. Additionally, the seamlessly global nature of the Internet creates yet another medium over which material, nonpublic information can be transmitted or acquired by those who engage in insider trading.

For regulatory bodies, such as the SEC, the development of the Internet creates a dangerous intersection of two jurisdictional problems. First, the global nature of the securities business has for many years created jurisdictional confusion[331] and enforcement problems, especially in insider trading cases.[332] Second, the Internet's creation of cyberspace has created its own set of jurisdictional problems. Who, if anyone, has the right (and power) to regulate cyberspace? The intersection of these two sets of dilemmas creates difficult and critically important problems,[333] especially for insider trading enforcement.[334] Some commentators fear that "inside traders [on the Internet] are beyond the

---

327. *See* Suzanne Woolley, *The New Stock Traders*, BUS. WK., May 4, 1998, at 124, 125, 127; *see also* Marc Ferranti, *SEC Proposes Electronic Stock Trading Rules*, INFOWORLD, Apr. 27, 1998, at 80 (describing recent SEC regulatory initiatives for these electronic exchanges).

328. *See* Woolley, *supra* note 327, at 125 (citing study by Forrester Research). The average commission paid to an online broker fell from $34.65 at the beginning of 1997 to $15.95 by the year end. *See id.* at 127. Others cite $8–$9 as the common cost of an online trade today. *See Regulatory Issues Multiply*, *supra* note 274.

329. *See* Winton, *supra* note 6.

330. *See supra* note 6 and accompanying text.

331. *See* Thomas, *supra* note 325, at 110 ("[Q]uestions still remain concerning the rules of the globalized [securities] market and the SEC's role in that market.").

332. *See id.* ("The globalization of [securities] markets is continuing, but that process is also producing an environment conducive to international crime.").

333. *See* Brakebill, *supra* note 1, at 909–10 ("Cyberspace has created a host of potential legal questions and challenges for courts and regulatory bodies [in the securities field]. For example, Internet offerings are still open to liability concerns and compliance issues under the securities laws of jurisdictions worldwide . . . .").

334. *See* Peter E. Millspaugh, *Global Securities Trading: The Question of a Watchdog*, 26 GEO. WASH. J. INT'L L. & ECON. 355, 370 (1992) ("Ironically, the assimilation of modern technology could well be creating a new vulnerability to ever more sophisticated forms of securities fraud.").

short arms of national securities regulators or police."[335] Because global developments and Internet developments present very similar sorts of jurisdictional and enforcement considerations,[336] this Part will briefly discuss the evolution of SEC enforcement of insider trading rules in the global marketplace, and then address the implications of extension of those enforcement efforts into cyberspace.

B. SEC Insider Trading Enforcement in the Global Marketplace

Liquidity considerations have led to great increases in secondary market trading activity outside investors' home countries.[337] Not surprisingly, foreign investors have traded in U.S. securities while possessing nonpublic inside information.[338] Also, in conscious attempts to evade SEC detection and punishment, U.S. residents have traded U.S. stocks through foreign accounts based on nonpublic inside information.[339] Not content to allow these evasions of U.S. insider trading rules, the SEC has sought aggressively to enforce, internationally, Section 10(b)/Rule 10b-5 and related rules regarding insider trading and other forms of securities fraud.[340]

---

335. Diane Francis, *Lies & Rumors*, TORONTO SUN, Mar. 25, 1997, at 12.

336. *See* Brakebill, *supra* note 1, at 910 ("A distinctive feature of cyberspace is that it is an international medium.").

337. *See* Uri Geiger, *Harmonization of Securities Disclosure Rules in the Global Market — A Proposal*, 66 FORDHAM L. REV. 1785, 1786 (1998) (citing numbers); Charles Vaughn Baltic, III, Note, *The Next Step in Insider Trading Regulation: International Cooperative Efforts in the Global Securities Market*, 23 LAW & POL'Y INT'L BUS. 167, 170 (1991–92) (citing numbers).

338. *See, e.g.*, SEC v. Certain Purchasers of the Call Options of Duracell Int'l, Inc., No. 96 Civ. 7017, 1996 U.S. Dist. LEXIS 14425 (S.D.N.Y. Oct. 2, 1996) (unknown investors, some apparently from Italy, traded Duracell options anonymously through institutions in Switzerland and the Bahamas); SEC v. Traboulsi, Litig. Release No. 15,429, 65 SEC Docket 332 (Aug. 4, 1997) (residents of Lebanon and France, through accounts in Switzerland and the British West Indies, traded in stocks of Delaware corporation).

The SEC received almost 600 referrals about suspected insider trading from U.S. stock exchanges in 1986 and 1987. Of those, more than one-third included one or more suspicious trades executed through foreign institutions. *See* GENERAL ACCOUNTING OFFICE, SECURITIES REGULATION: EFFORTS TO DETECT, INVESTIGATE, AND DETER INSIDER TRADING, GAO/GGD-88-116, at 49 (1988).

339. *See, e.g.*, Redtail Leasing, Inc. v. Bellezza, No. 95 Civ. 5191, 1997 U.S. Dist. LEXIS 1685 (S.D.N.Y. Feb. 19, 1997) (law firm employee misappropriated information and tipped confederates who traded through accounts in Europe); SEC v. Dabah, Litig. Release No. 15,189, 63 S.E.C. 1125 (Dec. 18, 1996) (insiders of Gitano Group, Inc. traded through accounts at banks in Luxembourg and Switzerland).

340. *See* Roberta S. Karmel, *Changing Concepts of Extraterritoriality*, N.Y. L.J., Jan.

To effectuate its global enforcement program, the SEC must overcome three primary roadblocks. First, U.S. courts must have subject matter jurisdiction over cases. Second, U.S. courts must be able to exercise personal jurisdiction over defendants. Third, the SEC must be able to investigate and enforce the rules effectively. The SEC has largely solved these three problems in the global context.

30, 1998, at 3 [hereinafter Karmel, *Changing Concepts*] ("In antifraud cases the SEC generally has advocated the broadest possible coverage in order to protect U.S. investors and U.S. markets."). A full-fledged examination of whether such aggressive enforcement is wise or not is beyond the scope of this Article. I do generally favor aggressive enforcement, especially in the case of fraudulent acts, such as insider trading. This is no minor matter; one estimate is that in 1988 alone, when cross-border trading was just a fraction of what it is today, investors lost more than $5 billion as a result of illegal international securities transactions. *See The SEC's New World Role*, ECONOMIST, Jan. 6, 1990, at 73 (estimating loss to Americans at $1.6 billion).

Both courts, *see, e.g.*, Consolidated Gold Fields PLC v. Minorco, S.A., 871 F.2d 252, 262–63 (2d Cir. 1989), and the Restatement (Third) on Foreign Relations Law of the United States, *see* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 416 cmt. a (1987) [hereinafter RESTATEMENT (THIRD)], seem to agree that the United States has a stronger legitimate interest in applying extraterritorially its antifraud provisions than its simple disclosure requirements. However, Professor Fisch has pointed out a problem in that Section 10(b) fraud liability is based in significant part upon particular SEC disclosure rules and, in the case of the misappropriation theory, upon state common law doctrines. *See* Jill E. Fisch, *Imprudent Power: Reconsidering U.S. Regulation of Foreign Tender Offers*, 87 NW. U. L. REV. 523, 560 (1993) [hereinafter Fisch, *Imprudent Power*].

1. Subject Matter Jurisdiction

Over the years, the SEC has tried to export U.S. securities law[341] much as American high-tech companies have sought to export computer hardware and software.[342] The SEC has generally taken the view that jurisdiction is a legal rather than a geographical concept.[343] U.S. courts have acceded to the application of two different jurisdictional tests; satisfaction of either will suffice to establish subject matter jurisdiction under Section 10(b)/Rule 10b-5 in insider trading and other securities fraud cases.

First is the "conduct" test, which proceeds under the theory that Congress, although it did not specify the extent of the extraterritorial reach of federal securities law, would not have wanted the United States to serve as a base for the export of fraudulent conduct. Therefore, if fraudulent acts, such as insider trading, occur in the United States and

---

341. Private plaintiffs in securities fraud suits have also pushed the jurisdictional envelope to the extent possible. *See, e.g.*, Butte Mining PLC v. Smith, 76 F.3d 287, 288–89 (9th Cir. 1996) (finding no subject matter jurisdiction in United States because acts in United States were "merely preparatory" to alleged fraud and no effects in United States were alleged); Itoba Ltd. v. LEP Group PLC, 54 F.3d 118, 120–24 (2d Cir. 1995) (finding jurisdiction based on both conduct and effects tests); Grunenthal GmbH v. Hotz, 712 F.2d 421, 425 (9th Cir. 1983) (finding jurisdiction over dispute involving only foreign parties based on single contact with Los Angeles); Continental Grain (Australia) Pty. Ltd. v. Pacific Oilseeds, Inc., 592 F.2d 409, 414–16 (8th Cir. 1979) (holding that conduct in United States that was "essential link" to impact in Australia provided basis for subject matter jurisdiction); Bersch v. Drexel Firestone, Inc., 519 F.2d 974, 993 (2d Cir. 1975) (setting up three-tiered approach with very broad jurisdictional reach if Americans resident in United States were victims or if conduct occurring in United States contributed to the fraud, but no jurisdiction over losses to foreigners living outside United States unless conduct within United States directly caused the losses); Leasco Data Processing Equip. Corp. v. Maxwell, 468 F.2d 1326, 1333 (2d Cir. 1972) (holding that fraudulent conduct in United States conferred subject matter jurisdiction even though parties were foreign citizens and shares involved were not listed on U.S. exchange); Schoenbaum v. Firstbrook, 405 F.2d 200, 206 (2d Cir.), *rev'd on other grounds*, 405 F.2d 215 (2d Cir. 1968) (en banc) (holding that insider trading that occurred in Canada between Canadian corporations was subject to U.S. jurisdiction because stock was registered on U.S. exchanges and activities were "detrimental to the interests of American investors"); Department of Econ. Dev. v. Arthur Andersen & Co., 683 F. Supp. 1463, 1470–71 (S.D.N.Y. 1988) (finding jurisdiction in United States over audit done in Ireland because ultimate responsibility lay in defendant's U.S. office).

342. Although the SEC is the most aggressive enforcer of securities laws across national borders, most nations' insider trading laws purport to have extraterritorial application. *See* Conrad Raj, *MAS May Change Laws to Allow Cross-Border Probes*, BUS. TIMES (Singapore), Feb. 26, 1998, at 1 (noting that Singapore's insider trading laws, unlike those of most other nations, have no extra-territorial jurisdiction).

343. *See* Karmel, *Changing Concepts*, *supra* note 340, at 3 (surveying case law).

directly cause harm elsewhere, foreign citizens as well as Americans living abroad can bring suit in U.S. courts under Section 10(b)/Rule 10b-5. The SEC can also hale such wrongdoers into U.S. courts to impose, at a minimum, civil penalties.

Second is the "effects" test, under which fraudulent acts occurring abroad can be the basis of Section 10(b)/Rule 10b-5 actions in the United States if they substantially injure U.S. investors or markets in the United States. In one leading case, the Second Circuit opined that "Congress intended the Exchange Act to have extraterritorial application in order to protect domestic investors who have purchased foreign securities on U.S. exchanges and to protect the domestic securities market from the effects of improper foreign transactions in U.S. securities."[344]

These two jurisdictional approaches,[345] applied together, have transformed Section 10(b)/Rule 10b-5 into a broad protective layer sheltering from fraud and compensating not only foreign investors buying U.S. securities but also U.S. investors injured by foreign frauds.[346] Broad application of U.S. subject matter jurisdiction in Section 10(b)/Rule 10b-5 cases has been harshly criticized,[347] but courts

---

344. *Schoenbaum*, 405 F.2d at 206.

345. These two jurisdictional approaches were based roughly on sections 17 and 18 of the Restatement (Second) of the Foreign Relations Law of the United States. *See* Ronald E. Bornstein & N. Elaine Dugger, *International Regulation of Insider Trading*, 1987 COLUM. BUS. L. REV. 375, 400–02 (describing these provisions).

346. *See, e.g.*, Robinson v. TCI/U.S. West Communications, Inc., 117 F.3d 900, 907 (5th Cir. 1997) (allowing U.K. citizen and resident to sue in United States based on allegations that fraudulent scheme was directed from Colorado); *Butte Mining*, 76 F.3d at 290–91 (spelling out bases for jurisdiction but ultimately finding that neither effects nor conduct test was satisfied); *Itoba*, 54 F.3d at 121–25 (finding jurisdiction based on combination of effects and conduct test); Alfadda v. Fenn, 935 F.2d 475, 479 (2d Cir. 1991) (finding jurisdiction over claims by foreign investors).

347. For example, Choi and Guzman have recently argued that countries should regulate only territorially, not extraterritorially. This, they believe, could lead to regulatory competition among countries that would ultimately shake out into a separating equilibrium (rather than a "race to the top" or "race to the bottom") of legal regimes. *See* Stephen J. Choi & Andrew T. Guzman, *National Laws, International Money: Regulation in a Global Capital Market*, 65 FORDHAM L. REV. 1855 (1997) [hereinafter Choi & Guzman, *National Laws*]; *see also* Stephen J. Choi & Andrew T. Guzman, *Portable Reciprocity: Rethinking the International Reach of Securities Regulation*, 71 S. CAL. L. REV. 903 (1998) (extending their argument). For many aspects of securities regulation, such as disclosure requirements, this is a plausible argument. However, it remains unclear how the global financial markets are better off with varying degrees of insider trading occurring around the globe rather than with *no* insider trading occurring.

On the other hand, some commentators have been quite supportive of broad efforts to enforce U.S. antifraud securities provisions. *See* Edward F. Greene et al., *Toward a*

have generally defended it as consistent with international law. It is also generally consistent with the Restatement (Third) of Foreign Relations Law of the United States.[348]

2. Personal Jurisdiction

In order to enforce U.S. securities laws against frauds occurring abroad, U.S. courts must be able to exercise personal jurisdiction properly over the defendants. This is not a problem when the defendants are U.S. citizens who are using foreign securities exchanges in an attempt to evade detection or application of U.S. laws. However, establishing personal jurisdiction over foreign citizens in U.S. courts can be more problematic.[349]

Courts have settled that the Exchange Act permits the exercise of personal jurisdiction to the limits of the Due Process Clause.[350] The due process requirement, according to hornbook law, is not met unless

---

Cohesive International Approach to Cross-Border Takeover Regulation, 51 U. MIAMI L. REV. 823 (1997) (supporting aggressive assertion of antifraud rules even in prickly context of cross-border takeover battles).

The Australian Securities Commission ("ASC") has taken the position that raising global electronic capital may well create a "race to the bottom" as entities seeking to raise capital migrate toward the regimes with the least stringent regulation. In response, the ASC has declared that it will "strive to maintain its high regulatory standards, and encourage other securities and market regulators to avoid the 'lowest common denominator approach' to regulation." AUSTRALIAN SECURITIES COMMISSION, *supra* note 10, at 215–16; *see also* Merritt B. Fox, *Securities Disclosure in a Globalizing Market: Who Should Regulate Whom?*, 95 MICH. L. REV. 2501, 2585 (1997) [hereinafter Fox, *Securities Disclosure*] (expressing related "race to the bottom" concerns).

348. The Restatement (Third) added a reasonableness requirement, which instructs courts to "consider various interests, examine contacts and links, give effect to justified expectations, search for the 'center of gravity' of a given situation and develop priorities." RESTATEMENT (THIRD), *supra* note 340, pt. IV, ch. 1, introductory note. For a general discussion of the "reasonableness" requirement, see David Michaels, Note, *Subject Matter Jurisdiction Over Transnational Securities Fraud: A Suggested Roadmap to the New Standard of Reasonableness*, 71 CORNELL L. REV. 919 (1986).

The Restatement (Third) also contains a specific provision, section 416, dealing with securities regulation. That provision sanctions an extremely broad extraterritorial application of U.S. securities laws. *See generally* Testy, *supra* note 324, at 936–37 (discussing and criticizing such provisions).

349. This discussion focuses on the SEC's attempts to impose *civil* sanctions on insider trading. In criminal cases, personal jurisdiction simply depends upon the presence of the defendant in the forum jurisdiction. *See generally* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 35–36 (1996).

350. *See* SEC v. Unifund SAL, 910 F.2d 1028, 1033 (2d Cir. 1990); Leasco Data Processing Equip. Corp. v. Maxwell, 468 F.2d 1326, 1339 (2d Cir. 1972).

(1) the defendant has directed sufficient "minimum contacts" toward the forum jurisdiction, and (2) assertion of jurisdiction over the defendant would satisfy considerations of fair play and substantial justice.[351] What constitutes "sufficient minimum contacts" has been widely litigated, if not clearly settled, in the domestic context. International cases have been more troublesome.

The SEC has been aggressive in asserting the existence of personal jurisdiction over foreign defendants in securities fraud cases.[352] The SEC has received substantial assistance from the courts. Consider the recent case of *SEC v. Carrillo*.[353] The targets of the action were a Costa Rican corporation and Costa Rican citizens domiciled in Costa Rica who were officers of the corporation. The defendants had placed advertisements promoting the defendant corporation's securities in the complimentary in-flight magazines of American Airlines and Lacsa Airlines. They had also (1) via telephone arranged for a Florida free lance writer to pen two favorable articles which would later be published in Lacsa's in-flight magazine, (2) mailed offering materials and application forms directly to U.S. investors, (3) maintained bank accounts in Miami to receive payments from investors, and (4) mailed at least one stock certificate to a U.S. investor. The trial court dismissed the action for lack of personal jurisdiction, but the Eleventh Circuit reversed, holding that the acts were clearly related to the cause of action (securities fraud and selling unregistered securities), constituted a purposeful availment of the privilege and benefits of conducting activities in the forum, and gave rise to a reasonable expectation by the defendants that they could be haled into U.S. courts to answer for their misdeeds.[354]

In *SEC v. Knowles*,[355] the Tenth Circuit upheld personal jurisdiction over a Bahamian citizen based on his contacts with the United States, noting the distinction between specific personal jurisdiction and general

---

351. *See generally* Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102 (1987); Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980); Shaffer v. Heitner, 433 U.S. 186 (1977); International Shoe Co. v. Washington, 326 U.S. 310 (1945).

352. *See* James R. Doty, *The Role of the Securities and Exchange Commission in an Internationalized Marketplace*, 60 FORDHAM L. REV. S77, S82 (1992) (noting that SEC general counsel stated, although supposedly in a private capacity, that the ability to establish broad jurisdiction in securities fraud cases is "crucial to the [SEC's] ability to bring enforcement actions to protect United States markets and United States investors").

353. 115 F.3d 1540 (11th Cir. 1997).

354. *See id.* at 1542–45.

355. 87 F.3d 413 (10th Cir. 1996).

personal jurisdiction,[356] and noting in passing that even à single purposeful contact may be sufficient to meet the "minimum contacts" requirement if the suit arises directly out of that contact.[357]

In the insider trading case *SEC v. Unifund SAL*,[358] the defendants included Lebanese and Panamanian investment companies who, through Swiss banks and a Swiss branch of Dean Witter Reynolds, Inc., (1) bought stock, over the NYSE, of an American company involved in merger negotiations with a French firm, and (2) purchased options, over the American Stock Exchange, in that company. The defendants' motion to dismiss for lack of personal jurisdiction was denied. The court stated in part:

> Not every securities law violation involving shares of a United States corporation will have the requisite effect within the United States. Insider trading, however, has serious effects that can reasonably be expected to be visited upon United States shareholders where, as here, the securities are those of a United States company traded exclusively on a United States exchange.[359]

Thus, an inside trader, whether or not a citizen or resident of the United States, who uses international securities facilities to engage in insider trading in securities traded on U.S. exchanges is generally subject to the personal jurisdiction of U.S. courts, whether pursuant to the traditional "minimum contacts" analysis or the Restatement's "reasonableness" approach more generally consistent with international law.[360] Under either approach, the intent purposefully to engage in

---

356. Specific personal jurisdiction is based upon the defendant's purposeful contacts with the forum jurisdiction. When a lawsuit arises out of such contacts, relatively few contacts are needed to establish personal jurisdiction. *See, e.g.*, *Burger King*, 471 U.S. at 472. If the lawsuit arises out of actions occurring outside the forum jurisdiction, a court will hale the defendant into the forum only if she is subject to general personal jurisdiction. In such cases, the plaintiff must show that the defendant had "continuous and systematic" contacts with the forum jurisdiction in order to establish personal jurisdiction. *See, e.g.*, Helicopteros Nacionales de Colombia v. Hall, 466 U.S. 408, 415 (1984).

357. *See Knowles*, 87 F.3d at 419 (citing McGee v. International Life Ins. Co., 355 U.S. 220, 223 (1957)).

358. 910 F.2d 1028 (2d Cir. 1990).

359. *Id.* at 1033.

360. According to the Restatement (Third), a state's exercise of jurisdiction to adjudicate will usually be deemed reasonable if, at the time it is asserted:

conduct that will violate U.S. laws and have an adverse effect on U.S. securities markets provides an ample basis for the assertion of personal jurisdiction.

3. Investigation and Enforcement

The ability to establish subject matter and personal jurisdiction in U.S. courts is of little use if the SEC cannot investigate and take enforcement action against inside traders operating abroad. In at least two different ways the SEC has gone about solving the many problems presented by international considerations, such as differences in law, culture, and legal systems. First, it has convinced many foreign countries to assist SEC investigations of violations of U.S. securities laws by offering reciprocal assistance.[361] Second, it has spearheaded a

---

(a) the person or thing is present in the territory of the state, other than transitorily;
(b) the person, if a natural person, is domiciled in the state;
(c) the person, if a natural person, is resident in the state;
(d) the person, if a natural person, is a national in the state;
(e) the person, if a corporation or comparable juridical person, is organized pursuant to the law of the state;
(f) a ship, aircraft or other vehicle to which adjudication relates is registered under the laws of the state;
(g) the person, whether natural or juridical, has consented to the exercise of jurisdiction;
(h) the person, whether natural or juridical, regularly carries on business in the state;
(i) the person, whether natural or juridical, had carried on activity in the state, but only in respect of such activity;
(j) the person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity; or
(k) the thing that is the subject of adjudication is owned, possessed, or used in the state, but only in respect of a claim reasonably connected with that thing.

RESTATEMENT (THIRD), *supra* note 340, § 421(2).

361. Congress has boosted the SEC's efforts in this area in at least two specific ways. First, Congress passed ITSFEA, which contained an authorization for the SEC to join the International Organization of Securities Commissions ("IOSCO") and to cooperate with foreign securities regulators seeking information within the grasp of the SEC. *See supra* note 175. The House Report indicated that a main goal of the provision was to secure reciprocal cooperation from foreign governments when the SEC was seeking evidence located abroad in the course of one of its investigations. *See* H.R. REP. NO. 100-910, at 39 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6076. Second, Congress passed the International Securities Enforcement Cooperation Act of 1990 ("ISECA"), Pub. L. No.

successful movement to make insider trading an internationally-recognized offense so that other countries can enforce their own laws to stop the type of fraud the SEC condemns.

a. MOUs and More

Slightly more than a decade ago, the SEC faced daunting challenges in trying to enforce U.S. insider trading laws when foreign activity was involved. The most tangible problem lay in blocking and privacy statutes that made it extremely difficult for the SEC to investigate violations,[362] even if there were strong reasons to believe that personal and subject matter jurisdiction could be established in U.S. courts.[363] Traditional methods of gathering evidence, such as letters rogatory[364] or proceedings under the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters,[365] were insufficient.

Over the past ten to fifteen years, however, the SEC has made tremendous strides in overcoming these barriers. Of primary significance, perhaps, was its success in negotiating with Switzerland some realistic limitations on the famed Swiss bank secrecy laws.[366] Although there remain a small number of jurisdictions intent on

---

101-550, 104 Stat. 2714 (codified as amended at 15 U.S.C. §§ 77uuu, 78a, 80a-45, 80b-18 (1994)), the purpose of which was to "enhance the [SEC's] ability . . . to prevent and detect violations of U.S. securities laws that are committed at least in part abroad and whose investigation may require the [SEC] to obtain substantial foreign-based evidence." H.R. REP. NO. 101-240, at 2, 20–23 (1990), *reprinted in* 1990 U.S.C.C.A.N. 3888, 3889, 3907–10.

362. *See generally* Dora L. McNew, *Blocking Laws and Secrecy Provisions: Do International Negotiations Concerning Insider Trading Provide a Solution to Conflicts in Discovery Rules*, 26 CAL. W. L. REV. 103, 104–05 (1989–90) (describing such laws and the motivation that inside traders have to hide behind them); Jill Elizabeth Asch, Note, *Bank Secrecy: A Barrier to the Prosecution of Insider Trading*, 4 EMORY INT'L L. REV. 185 (1990) (describing how such laws operate in Switzerland and other nations).

363. *See* Bornstein & Dugger, *supra* note 345, at 412–13 (describing limits of SEC's unilateral subpoena power in extraterritorial cases); Pamela Jimenez, Note, *International Securities Enforcement Cooperation Act and Memoranda of Understanding*, 31 HARV. INT'L L.J. 295, 296 (1990) (same).

364. A letter rogatory is "[a] request by a court made of a foreign court in writing to secure the aid of the foreign court, backed by its power, in obtaining desired information in the form of a deposition by a person within the jurisdiction of the foreign court or to obtain the production of a record within the jurisdiction of such court." BALLENTINE'S LAW DICTIONARY 726 (3d ed. 1969).

365. *Opened for signature* Mar. 18, 1970, 23 U.S.T. 2555, 84 U.N.T.S. 231.

366. *See generally* Catherine F. Donohue, Note, *Swiss Law Prohibiting Insider Trading: Its Impact on Switzerland and the United States*, 16 BROOK. J. INT'L L. 382, 389–91 (1990).

establishing a level of privacy protection that provides comfort for scalawags on the international securities markets,[367] a large number of nations have begun large-scale mutual cooperation with the SEC for securities law enforcement.

Much of the progress has been made through negotiation of Memoranda of Understanding ("MOUs"), cooperative agreements under which nations pledge mutual support in the enforcement of insider trading and other securities laws. These agreements are not binding, but the parties generally live up to them. For example, in 1982 and 1987 the SEC entered into MOUs with Switzerland that served as models for MOUs later negotiated with many other countries. The MOU of 1982 clearly recognized that both nations had an interest in cooperating on insider trading investigations and balancing the needs of such investigations with Swiss bank secrecy policies.[368] The MOU of 1987 was designed to improve the exchange of information between the United States and Switzerland in the investigation of insider trading and other crimes.[369]

In the past decade or so, these MOUs have multiplied to more than thirty[370] and have become an effective addition to the SEC arsenal of weaponry to attack international insider trading,[371] especially because they often serve as a precursor to binding bilateral treaties.[372] A key

---

367. *See* Millspaugh, *supra* note 334, at 363 n.58 (1992) (citing Liechtenstein, Monaco, Luxembourg, and the Cayman Islands as examples).

368. *See* Memorandum of Understanding to Establish Mutually Acceptable Means for Improving International Law Enforcement in the Field of Insider Trading, Aug. 31, 1982, U.S.-Switz., 22 I.L.M. 1.

369. *See* Memorandum of Understanding on Mutual Assistance in Criminal Matters and Ancillary Administrative Proceedings, Nov. 10, 1987, U.S.-Switz., 27 I.L.M. 480.

370. *See* Greene et al., *supra* note 347, at 866. The IOSCO website contains a listing of virtually all international MOUs in the securities law field. *See* IOSCO, *An Index of Memoranda of Understanding and Similar Agreements Between IOSCO Members* (visited Feb. 9, 1999) <http://www.iosco.org/mou/mou01.html>.

371. *See* Michael D. Mann & Lise A. Lustgarten, *Internationalization of Insider Trading Enforcement: A Guide to Regulation and Cooperation*, *in* INTERNATIONAL SECURITIES MARKETS 1991, at 511, 534 (PLI Corp. Law & Practice Course Handbook Series No. B4-6967, 1991) (explaining advantages of MOUs for SEC, especially in improving working relationships with regulators in other nations); Elizabeth E. Barlow, Note, *Enforcing Securities Regulation Through Bilateral Agreements with the United Kingdom and Japan: An Interim Measure or a Solution?*, 23 TEX. INT'L L.J. 251, 268 (1988) ("Bilateral agreements . . . present the best option for the SEC."); Mark S. Klock, Comment, *A Comparative Analysis of Recent Accords Which Facilitate Transnational SEC Investigations of Insider Trading*, 11 MD. J. INT'L L. & TRADE 243, 265 (1987) (concluding that MOUs are preferable to unilateral U.S. action, which is resented by other nations, and to broad multinational action, which is not yet politically feasible).

372. *See* Kehoe, *supra* note 324, at 359–60.

example is the treaty between the United States and the United Kingdom expanding the power of the SEC to investigate insider trading traditionally shielded by the bank secrecy laws of the Cayman Islands.[373]

The United States has certainly been the leader in international efforts to break down barriers to cooperation in enforcement, but other groups have been active as well.[374] Additionally, the International Organization of Securities Commissions ("IOSCO"),[375] an organization consisting of 120 institutes from 70 countries around the world,[376] has studied enforcement issues carefully and endorsed a declaration requiring members "to provide assistance on a reciprocal basis in the gathering of information related to market oversight and protection of investors against fraudulent securities transactions."[377]

Even Professor Mahoney, who believes, for reasons mostly related to the concept of regulatory competition, that exchanges would be better regulators of the securities markets,[378] admits that when it comes to matters of regulating fraud, national governments will have to do the job, hopefully in a manner involving much international cooperation.[379] And

---

373. *See* Treaty Concerning the Cayman Islands and Mutual Legal Assistance in Criminal Matters, July 3, 1986, U.S.-U.K., 26 I.L.M. 536; *see also* Kehoe, *supra* note 324, at 365–69 (discussing strengths and limitations of this treaty as well as agreements with France and Netherlands).

374. *See* Millspaugh, *supra* note 334, at 375–76 (detailing other efforts, such as the Council of Europe's directives on insider trading and other regulatory matters, and European discussions about creating Interpol-like securities agency).

375. For a general background on IOSCO, see A.A. Sommer, Jr., *IOSCO: Its Mission and Achievement*, 17 NW. J. INT'L L. & BUS. 15 (1996).

376. *See Int'l Panel IOSC Plans Measures to Monitor Net Trading*, ASIA PULSE, Sept. 8, 1997 [hereinafter *Int'l Panel*] (reporting these numbers).

377. INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, 1990 ANNUAL REPORT 1. Millspaugh points out that IOSCO has also been coordinating its efforts with private securities industry organizations, such as the International Federation of Stock Exchanges. *See* Millspaugh, *supra* note 334, at 371.

378. *See* Paul G. Mahoney, *The Exchange as Regulator*, 83 VA. L. REV. 1453, 1454 (1997) [hereinafter Mahoney, *Exchange as Regulator*].

Professor Taylor has similarly argued that "[t]he once exclusive, inviolable nature of sovereignty has little relevance in an interdependent, technologically connected world." Celia R. Taylor, *A Modest Proposal: Statehood and Sovereignty in a Global Age*, 18 U. PA. J. INT'L ECON. L. 745, 808 (1997). She believes that nonstate players must play a greater role in the global age and that concepts of sovereignty and statehood must be de-emphasized.

379. *See* Mahoney, *Exchange as Regulator*, *supra* note 378, at 1499.

> It is not a substantial defect in exchange regulation that exchanges require governmental assistance to deter fraud. Even national governments — to say nothing of state governments — cannot single-handedly punish fraudulent conduct that occurs

Choi and Guzman, who generally oppose international cooperation in securities regulation, agree that the national (territorial) regulation that they do favor should be effectuated via agreements among nations that encourage the sharing of information and effective enforcement of national securities laws.[380]

b. Outlawing Insider Trading

Twenty years ago, the United States stood largely alone in its determination to regulate insider trading aggressively. No matter how many MOUs are negotiated, the SEC will have difficulty making a dent in cross-border insider trading if it is the only agency interested in pursuing that agenda. However, due in at least some measure to U.S. pressure,[381] many nations around the world have either enacted more stringent rules against insider trading, stiffened their enforcement resolve, or both.[382]

> within or has effects within their borders. Securities and their salesmen are highly mobile and those who engage in fraud can often put themselves beyond the reach of the regulator whose rules they have broken before the regulator can detect the violation. The detection and punishment of fraud, therefore, presents a compelling case for interjurisdictional cooperation. The growing tendency of governmental regulators to enter into agreements to cooperate in enforcing each other's rules against fraud is therefore sensible.

Id.

Professor Kahan, who has offered some trenchant criticism of Mahoney's thesis that exchanges could be better regulators than governments, clearly agrees that governments would be better at sanctioning fraudulent activity such as insider trading. *See* Marcel Kahan, *Some Problems with Stock Exchange-Based Securities Regulation*, 83 VA. L. REV. 1509, 1517 (1997).

380. *See* Choi & Guzman, *National Laws*, *supra* note 347, at 1899.

381. The SEC believes that it has a responsibility to be the world leader in international securities regulation and in that role has called for global uniformity in securities laws and regulation, especially in the insider trading realm. *See* Paul G. Mahoney, *Securities Regulation by Enforcement: An International Perspective*, 7 YALE J. ON REG. 305, 312, 320 (1990) [hereinafter Mahoney, *Regulation by Enforcement*].

382. *See generally* Raffaello Fornasier, *The Directive on Insider Trading*, 13 FORDHAM INT'L L.J. 149 (1989–90) (describing and analyzing EU directive on insider trading); H. Fenwick Huss & Burt A. Leete, *Insider Trading Regulations: A Comparison of Judicial and Statutory Sanctions*, 25 AM. BUS. L.J. 301, 313 (1987) (describing 1980 and 1985 U.K. enactments); Theodore A. Levine & W. Hardy Callcott, *The SEC and Foreign Policy: The International Securities Enforcement Cooperation Act of 1988*, 17 SEC. REG. L.J. 115, 123 (1989) ("The SEC raised foreign consciousness about the harmful effects of insider trading, and this directly led to legislation criminalizing insider trading or increasing enforcement in countries such as Switzerland, Japan, Canada, and England."); Harvey L. Pitt & David B. Hardison, *Games Without Frontiers: Trends in*

International cooperation in the battle against insider trading has also been a priority of IOSCO.[383] Largely at the prompting of the United States, a May 1996 IOSCO meeting resulted in an agreement by international securities regulators to establish insider trading as one of five targeted criminal securities activities, enabling states to cooperate and not become havens for illegal activity.[384] IOSCO also promulgated standards in order to stimulate the negotiation and implementation of MOUs. Between 1988 and 1996, the number of international MOUs quickly grew from just a few to more than 200.[385]

Many have urged the SEC to be cautious. Professor Fox, for example, has urged the SEC to allow foreign regulators to control foreign issuers even in tort cases.[386] Professor Karmel has urged the

---

the International Response to Insider Trading, 55 LAW & CONTEMP. PROBS. 199, 199 (1992) ("Virtually every country with a major stock market has adopted, or is actively considering, outlawing insider trading."); Donohue, *supra* note 366, at 382 (describing new Swiss insider trading law); John F. Imhof, Jr., Note, *The Pathology of Insider Trading and Japan's Amended Securities Exchange Law*, 16 SYRACUSE J. INT'L L. & COM. 247 (1990) (describing new Japanese provisions on insider trading, but expressing some skepticism as to how vigorously they would be enforced); Mann & Lustgarten, *supra* note 371, at 556 (describing new legislation in Netherlands making insider trading criminal offense).

In inducing so much of the developed world to adopt insider trading regulations comparable to those extant in the United States, the United States has seen a level of success comparable to its recent triumph in the field of commercial bribery. Approximately 20 years after passage of the Foreign Corrupt Practices Act, the United States finally saw its two decades of coaxing and hectoring come to fruition when the 29 members of the Organization for Economic Cooperation and Development and five other non-member states signed the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. *See* Stanley S. Arkin, *Bribery of Foreign Officials: Leveling the Playing Field*, N.Y. L.J., Feb. 19, 1998, at 3 (describing and analyzing Convention).

383. *See generally Polish Regulator to Hold Manipulation Seminar*, GLOBAL COMPLIANCE REP., Nov. 17, 1997, at 5 (reporting that Polish Securities Commission was holding seminar for all IOSCO members focusing on price manipulation, insider trading, and other market violations).

384. *See* William H. Lash III, *International Securities Regulations*, 31 INT'L L. 361, 364 (1997) (citing *Warsaw Meeting Focuses on "Common Offenses," Increasing Police Powers*, INT'L SEC. REG. REP., June 17, 1996)). The other four criminal activities are disseminating inaccurate information, divulging professional secrets, misleading clients, and manipulating the market. *See id.* This IOSCO action might be viewed as the first step toward a uniform international statute defining insider trading and operationalizing enforcement of the type proposed by Professor Salbu. *See* Steven R. Salbu, *Regulation of Insider Trading in a Global Marketplace: A Uniform Statutory Approach*, 66 TUL. L. REV. 837 (1992) [hereinafter Salbu, *Statutory Approach*].

385. *See* Sommer, *supra* note 375, at 28.

386. At the same time, Professor Fox would urge the SEC to impose its rules

SEC to avoid confrontations and conflicts with foreign regulators by sticking with a territorial approach to jurisdictional issues.[387] Professor Salbu has advocated harmonization through statutes.[388]

Because a true international securities enforcement organization is not a realistic possibility for the foreseeable future,[389] harmonization and cooperation are the most realistic approaches for the SEC to continue to take. Complete uniformity of rules, attitudes, enforcement resources, and commitment is years away, if attainable at all. Still, substantial uniformity has been achieved through a combination of aggressive SEC export of U.S. law,[390] cooperation and coordination with other nations in enforcement activities, and SEC initiatives to minimize differences among nations' regulatory systems.[391] As long ago as 1987, SEC Counsel Edward F. Greene stated that "[w]hat's beginning to come together is a perception that insider trading is wrong. We are evolving towards markets that look, act, feel, and smell the same worldwide. Market regulation is bound to converge."[392] It has. And in no field has the SEC been more successful at producing this convergence than in insider trading.[393] It is now possible to speak of an "emerging global

---

wherever transactions occurred, so long as U.S. issuers were involved. *See* Fox, *Securities Disclosure*, *supra* note 347, at 2505 (focusing primarily on disclosure issues rather than insider trading per se in concluding that United States "should apply its securities regime only to issuers of U.S. nationality, but do so regardless of the location of transactions in the issuer's shares and regardless of who the buyers are"); Merritt B. Fox, *Insider Trading in a Globalizing Market: Who Should Regulate What?*, 55 LAW & CONTEMP. PROB. 263, 297 (1992) ("For a number of reasons, the country that will [regulate insider trading in the fashion that most enhances global welfare] generally turns out to be the country of the issuer's nationality.").

387. *See* Karmel, *Changing Concepts*, *supra* note 340.

388. *See* Salbu, *Statutory Approach*, *supra* note 384.

389. *See* Millspaugh, *supra* note 334, at 376 ("For the 1990s, it is not realistic to expect the integrity of the global securities market to be policed by a fresh, new, powerful, and expert international regulatory body.").

390. One commentator has concluded that "the SEC's vigorous efforts to enforce insider trading has resulted in the globalization of U.S. insider trading laws." Kehoe, *supra* note 324, at 347–48.

391. *See* Regulation of International Securities Markets, Securities Act Release No. 6807, 53 Fed. Reg. 46,963 (Nov. 14, 1988).

392. *The Insider Trading Dragnet is Stretching Across the Globe*, BUS. WK., Mar. 23, 1987, at 56.

393. *See* Roberta Karmel, *Transnational Takeover Talk — Regulations Relating to Tender Offers and Insider Trading in the United States, the United Kingdom, Germany, and Australia*, 66 U. CIN. L. REV. 1133, 1177 (1998) (noting and generally supporting this SEC success); Amir N. Licht, *International Diversity in Securities Regulation: Roadblocks on the Way to Convergence*, 20 CARDOZO L. REV. 227, 233 (1998) (noting success of SEC and IOSCO efforts at creating international "convergence" of insider

consensus favor[ing] punish[ment of insider trading] activity because it undermines the integrity of the marketplace and threatens the market's efficiency."[394] In addition, to the extent that the SEC can induce other nations to implement American-style regulation, it can rely less and less on the aggressive export of U.S. laws that other nations have tended to find so irritating.[395]

C. SEC Insider Trading Enforcement in Cyberspace

As the preceding Section has indicated, policing insider trading in international markets is a complicated matter, fraught with both legal and practical problems. These problems multiply when the insider trading activity occurs over the Internet.[396] There is no doubt that information technology is restructuring the securities business worldwide.[397] Although the Internet's impact on U.S. securities markets promises to be profound, its impact on international markets may be even greater.[398]

---

trading regulation); Mahoney, *Regulation by Enforcement*, *supra* note 381, at 315.

394. Baltic, *supra* note 337, at 182; *see also* Pitt & Hardison, *supra* note 382, at 229 (speaking of "growing international consensus" that insider trading is unfair and must be prohibited and punished).

395. This success makes more feasible the basic approach of Regulation S, 17 C.F.R. § 230.901–.904 (1998), which couples a territorial approach (i.e., the United States is primarily concerned with what happens on U.S. soil) with principles of comity and cooperation with other nations. This approach has been applauded by those who object to expansive extraterritorial application of U.S. securities laws. *See* Testy, *supra* note 324, at 955–58. Similarly, in tender offer regulation the SEC has generally chosen to minimize application of U.S. laws in cases where only a small percentage of the shareholders of the involved firms were Americans. *See* International Tender and Exchange Offers, Securities Act Release No. 6897, 56 Fed. Reg. 27,582 (June 5, 1991). *See generally* Jean-Pierre R. Bourtin, Jr., *United States Regulation of Foreign Takeovers*, 70 TUL. L. REV. 1609 (1996) (citing this measure and others taken by SEC to minimize regulation of transnational takeovers, yet criticizing SEC for not having gone far enough in deregulatory direction); Fisch, *Imprudent Power*, *supra* note 340, at 423.

396. *See* Stephen J. Choi, *Gatekeepers and the Internet: Rethinking the Regulation of Small Business Capital Formation*, 2 J. SMALL & EMERGING BUS. L. 27, 40 (1998) ("[T]hrough the Internet, the possibility of transactions taking place across multiple jurisdictions is increased many times.").

397. *See* Brakebill, *supra* note 1, at 904 ("Information technology has had a substantial impact on the investment process and the marketplace in general.").

398. *See* Michael D. Mann, *Jurisdiction in Cyberspace: International Implications of Electronic Markets*, WALLSTREETLAWYER.COM, June 1997, at 24 ("Although electronic technology is changing the U.S. marketplace radically, it may have the most profound effect on the international markets.").

Therefore, like other domestic agencies, the SEC faces the question of how its enforcement efforts apply in cyberspace.[399]

Although the SEC has made various adjustments in its rules to accommodate Internet developments, such as promulgating guidelines as to how Internet websites may be used to solicit offshore securities transactions and foreign investors without being required to register under the 1933 Securities Act,[400] the SEC has made it clear, regarding anti-fraud and anti-manipulation activity, that it intends to continue pressing its authority to the limit of its jurisdictional power.[401] Furthermore, although the website directive stands as an example of SEC self-restraint, at the same time that directive was issued the SEC was considering new rules regarding Regulation S[402] and Rule 15a-6.[403] These new rules would move away from an earlier, limited territorial approach and expand jurisdictional reach.[404] At a practical level, the SEC was largely motivated to expand U.S. jurisdictional reach by its belief that the territorially-based approach had been abused by some issuers who used Regulation S as a guise for introducing unregistered securities into the United States.[405] At a broader policy level, the SEC's rationale for contemplating such a major change in approach was stated to be the "increasing internationalization of global securities markets, *the growing use of the Internet for securities transactions*, the further integration of the European and other markets through common currencies and regulatory treatments, and other recent and ongoing developments in the securities markets . . . ."[406]

---

399. Securities law is not the only area where such issues are arising. *See, e.g.*, Martin Flumenbaum & Brad S. Karp, *Second Circuit Review*, N.Y. L.J., Mar. 25, 1998, at 4 ("With the advent of the Internet and with companies broadly thrusting their '[trade]marks' into cyberspace, Lanham Act extraterritorial jurisdiction will be required to adapt.").

400. *See* Statement of the Commission Regarding Use of Internet Web Sites to Offer Securities, Solicit Securities Transactions or Advertise Investment Services Offshore, Securities Act Release No. 7516, 63 Fed. Reg. 14,806 (Mar. 23, 1998).

401. *See id.*

402. 17 C.F.R. § 230.901–.904 (1998).

403. 17 C.F.R. § 240.15a-6 (1998).

404. *See* Karmel, *Changing Concepts*, *supra* note 340, at 3 (explaining mechanics of proposed new rules).

405. The SEC has initiated many enforcement actions in response to abuses of Regulation S. *See, e.g.*, GFL Ultra Fund, Ltd., Admin. Proceeding Release No. 3-9333, 64 SEC Docket 1958 (June 18, 1997); Candies, Inc., Admin. Proceeding File No. 3-8953, 61 SEC Docket 758 (Feb. 21, 1996); United States v. Sung & Feher, Litig. Release No. 14,500, 59 SEC Docket 832 (May 15, 1995); SEC v. Softpoint, Inc., Litig. Release No. 14,480, 59 SEC Docket 426 (Apr. 27, 1995).

406. Offshore Offers and Sales, Securities Act Release No. 7392, 62 Fed. Reg. 9258,

The increasing execution of securities transactions through cyberspace multiplies the chances that the SEC will attempt to exert jurisdiction over what a foreign government might consider a purely domestic matter.[407] What this Section will demonstrate is that the same approach the SEC has taken to insider trading enforcement in the global marketplace — aggressive assertion of jurisdiction facilitated and tempered by MOUs and other forms of international cooperation — is also the most feasible approach to insider trading enforcement in cyberspace.

1. Cyberspace Implications for Subject Matter Jurisdiction

Is the Internet governable by traditional governmental units?[408] Should activities on the Internet be within the regulatory domain of any single nation (and therefore of all nations)? Many "netizens" take the position that the Internet generally is not so governable.[409] Many experts

---

9260 n.28 (Feb. 20, 1997) (emphasis added).

407. *See* A. Jared Silverman, *Cyberspace Offerings Raise Complex Compliance Issues*, N.J. L.J., Dec. 25, 1995, at 10; *see also id.* (noting that reverse situation might occur — foreign nations might attempt to impose jurisdiction on what might normally be viewed as purely U.S. transaction).

408. Dean Perritt has observed that "[t]he Internet is part of a revolution that is sweeping away old political and economic structures . . . [and] will reduce traditional state sovereignty, regardless of American policy." Henry H. Perritt, Jr., *Cyberspace and State Sovereignty*, 3 J. INT'L LEGAL STUD. 155, 203–04 (1997).

409. The most famous capsulation of this view comes from the Internet posting of former Grateful Dead lyricist John Perry Barlow:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

John Perry Barlow, *A Cyberspace Independence Declaration* (Feb. 9, 1996) <http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration>.

believe that the Internet should be largely self-governing,[410] or that, at the very least, it should have its own unique body of law.[411]

Similar positions have been taken regarding the more specific issue of securities activity on the Internet. One experienced securities attorney has stated:

> I question whether the [Securities and Exchange Commission] and the self-regulatory organizations have the right to regulate the Internet . . . . In essence, the Internet may be a super country or a parallel universe. We're dealing with a technology that at this point doesn't lend itself to traditional concepts and legal values. I think the Internet is not something that belongs to any one country.[412]

---

410. *See, e.g.*, David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378 (1996) (suggesting that self-regulating structures will arise in cyberspace that are better suited to regulate the Internet than traditional sovereignties); Henry H. Perritt, Jr., *President Clinton's National Information Infrastructure Initiative: Community Regained?*, 69 CHI.-KENT L. REV. 991, 997 (1994) (recommending that electronic communities create "their own legal systems, more or less independent of national systems of law, and from each other"); David Post, *The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521 (1998) (arguing that "settlement" of cyberspace may lead to creation of a-territorial governments); Eric J. McCarthy, Comment, *Networking in Cyberspace: Electronic Defamation and the Potential for International Forum Shopping*, 16 U. PA. J. INT'L BUS. L. 527, 566 (1995) ("[C]yberspace citizens should choose for themselves what type of regulation should govern their travels.").

411. *See, e.g.*, Johnson & Post, *supra* note 410, at 1378 (suggesting as a governing principle that we "conceiv[e] of Cyberspace as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world'").

412. *Regulatory Talk: Bill Singer*, FIN. NETNEWS, May 17, 1997 [hereinafter *Bill Singer*] (interview with broker-dealer attorney Bill Singer). More recently, Mr. Singer has argued that the SEC should keep its hands off alternative trading systems sprouting up on the Internet, arguing: "These alternative systems are innovation in their purest form. I wonder if the ultimate solution here would have been to allow some of the alternative trading systems to develop, far less hindered by regulation and be given the opportunity to prove their mettle." Bencivenga, *Solomonic Approach*, *supra* note 326, at 5 (internal quotation marks omitted) (quoting Singer).

However, serious commentators disagree.[413] People who use the Internet to engage in insider trading are real people whose actions have real consequences in the real world. Those consequences, most commentators believe, justify governmental regulation. Perhaps more relevant, most governments also believe that regulation is warranted. Many local and national governmental entities not only want to regulate cyberspace, but are already doing so and will continue to do so.[414] This is true in the securities area as well as many others.[415]

---

413. *See, e.g.*, William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 WAKE FOREST L. REV. 197, 199 (1995) (noting that although cyberspace is without physical walls or dimensions, "it cannot exist independently of the real world"); Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423 (1998) (suggesting that the Internet may strengthen rather than undermine sovereignty of national states); Steven R. Salbu, *Who Should Govern the Internet? Monitoring and Supporting a New Frontier*, 11 HARV. J.L. & TECH. 429 (1998) [hereinafter Salbu, *Who Should Govern*] (recognizing need for legal regulation of Internet activities and suggesting guidelines for dividing federal and state jurisdiction); Stephen Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 124 (1997) ("[I]t is hard to maintain that the Net is some kind of free city in the sky."); Richard S. Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L.J. SCI. & TECH. 339, 347 (1996) ("The term cyberspace should properly be thought of as a communication medium through which real persons do real things. Cyber-activity is not above the law, nor should it be."); Erick J. Heels & Richard P. Klau, *Let's Make a Few Things Perfectly Clear: Cyberspace, the Internet, and that Superhighway*, STUDENT LAW., May 1995, at 17 ("Never forget that the Internet is simply a bunch of interconnected wires, with computers at the ends of the wires, and with people in front of the computers.").

Even those who oppose national enforcement of securities rules for cases involving Internet activities admit that "a fraudulent message on the Internet can literally reach millions of people in a split second. The Internet has the capacity to spread the securities industry version of the Ebola virus — fraud — all over the world. We have to address this on an international basis. The Internet is almost forcing the creation of some form of international Securities and Exchange Act." *Bill Singer*, *supra* note 412.

414. *See* Wilske & Schiller, *supra* note 413, at 174–75 (noting many examples of current efforts to regulate the Internet and concluding "there is little hope that States will respect the 'independence of cyberspace'"); Amy Knoll, Comment, *Any Which Way but Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275, 299 (1996) (giving examples of current regulation and concluding that "[i]t is unlikely that any government is going to relinquish any of its authority simply because new media have developed or, in the case of the Internet, expanded and popularized").

A leading example of this assertion of authority is Minnesota's efforts to regulate Internet gambling. *See, e.g.*, Pat Doyle, *Ruling Leaves Question of Web Gambling's Legality Unanswered*, STAR TRIB. (Minneapolis), May 12, 1998, at 1A.

415. *See, e.g.*, Alan Cameron, *Regulating the Marketspace: The ASC's Experience* (1997), *reprinted in* SECURITIES IN THE ELECTRONIC AGE, *supra* note 10, at 175, 176

There is no doubt that these efforts to regulate securities trading and other activities in cyberspace create major jurisdictional questions that are potentially more serious than those created by mere international transactions over more established facilities.[416] Importantly, "there is no settled law that deals with the assertion of jurisdiction over electronic markets for securities transactions."[417] And some have questioned whether jurisdictional expansion is "feasible or advisable in today's cyberspace markets."[418]

Although the federal securities statutes arguably indicate that Congress wished some degree of application to transnational securities markets,[419] there is no such direct guidance regarding such markets in cyberspace. Still, there is no reason to believe that Congress would wish that someone accessing the Internet from inside the United States should be able to commit securities fraud injuring investors abroad with impunity. Nor would Congress wish to allow persons accessing the Internet in foreign nations to be able to damage the integrity of U.S. securities markets with impunity. Therefore, the SEC's determination to regulate insider trading and other securities fraud in cyberspace is well justified and even consistent with international law.

(noting argument by chair of ASC that "there is no case for putting cyberspace above the law just because it is a new medium"); INVESTMENT MANAGEMENT REGULATORY ORGANISATION, THE INTERNET (1997), *reprinted in* SECURITIES IN THE ELECTRONIC AGE, *supra* note 10, at 263, 267 (taking position that any Internet advertisement "accessible on screen in the UK [is] within the UK regulatory scheme").

416. *See* Mann, *supra* note 398, at 24.

> [F]rom the regulator's perspective, electronic markets pose the greatest challenge to their ability to assert effectively and enforce jurisdiction. While the development of electronic markets has made every market international in nature, each market remains governed by domestic law. So, as information, trading, and money move seamlessly across borders, they may, or may not, implicate the legal jurisdiction of the country upon whose border they cross.

Id.

417. *Id.*

418. Karmel, *Changing Concepts*, *supra* note 340, at 3.

419. For example, in both the Securities Act of 1933 and the Securities Exchange Act of 1934, the rules apply to securities transactions occurring in or affecting interstate commerce, and both Acts define "interstate commerce" to include transportation or communication among the states and between any state and any foreign country. *See* 15 U.S.C. §§ 77(b)(7), 78c(a)(7) (1994). Furthermore, as noted above, *see supra* note 361, Congress has twice in recent years acted to facilitate SEC efforts to enforce securities laws extraterritorially. This should be enough evidence to overcome the normal presumption against extraterritorial application of U.S. laws. *See* United States v. Arab Am. Oil Co., 499 U.S. 244 (1991).

A strong argument can be made that under international law, the United States will have "jurisdiction to prescribe," and U.S. courts will consequently be justified in exercising subject matter jurisdiction, when there is compliance with the Restatement (Third) of Foreign Relations Law of the United States.[420] Subject to the requirement of

---

420. *See* RESTATEMENT (THIRD), *supra* note 340, §§ 402–03. Regarding jurisdiction to prescribe, the keys are sections 402 and 403. Section 402 provides:

> Subject to § 403, a state has jurisdiction to prescribe law with respect to
>
> (1) (a) conduct that, wholly or in substantial part, takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside its territory that has or is intended to have substantial effect within its territory;
>
> (2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and
>
> (3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

Id. § 402. Section 403 provides:

> (1) Even when one of the bases of jurisdiction under § 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of jurisdiction is unreasonable.
>
> (2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including, where appropriate:
>
> (a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;
>
> (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;
>
> (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted;
>
> (d) the existence of justified expectations that might be protected or hurt by the regulation;
>
> (e) the importance of the regulation to the international political, legal, or economic system;
>
> (f) the extent to which the regulation is consistent with the traditions of the international system;

"reasonableness," jurisdiction to prescribe would exist with respect to, inter alia, conduct outside the United States that has or is intended to have substantial effect within the United States (for example, insider trading, occurring abroad via the Internet, that undermines the integrity of U.S. securities markets[421]), and conduct of U.S. nationals outside as well as within the United States (for example, U.S. citizens acting through the Internet to trade on inside information, whether they access the Internet inside[422] or outside the country[423]).

Of course, such an exercise of jurisdiction must be "reasonable," but it has been held to be so in the global marketplace in cases not involving the Internet. There is no obvious reason why the introduction of the Internet as the mechanism through which inside information is transmitted or trades are transacted should alter the result.[424]

2. Cyberspace Implications for Personal Jurisdiction

Relatively few Internet cases have considered personal jurisdiction across national borders, and virtually none has involved securities litigation. Some commentators have suggested that the Internet presents unusual considerations for personal jurisdiction, particularly because the Internet challenges minimum-contacts analysis: "[A] defendant committing securities fraud through use of the Internet possesses a more attenuated connection with the forum [jurisdiction] than a defendant in a similar situation without the use of the Internet."[425] These

---

(g) the extent to which another state may have an interest in regulating the activity; and
(h) the likelihood of conflict with regulation by another state.

Id. § 403.

421. Under the "effects principle," governments have jurisdiction to prescribe when acts occurring in other States have impact within the prescribing government's territory.

422. Under the "territoriality principle," governments have jurisdiction to prescribe conduct that occurs within their geographic borders.

423. Under the "nationality principle," governments have jurisdiction to prescribe and proscribe the conduct of their nationals wherever they may be located.

424. *See* Jack L. Goldsmith, *The Internet and the Sovereign State: The Role and Impact of Cyberspace on National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 475, 479 (1998) ("The territorial effects rationale for regulating these harms [including securities fraud committed via the Internet] is the same as the rationale for regulating similar harms in non Internet cases."); Charles H. Kennedy, Comment, *Is the Internet a New Legal Frontier?*, 39 HOW. L.J. 581, 586 (concluding that current law will incrementally absorb new challenges posed by the Internet just as it has absorbed new challenges presented by earlier technological advances).

425. Brakebill, *supra* note 1, at 922.

commentators argue that traditional geography-based notions of jurisdiction are irrelevant to Internet cases because cyberspace is divided into networks, domains, and hosts rather than along geopolitical boundaries;[426] other commentators, however, riposte that cyberspace has as much physical location as does a telephone system and should be treated simply as an advanced form of communication.[427] In general, courts have sided with the traditionalists and simply applied familar doctrine to determine the existence of personal jurisdiction in Internet cases,[428] which has produced perfectly sensible results. There is no reason that should change in the insider trading context.

Minimum-contacts analysis turns on "purposeful availment," which consists of foreseeability and voluntariness.[429] Persons who voluntarily engage in insider trading either by sending or receiving material, nonpublic information over the Internet, or by executing purchases or sales over the Internet, can foresee that if the stocks of U.S. companies or stocks traded on U.S. exchanges are involved, the integrity of those markets will be undermined in a manner that will have significant impact in the United States, providing a basis for personal jurisdiction. Therefore, such inside traders should not be surprised when the SEC hauls them into U.S. courts to answer for their misdeeds.[430]

3. Cyberspace Implications for Investigation and Enforcement

The rise of the Internet exacerbates insider trading enforcement difficulties in at least two ways. First, increased Internet trading and communication multiplies the frequency of insider trading cases having

---

426. *See* Burnstein, *supra* note 278, at 81.

427. *See* Ryan Yagura, *Does Cyberspace Expand the Boundaries of Personal Jurisdiction?*, 38 IDEA 301, 302 (1998).

428. *See* Daniel V. Logue, *If the International Shoe Fits, Wear It: Applying Traditional Jurisdiction Analysis to Cyberspace in* Compuserve, Inc. v. Patterson, 42 VILL. L. REV. 1213, 1231 (1997).

429. *See* Ticketmaster-New York, Inc. v. Alioto, 26 F.3d 201, 207 (lst Cir. 1994). *See generally* 4 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 1067, at 274 & n.29 (2d ed. 1987 & Supp. 1998) (collecting cases).

430. This Article focuses on *civil* actions and does not consider criminal cases. However, it should be noted that the United States has extradition treaties with about 100 nations covering cases where the act is a crime in both countries. *See* Jack E. Brown, *Jurisdiction to Prosecute Crimes Committed by Use of the Internet*, 38 JURIMETRICS J. 611, 613 (1998); *see also* OFFICE OF THE LEGAL ADVISER, U.S. DEP'T OF STATE, TREATIES IN FORCE (1997), *available at* <http://www.acda.gov/state/tifjan97.pdf>. These treaties allow the SEC to refer cases of international insider trading to the Department of Justice for criminal prosecution.

the cross-border dimensions and attendant jurisdictional complications discussed in Part VI.B. Second, the technology of the Internet, including its anonymizing features, makes detection and enforcement more difficult than ever before.[431]

For the SEC, this means several things. First, the SEC must expand its own Internet surveillance efforts[432] and push IOSCO[433] and other regulators to pursue insider trading activity on the Internet.

Second, the SEC must consider the implications of Internet technology when negotiating and renegotiating its MOUs. For example, Wilske and Schiller envision an agency such as the SEC or Federal Bureau of Investigation running computer programs that could search databases located in other countries. They suggest regulators could send "dog sniffs"[434] over the network to check the contents of hard drives or could attempt to filter streams of e-mail communications by searching for keywords, scrutinizing communications within news groups, or investigating suspicious websites.[435] They make the point that for an enforcement agency of one nation to cross a national boundary, even electronically, to search computers or other paraphernalia located in another nation without consent is arguably a violation of the latter

---

431. *See generally* Stuart David Meissner, *Securities Fraud and Manipulation in Cyberspace*, WALLSTREETLAWYER.COM, Aug. 1998, at 12, 14–15 (discussing major international fraud perpetrated over the Internet that U.S., Canadian, and Swedish authorities have yet to crack).

432. In the summer of 1998, the SEC created a new Office of Internet Enforcement to specialize in stopping Internet-related securities violations. *See* Jeri Clausing, *Compressed Data: A New Watchdog Against Internet Fraud*, N.Y. TIMES, Aug. 3, 1998, at D3.

433. IOSCO has already extended its insider trading surveillance and international enforcement cooperation to the Internet. *See Int'l Panel*, *supra* note 376 (noting September 11–12, 1997 meeting at which IOSCO members planned to work out guidelines to prevent illegal insider trading over the Internet).

434. A "dog sniff" is essentially an interactive, simultaneous exchange of information between two computers. *See* Steven DeRosa, *The Luddite's Dictionary*, S.F. CHRON., May 8, 1994, at 2.

435. *See* Wilske & Schiller, *supra* note 413, at 172–73; *see also* Eric Hubler, *Investing It: Brokerage Cops Wary of Cyberspace*, N.Y. TIMES, Apr. 12, 1998, § 3, at 4 (explaining use of screening software by brokerage-firm compliance officials).

nation's sovereignty.[436] Therefore, MOU negotiations should cover such matters.

Third, regulators should share information regarding surveillance and detection techniques.[437] Most lawyers, even those in the United States, have little experience in collecting and analyzing electronic evidence.[438] As Internet transactions cross national borders, matters become even more complicated. Like the SEC, the Australian Securities Commission ("ASC") has assembled a team of employees to research the latest developments in search tools. The team "regularly uses these search tool facilities (and can customise its own search tools) in order to help obtain tactical information from the Internet, and find[ ]suspect activity and track it to its source."[439] Certainly the SEC must keep up-to-date on the latest technology that allows such Internet searches, and should encourage and perhaps financially assist other nations in adopting and mastering such technology. For example, SRA International, Inc. recently launched a software package that monitors e-mail communications between securities firms and their clients in order to detect insider trading or other illegal activity.[440] Such programs could be helpful in the United States and abroad. IOSCO has recognized that regulators must master new techniques for Internet surveillance[441] and generally be Internet-literate to succeed.[442] Regulators should be

---

436. *See* Wilske & Schiller, *supra* note 413, at 172 & n.326 ("The Swiss Federal Tribunal, Lausanne, decided in 1982 that a violation of sovereignty did not necessarily require that the violating person acted on the territory of the violated State."). On the other hand, U.S. courts have disagreed. *See, e.g.*, United States v. Romano, 706 F.2d 370, 375 (2d Cir. 1983) (holding that absent any physical entry by foreign official onto Italian territory, "there was no violation of territorial sovereignty or offense to any State").

437. *See* TECHNICAL COMMITTEE, IOSCO, REPORT ON ENFORCEMENT ISSUES RAISED BY THE INCREASING USE OF ELECTRONIC NETWORKS IN THE SECURITIES AND FUTURES FIELD (1997), *reprinted in* SECURITIES IN THE ELECTRONIC AGE, *supra* note 10, at 157, 169 [hereinafter IOSCO, REPORT ON ENFORCEMENT ISSUES].

438. *See* Joan E. Feldman & Rodger I. Kohn, *Collecting Computer Based Evidence*, N.Y. L.J., Jan. 26, 1998, at S5.

439. AUSTRALIAN SECURITIES COMMISSION, ASC INITIATIVES IN RELATION TO ELECTRONIC COMMERCE DEVELOPMENTS (1997), *reprinted in* SECURITIES IN THE ELECTRONIC AGE, *supra* note 10, at 217, 233.

440. *See* Matt Andrejczak, *SRA Software Monitors Brokers' Online Messages*, WASH. BUS. J., Jan. 30, 1998, at 6 (noting that SRA initially intended to sell software in United States, United Kingdom, Japan, Germany, and Switzerland).

441. *See* IOSCO, REPORT ON ENFORCEMENT ISSUES, *supra* note 437, at 166.

442. The IOSCO Technical Committee has recognized that regulators in many nations are not up to speed with Internet technology and therefore are behind the learning curve necessary for effective regulation. *See id.* at 172.

particularly concerned with "anonymizing tools"; for the would-be violator of securities laws, "electronic markets provide a new veil behind which to hide."[443] Regulators will have to overcome "remailer" sites and anonymizing software in order to identify and locate wrongdoers.[444]

Fourth, regulators must overcome various difficulties in collecting evidence about communications over the Internet. As noted earlier,[445] under pressure from the SEC, both the NYSE and the NASD[446] instituted procedures for the monitoring and retention of e-mail correspondence between members and customers in order to facilitate enforcement of various rules, including those relating to insider trading. Other nations should institute similar rules. However, even if regulators surmount these challenging technical difficulties, legal barriers may remain. For example, there is considerable variation among nations in the laws that govern the ability of regulators to compel production of data from ISPs and others.[447] Although the United States, United Kingdom, and Australia have given substantial thought to the implications of Internet technology for their securities laws and have adjusted their rules and regulations accordingly, other nations may neither have thought through these implications nor acted on them.[448]

Fifth, regulators can educate investors about potential Internet abuses and remedies. The IOSCO report notes that "[t]here is a degree of self-regulation among Internet users who are resentful of Internet technology being used for illegal purposes. They seek to protect the integrity of the Internet by investigating suspicious matters and frequently make complaints or report potential abuses to regulators."[449] IOSCO recommends that regulators encourage this practice, which goes hand in glove with the ITSFEA provision that rewards investors who blow the whistle on inside traders.[450]

Ultimately, the key will be whether the SEC and IOSCO, which have been relatively successful in securing international cooperation for detecting and punishing insider trading activity in the global

---

443. Mann, *supra* note 398, at 24.

444. *See* IOSCO, REPORT ON ENFORCEMENT ISSUES, *supra* note 437, at 166–67.

445. *See supra* notes 287–94 and accompanying text.

446. *See* NYSE Procedures, *supra* note 289; NASD Procedures, *supra* note 289.

447. *See* IOSCO, REPORT ON ENFORCEMENT ISSUES, *supra* note 437, at 167.

448. *See id.*

449. *Id.* at 170.

450. *See* 15 U.S.C. § 78u-1(e) (1994). Additionally, Professor Choi predicts that private sources of investor protection, such as third-party certifiers of information, will flourish with the rise in Internet trading. As a result, governmental regimes may compete with private certifiers in a "race to the top" by providing efficient, general antifraud regulation. *See* Choi, *supra* note 396, at 54–55.

marketplace, can achieve similar success in the cyberspace marketplace.[451] One very positive sign is that IOSCO has issued reports that highlight the problems created by Internet trading and emphasize the importance of international coordination regarding such activity.[452]

The bottom line is this: "States have already regulated the moon and other celestial bodies, the deep seabed, and Antarctica. Although States will face seemingly insurmountable problems in their efforts to domesticate a network of computers, they will gradually find solutions."[453] Those solutions are found in the pattern of international cooperation that has evolved from regulation of the global marketplace. The cyberspace securities marketplace does not present what Professor Salbu categorizes as a "transformative" situation,[454] justifying creation of an entirely new regulatory paradigm.

Assuming for the purpose of argument that the SEC's rather aggressive approach toward enforcing insider trading rules in the global marketplace is a reasonable one,[455] there is no reason to blunt that program of enforcement as insider trading activity moves to the Internet. Basic approaches have served the SEC well in overcoming problems of subject matter jurisdiction, personal jurisdiction, and enforcement and investigation. The same basic approaches will, with slight modification, also work for cyberspace market regulation. Perhaps there is "no 'there'

---

451. *See* IOSCO, REPORT ON ENFORCEMENT ISSUES, *supra* note 437, at 168–69 (highlighting need for international cooperation). Regulators of commodities markets have noted the same need. *See Technological Advances Produce Global Regulatory Issues, CFTC Official Says*, BNA SEC. L. DAILY, Jan. 13, 1997 (quoting Andrea Corcoran, Director of CFTC Division of Trading and Markets, as noting that there is "widespread recognition" that no regulator "is an island" (internal quotation marks omitted) and that "the trend of the international community is to move away from merely discussing the goals of regulation, toward a practical and much more complex discussion of the techniques that are necessary to achieve such goals").

452. *See, e.g.*, IOSCO, REPORT ON ENFORCEMENT ISSUES, *supra* note 437; TECHNICAL COMMITTEE, IOSCO, SECURITIES ACTIVITY ON THE INTERNET (1998), *available at* <http://www.iosco.org/docs-public/1998-internet_security.html>. *See generally* Michael L. Michael, *IOSCO Issues Cybersecurities Report*, WALLSTREETLAWYER.COM, Oct. 1998, at 16 (summarizing IOSCO report).

453. Wilske & Schiller, *supra* note 413, at 174–75; *see also* Burnstein, *supra* note 278, at 116 ("It is doubtful . . . that nation-states in real-space will relinquish control over the communications medium of the twenty-first century.").

454. *See* Salbu, *Who Should Govern*, *supra* note 413, at 441–42.

455. As noted earlier, *see supra* note 340, this Article simply assumes that the SEC's approach is reasonable; some commentators have argued that a less expansive application of U.S. securities laws would be more sensible. *See, e.g.*, Fisch, *Imprudent Power*, *supra* note 340, at 553–72.

there"[456] in cyberspace, but "the legitimacy of regulation turns upon *effects*."[457] Whether insider information is tipped via telephone or e-mail, whether trades are executed over a physical exchange or over the Internet, the impact is the same and consequently the same basic regulatory regime should work. As the SEC keeps repeating, the "new" Internet frauds, including insider trading, are simply old wine in new bottles.[458] The old rules will work fine to regulate and punish such frauds, as long as regulators keep up with the crooks and facilitate "real international cooperation."[459]

VII. CONCLUSION

As the technological revolution forces reevaluation of the federal securities laws, many changes in regulation are to be expected. However, in the antifraud areas, such as insider trading, no revolution need occur. Some adjustment to the law is certainly in order, but fraud is fraud no matter what the medium.

In this Article, I have made five points. First, the SEC must reconsider the notion of what constitutes "nonpublic" information. The Internet creates so many new channels for disclosure and dissemination of information that new rules ("new" in part because there are no old rules) should be promulgated and should err on the side of recognizing the vast dissemination capabilities of the Internet.

Second, hackers and other thieves who steal inside information for the purpose of trading on that information should be classified and punished as misappropriators.

Third, ISPs may have negligence liability exposure in some jurisdictions when their lax security measures allow hackers to steal inside information belonging to the ISPs' customers. ISPs also face a very small chance of ITSFEA liability for hacking done by their own employees.

---

456. Rosaland Resnick, *Cybertort: The New Era*, NAT'L L.J., July 18, 1994, at A1 (with obvious apologies to Gertrude Stein).

457. Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1404 (1996) (emphasis added).

458. *See, e.g., Chat Room: John Stark: Securities and Exchange Commission, Special Counsel for Internet Projects*, FIN. NETNEWS, Feb. 24, 1997, at 10 (stating that SEC does not need any new rules or regulations to combat Internet securities fraud because "current antifraud provisions will do just fine").

459. *Internet Should Spur International Cooperation Among Regulators, Former SEC Member Says*, BNA SEC. L. DAILY, Apr. 21, 1998 (citing statement by former SEC Commissioner A.A. Sommer, Jr. at international institute that problems created by Internet fraud "should spur regulators worldwide to 'real international cooperation'").

Fourth, securities firms, public companies, lawyers, and accountants must recast their insider trading compliance rules, including their Chinese Walls, to account for the latest technology. Compliance programs are simply inadequate unless the newest Internet security devices have been considered and adopted.

Fifth, and finally, regulating insider trading in the Internet's electronic marketplace is much like regulating insider trading in the global marketplace. To the extent that the SEC plans to continue aggressive assertion of its regulatory powers, a controversial step that I personally applaud, it has an excellent game plan already established. The same active unilateral assertion of authority coupled with international cooperation through bilateral treaties, MOUs, and international organizations should serve to create a viable framework for regulating insider trading in cyberspace just as it has done for the global marketplace.