Computer Hacking as a Deceptive Device: Why the Courts Must Give Computers Legal Consciousness to Hold Hackers Liable for Insider Trading

Farid Sharaby
University of the Pacific, McGeorge School of Law

Follow this and additional works at: https://scholarlycommons.pacific.edu/mlr
Part of the Internet Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://scholarlycommons.pacific.edu/mlr/vol42/iss4/8

This Comments is brought to you for free and open access by the Journals and Law Reviews at Scholarly Commons. It has been accepted for inclusion in McGeorge Law Review by an authorized editor of Scholarly Commons. For more information, please contact mgibney@pacific.edu.
Computer Hacking as a “Deceptive Device”: Why the Courts Must Give Computers Legal Consciousness to Hold Hackers Liable for Insider Trading

Farid Sharaby*

TABLE OF CONTENTS

I. INTRODUCTION .................................................................................................................. 930

II. BACKGROUND OF INSIDER TRADING LAW .................................................................. 932
   A. Section 10(b) and Rule 10b-5 ......................................................................................... 932
   B. The Classical Theory of Insider Trading ......................................................................... 933
   C. The Misappropriation Theory of Insider Trading ............................................................. 934

III. HACKING AS A “DECEPTIVE DEVICE” .......................................................................... 937
   A. Different Hacking Techniques ......................................................................................... 937
   B. The SEC’s Argument That a Computer Can Be Deceived ............................................... 938
   C. Why the SEC’s Argument Is Problematic ....................................................................... 939

IV. CAN A COMPUTER BE DECEIVED? .................................................................................. 941
   A. Door-Lock Hypothetical .................................................................................................. 942
   B. Thinking Is Beyond a Computer’s Capacity ....................................................................... 943
      1. Difference in Intelligence .............................................................................................. 944
      2. The Chinese Room ....................................................................................................... 945
   C. Computers Can Think .................................................................................................... 946
      1. The Turing Test ............................................................................................................. 946
      2. Computing Is Thinking ............................................................................................... 948
         a. Detailed Processing Analogy .................................................................................. 948
         b. Simple Processing Analogy .................................................................................... 949

V. SATISFYING THE DECEPTIVE DEVICE ELEMENT .......................................................... 950

VI. INTRODUCING AN ALTERNATIVE APPROACH: APPLYING PERSONHOOD TO COMPUTERS ........................................................................................................... 951
   A. Corporate Personhood .................................................................................................... 951

* J.D. Candidate, University the Pacific, McGeorge School of Law, 2011; B.A., Political Science, California State University, Northridge, 2007. I wish to thank Professor Franklin A. Gevurtz for providing me with invaluable assistance and insight in writing this Comment. I also offer thanks to my family for giving me endless support throughout my law school experience.
As the Internet continues to have an impact on securities law, new issues arise that must be resolved.1 Internet use especially impacts the ever-changing area of insider trading.2 Specifically, the rise of the Internet is problematic because individuals can hack into computers, acquire nonpublic information, and then trade on that information. To be found guilty of insider trading under § 10(b) of the Securities Exchange Act, a defendant must acquire the inside information by deception.3 While some writers have touched on this topic briefly,4 there has been no in-depth analysis as to whether a hacker can satisfy the deception element of insider trading by deceiving a computer.5 Recently, in SEC v. Dorozhko, the Second Circuit had the chance to decide the issue.6

On October 9, 2007, IMS Health (IMS), a company that provides market information to the healthcare and pharmaceutical companies,7 announced that it would post its earnings on the 17th of that month.8 Although IMS planned to announce negative earnings that were below prior estimates, there were no media reports predicting such a negative announcement, and some analysts even opined that IMS was in good financial health.9 Thomson Financial, an information company, had the responsibility of posting the earnings over the Internet.10 However, days before IMS announced that it would publicize its earnings, Oleksandr Dorozhko transferred $42,500 to Interactive Brokers LLC and opened an online trading account.11 On October 17, using a technique called “spoofing,”12 Dorozhko hacked into Thomson Financial’s website, searching for the IMS

---

1. Robert A. Prentice, The Internet and Its Challenges for the Future of Insider Trading Regulation, 12 HARV. J.L. & TECH. 263, 265 (1999) (“There is no doubt that the Internet is revolutionizing the securities business. This revolution mandates a reexamination of most aspects of how the Securities Exchange Commission ("SEC") regulates securities.").
2. See generally id. (examining the Internet’s affect on insider trading law).
4. See, e.g., FRANKLIN A. GEVURTZ, CORPORATION LAW 627 (2010) (raising the issue of whether hacking into a computer satisfies the deception element).
5. See, e.g., Prentice, supra note 1, at 306 (briefly opining that hacking would satisfy the deception element).
9. Id.
10. Id.
11. Id. at 324-25.
12. Id. at 325 n.3 (noting that “spoofing” is a location hiding technique).
McGeorge Law Review / Vol. 42

earnings report.13 Once IMS transferred the earnings report to Thomson Financial, Dorozhko found the information and downloaded it.14 Subsequently, Dorozhko purchased $41,670.90 worth of put options in IMS.15 After IMS announced its below-expected earnings, its stock dropped significantly.16 Dorozhko then sold his put options and made a profit of $286,456.59.17

The Second Circuit had to decide two pivotal issues.18 First, whether a fiduciary duty is necessary in an insider trading case involving computer hacking.19 Importantly, the court found that Dorozhko could still be implicated as an insider even though he owed no fiduciary duty to the information supplier.20 Second, whether computer hacking constitutes deception.21 More specifically: whether a computer can be deceived.22 Avoiding the second issue, the court remanded that specific question to the district court.23

Part II of this Comment will provide a background of insider trading law, with a focus on the deceptive device element of § 10(b) of the Securities and Exchange Act of 1934. Part III will present the SEC’s arguments which support the view that hacking amounts to deception, and will then explain why those arguments do not adequately address the issue. Part IV will examine the competing arguments concerning whether computers have the capacity to think. This discussion will highlight the fact that such a philosophical determination, while necessary for 10(b) purposes, is beyond the grasp of the courts. Since both

13. Id. at 325.
15. Id. An “option” is defined as “[t]he right (but not the obligation) to buy or sell a given quantity of securities . . . at a fixed price within a specified time [.]” BLACK’S LAW DICTIONARY 1203 (9th ed. 2009). A “put option” is defined as “[a]n option to sell something . . . at a fixed price even if the market declines.” Id.
16. Dorozhko, 574 F.3d at 44 (“When the market opened [on October 18th], IMS’s stock price sank approximately 28% almost immediately . . . .”).
17. Id. Traders purchase put options to take advantage of a drop in price of the stock. Id. at 44 n.1.
18. See id. at 50–51 (introducing both issues presented by the case).
19. Id. at 43–44 (“We are asked to consider whether . . . computer hacking may be ‘deceptive’ where the hacker did not breach a fiduciary duty . . . .”).
20. Id. at 45 (finding that Dorozhko was an inside trader even though the SEC acknowledged that Dorozhko had not breached any fiduciary duty).
21. Id. at 45–46.
22. See id. at 50–51 (questioning whether computer hacking can be deceptive).
23. Id. at 51 (“[W]e are hesitant to move from this general principle to a particular application without the benefit of the district court’s views as to whether the computer hacking in this case—as opposed to computer hacking in general—was ‘deceptive.’”). On remand, the district court granted the Commission’s motion for summary judgment. Litigation Release, SEC, SEC Obtains Summary Judgment Against Computer Hacker for Insider Trading (Mar. 29, 2010), available at http://www.sec.gov/litigation/litreleases/2010/lr21465.htm (on file with the McGeorge Law Review). The motion was unopposed, however, seemingly because the defendant was unwilling to communicate with his attorney. Yin Wilczek, Insider Trading: Enforcers Turn Corner on Insider Trading by Hedge Funds, Say Current, Ex-SEC Staff, 42 SRLR 519 (Mar. 22, 2010) (“The defendant ‘has failed to respond to numerous requests from counsel for directions as to how to proceed in connection with the instant litigation,’ [the defendant’s attorney] said. Accordingly, counsel is without any factual basis to respond to the instant summary judgment motion and therefore does not oppose it.”).
computers and humans have the ability to process information, computers arguably have the capacity to think for insider trading purposes. Thus, courts have grounds for giving computers legal consciousness. Part V concisely explains the reasoning that courts can rely on. Part VI sets forth an alternative approach whereby courts can give computers personhood, finding that computers can be deceived for the purposes of insider trading.

This Comment ultimately argues that, while the debate about artificial intelligence continues without end in sight, it would be wise for courts to give computers a legal ability to think in the Section 10(b) context as it relates to hacking. Computers process information in a manner that is analogous to the human brain, which provides the courts enough support to make such a ruling.

II. BACKGROUND OF INSIDER TRADING LAW

A. Section 10(b) and Rule 10b-5

An understanding of insider trading law begins with The Security Exchange Act of 1934 (Act).24 This Act, a response to the 1929 stock market crash, seeks to supervise and regulate securities trading.25 Section 10(b) and Rule 10b-5, the relevant provisions of the Act, form the foundation of insider trading law.26 Indeed, the majority of inside traders are prosecuted under these two provisions.27

Section 10(b) provides that a person may not “use or employ, in connection with the purchase or sale of any security . . . 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.”28 Section 10(b) is implemented by Rule 10b-5, which makes it “unlawful for any person . . . to employ any device . . . to defraud . . . in connection with the purchase or sale of any security.”29 Under Rule 10b-5, the SEC can prosecute a defendant for fraud by showing the defendant made a “material misstatement or omission in connection with the purchase or sale of securities that has caused damages.”30 The deception element is satisfied by the
occurrence of a misrepresentation or an omission.\textsuperscript{31} However, an omission is only deceptive when there is a duty to inform.\textsuperscript{32} In the context of computer hacking, the device must be deceptive, not manipulative, due to the way "manipulative" has been defined by the courts.\textsuperscript{33} The Supreme Court has ruled that "manipulative" implies defrauding shareholders by rigging the price of securities.\textsuperscript{34} Hacking into a computer in no way amounts to rigging the price of securities.\textsuperscript{35}

While Section 10(b) and Rule 10b-5 are used to prosecute inside traders, these provisions fail to lay out a definition of "insider trading."\textsuperscript{36} Instead, courts have defined what it means to be an inside trader,\textsuperscript{37} and as discussed below, the definition of an inside trader has expanded over time.\textsuperscript{38}

\textbf{B. The Classical Theory of Insider Trading}

Under the classical theory, only a person who is literally "inside the firm"—including directors, officers, and employees—may be considered an insider.\textsuperscript{39} This theory provides that an insider who acquires material information not accessible to the public may not trade on that information, unless the person makes the information public before trading.\textsuperscript{40} It is the fiduciary duty between these insiders (agents) and the shareholders of the corporation (principals) that forms the basis of the classical theory.\textsuperscript{41} Since a duty exists between insiders and

\textsuperscript{31} SEC v. Dorozhko, 574 F.3d 42, 49 (2d. Cir. 2009) ("Chiarella, O'Hagan, and Zandford all stand for the proposition that nondisclosure in breach of a fiduciary duty 'satisfies § 10(b)'s requirement . . . [of] a 'deceptive device or contrivance[,]'.")

\textsuperscript{32} Basic Inc. v. Levinson, 485 U.S. 224, 239 n.17 (1988) ("Silence, absent a duty to disclose, is not misleading under Rule 10b-5.")

\textsuperscript{33} See, e.g., SEC v. Dorozhko, 606 F. Supp. 2d 321, 329 (S.D.N.Y. 2008) (ruling that hacking, at least in this case, does not amount to "manipulation").

\textsuperscript{34} See Ernst & Ernst v. Hochfelder, 425 U.S. 185, 199 (1976) ("[Manipulative] connotes intentional or willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities."); see also Santa Fe Indus. v. Green, 430 U.S. 462, 476 (1977) ("[Manipulation] refers generally to practices such as wash sales, matched orders, or rigged prices that are intended to mislead investors by artificially affecting market activity.").

\textsuperscript{35} Dorozhko, 574 F.3d at 46 n.3 (2d. Cir. 2009) (noting that the district court concluded that hacking is not manipulative and that the parties did not challenge that conclusion).

\textsuperscript{36} STRADER, supra note 25, at 108.

\textsuperscript{37} Id.


\textsuperscript{39} SMITH & WILLIAMS, supra note 30, at 957.

\textsuperscript{40} Id. at 956 ("The classical theory of insider trading is concerned with corporate insiders' unfair use of corporate information to make a profit at the expense of outsiders who couldn't possibly . . . discover the information."); see also Robert Steinbuch, Mere Thieves, 67 MD. L. REV. 570, 578 (2008) (providing that insider trading involves the trading of "material, nonpublic information").

\textsuperscript{41} SMITH & WILLIAMS, supra note 30, at 957; Steinbuch, supra note 40, at 578.
shareholders, failing to inform the shareholders of the nonpublic information amounts to a material omission of fact. Thus, the insiders are deceiving the shareholders.

In Chiarella v. United States, a majority of the Supreme Court formally adopted the classical theory. There, the defendant—a printer working for an independent financial printing company that regularly printed financial documents—printed documents announcing several corporate takeover bids. After using the documents to discern the identity of the target companies, the defendant bought stock in those companies. After the takeovers, the defendant sold the stock, realizing huge profits.

The issue in Chiarella was whether the defendant, an outsider, was required to publicize the information before trading. Using common law principals and prior case law, the majority noted that a person with material information is only required to disclose it when there was a duty to do so. Since the defendant was not an insider of any of the target or acquiring companies, he had no duty to the shareholders of those companies. Thus, the defendant was not liable as an inside trader.

C. The Misappropriation Theory of Insider Trading

Two seminal misappropriation cases stand for the proposition that stealing nonpublic information and trading on it amounts to fraud: one is Chief Justice Burger’s dissent in Chiarella and the other is United States v. O’Hagan. In his Chiarella dissent, Burger read the language of Section 10(b) and Rule 10b-5 as referring to any person committing fraudulent behavior. Thus, the difference

42. See Chiarella, 445 U.S. at 224 (holding that defendant was not an insider under the classical theory, and was thus wrongly convicted).
43. Id.
44. Id.
45. Id.
46. Id.
47. Id. at 227–28.
At common law, misrepresentation made for the purpose of inducing reliance upon the false statement is fraudulent. But one who fails to disclose material information prior to the consummation of a transaction commits fraud only when he is under a duty to do so. And the duty to disclose arises when one party has information that the other [party] is entitled to know because of a fiduciary or other similar relation of trust and confidence between them.
Id. (internal quotations omitted) (bracket in the original).
48. See id. at 232 ("[T]he element required to make silence fraudulent—a duty to disclose—is absent in this case.").
49. See id. at 237 (providing that the court reversed the defendant’s conviction).
51. Chiarella, 445 U.S. at 240 (Burger, J., dissenting) ("The language of §10(b) and of Rule 10b-5 . . . reach any person engaged in any fraudulent scheme.").
between an insider and an outsider was a legal fiction. With a utilitarian viewpoint, Burger reasoned that the policy behind limiting insider trading to insiders should itself be limited.

The rationale behind allowing outsiders to profit from the information they have lawfully gathered was to incentivize hard work. A knowledgeable trader who performs "hard work, careful analysis, and astute forecasting," will benefit from his conduct. However, if someone could merely steal information acquired through another's hard work, there would be no incentive to perform the hard work in the first place. Thus, when an outsider acquires information in an unlawful manner, Chief Justice Burger reasoned, the outsider should have a duty to disclose. Congress does not want those who deceive and steal to have an unfair advantage over those who refrain from engaging in such practices.

In O'Hagan, the Supreme Court adopted the misappropriation theory, but rather than embrace Burger's broad utilitarian approach, the Court laid out a much more limited theory. There, the defendant worked for a law firm that represented a client who made a tender offer for a target company. The defendant, who did not take part in the representation, bought over two thousand options and common stock in the target company after learning of the tender offer. After the tender offer was publicly announced, the defendant sold the options and common stock, making a profit of over $4.3 million.

The Court held that one commits deception when he takes information from a supplier and, feigning loyalty, uses that information for his own benefit. The Court embraced the policy behind the misappropriation theory. Investors will only trade in the market if they are sure that there will be laws to prevent the

---

52. See id. ("[The use of the word 'any'] negates the suggestion that congressional concern was limited to trading by 'corporate insiders' or to deceptive practices related to 'corporate information.'").

53. Id.

54. Id.

55. Id.

56. See id. (arguing that the rule allowing outsiders to profit from their hard work should not apply "when an informational advantage is obtained . . . by some unlawful means").

57. Id. ("I would read § 10(b) and Rule 10b-5 to encompass and build on this principle: to mean that a person who has misappropriated nonpublic information has an absolute duty to disclose that information or to refrain from trading.").

58. Id. at 241 ("The antifraud provisions were designed in large measure to assure that dealing in securities is fair and without undue preference or advantages among investors." (internal quotations omitted)).

59. GEVURTZ, supra note 4, at 625 ("Chief Justice Burger's utilitarian theory was not the theory adopted by the court in O'Hagan. Instead the court adopted what might be labeled the 'sneaky theft' theory.").


61. Id. at 647-48.

62. Id. at 648.

63. Id. at 653-54 ("A fiduciary who '[pretends]' loyalty to the principal while secretly converting the principal's information for personal gain, dupes or defrauds the principal.").

64. See id. at 658 ("Although informational disparity is inevitable in the securities markets, investors likely would hesitate to venture their capital in a market where trading based on misappropriated nonpublic information is unchecked by law.").
misappropriation of material, nonpublic information.\textsuperscript{65} Since \textit{O'Hagan}, a person "violates Section 10(b) and Rule 10b-5, when he misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information."\textsuperscript{66}

\textit{O'Hagan} also made an important ruling concerning the relationship between the "in connection with" element and the deception element of Rule 10b-5.\textsuperscript{67} There are two possible interpretations of the rule. One interpretation is that the "in connection with" element requires the deception to simultaneously occur with the purchase or sale of a security.\textsuperscript{68} This happens if the trader lies to the \textit{purchaser}, inducing the purchaser to buy the security. The second interpretation, found in \textit{O'Hagan}, takes a much more liberal view of the rule.\textsuperscript{69} Suppose a trader tells an information supplier that the inside information will not be traded on, but then later trades on the information. In reality, the deception takes place the moment the trader lies to the \textit{information supplier}.\textsuperscript{70} However, the Court ruled that the deception does not occur until the inside information is actually \textit{traded on}; if there was no trading, the trader did not actually lie in his statement to the information supplier.\textsuperscript{71}

Had the Court in \textit{O'Hagan} adopted the first interpretation, the issue of whether a computer can be deceived would be moot. The hacker first hacks into the computer, and subsequently, rather than simultaneously, trades on the

\begin{itemize}
  \item \textbf{65.} Id.
  \item \textbf{66.} Id. at 652.
  \item \textbf{67.} Id. at 656 (noting that the "in connection with" element is completed when the inside information is traded on, not when it is received from the information source).
  \item \textbf{68.} Under Justice Burger's utilitarian approach, which was not adopted by \textit{O'Hagan}, the duty to disclose information runs to the other party of the transaction. \textit{Gevurtz, supra} note 4, at 625–26. Thus, the other party is deceived when the misappropriator does not disclose the information. \textit{Id.} As a result, the deception would occur simultaneously with the purchase and sale of the security. \textit{See id.} (noting that Burger's approach would have "avoided the 'in connection with' issue"). In his dissent in \textit{O'Hagan}, Justice Thomas highlighted that the defendant could have done anything with the confidential information, including selling it to a newspaper. \textit{O'Hagan}, 521 U.S. at 685 (Thomas, J., dissenting). Thus, the majorities reasoning on the "in connection element" was problematic. \textit{Id.} at 686.
  \item \textbf{69.} \textit{See O'Hagan,} 521 U.S. at 656 (finding that the trader satisfies the deception element by lying to the information supplier).
  \item \textbf{70.} \textit{See Gevurtz, supra} note 4, at 626–27 (explaining that if a spy lies to a guard of a vault to gain secret documents, the guard has clearly been defrauded regardless of what the spy does with the documents).
  \item \textbf{71.} \textit{O'Hagan,} 521 U.S. at 656.
\end{itemize}

\textit{[The "in connection with"]} element is satisfied because the fiduciary's fraud is consummated, not when the fiduciary gains the confidential information, but when, without disclosure to his principal, he uses the information to purchase or sell securities. The securities transaction and the breach of duty thus coincide. This is so even though the person or entity defrauded is not the other party to the trade, but is, instead, the source of the nonpublic information . . . A misappropriator who trades on the basis of material, nonpublic information, in short, gains his advantageous market position through deception; he deceives the source of the information and simultaneously harms members of the investing public." \textit{Id.; see also Gevurtz, supra} note 4, at 627 ("[U]nless [the misappropriator] trades, the fiduciary has not misled anyone about his or her intentions.").

936
information taken from the computer. Even if the computer had the ability to be deceived, the deception took place prior to the trading, and thus was not in connection with it.

III. HACKING AS A “DECEPTIVE DEVICE”

When facing the issue of whether hacking satisfies the deception element, courts seem to focus on the fiduciary duty aspect rather than on whether a computer can be deceived. However, regardless of whether a duty is required, one cannot meet the deception element unless a computer can be deceived. Since the SEC prosecutes hackers as inside traders, it is important to evaluate the Commission’s reasoning concerning how the deception element can be met. The SEC believes that a computer can be deceived. “By its very nature,” the SEC urges, “computer hacking involves deceptive . . . conduct.” Before immersing ourselves into the SEC’s reasoning for such an assertion, a brief introduction of computer hacking is necessary for a complete understanding of the issue.

A. Different Hacking Techniques

Generally, two kinds of computer crimes exist: “traditional crimes committed using computers, and crimes of computer misuse.” Traditional computer crimes involve ordinary crimes committed using the Internet as a means. Examples include Internet gambling, disseminating child pornography over the Internet, and cyberstalking. Computer misuse, on the other hand, is “conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks.” Hacking is an example of computer misuse.
There are a number of ways to hack into a computer. One way is to “trick” a computer by using someone else’s code, leading the computer to give access to the unauthorized user. Suppose, for example, that H, aware of V’s username and password, accesses V’s account information. V is authorized to view the information, but H is not. The computer is “tricked” in this situation. There are a number of ways to gain access to an authorized user’s password. A hacker can simply try every possible combination, for instance, or guess passwords which are specifically tailored to the authorized user.

Another way to hack into a computer is to exploit a weakness in a computer’s program and cause a malfunction, which gives the hacker greater access to the information stored in the computer. An example of such a tactic is a buffer overflow attack. A buffer overflow attack occurs when a hacker uses a program to place more information into a buffer (the space within the computer’s memory used to store information) than there is remaining memory able to store the information. The computer will accept information, but will overwrite data that is required to control the program. As a result, the hacker gains control of the program.

B. The SEC’s Argument That a Computer Can Be Deceived

In Dorozhko, the SEC made a number of arguments to support its assertion that computer hacking satisfied the deception element of Section 10(b). It simply analogized fraud in the context of insider trading with fraud in the context

81. Id. at 1644–45 (explaining two different types of computer misuse).
82. Id. at 1644 (“[T]he user may engage in false identification and masquerade as another user who has greater privileges.”).
83. Id. at 1645.
84. Id.
86. Id.
87. Kerr, supra note 76, at 1645.
88. Id.
89. Id.; see also Maciej Ogorkiewicz & Piotr Frej, Analysis of Buffer Overflow Attacks, WINDOWS SECURITY.COM, http://www.windowsecurity.com/articles/Analysis_of_Buffer_Overflow_Attacks.html (last visited Apr. 2, 2011) (on file with the McGeorge Law Review) (“[B]uffer overflow occurs anytime the program writes more information into the buffer than the space it has allocated in the memory.”); STEVEN DEFINO ET AL., OFFICIAL CERTIFIED ETHICAL HACKER REVIEW GUIDE 162 (2010) (“A buffer overflow occurs when input given to an application exceeds the amount of memory that was set aside to store it.”).
90. DeFino et al., supra note 89, at 162 (“The input is still accepted, and it overwrites other critical data such as register counters that the CPU (Central Processing Unit) requires to manage the running of the program.”).
91. Kerr, supra note 76, at 1645; Ogorkiewicz & Frej, supra note 89.
92. See Posthearing Memorandum, supra note 74, at 8–11 (explaining how computer hacking is deceptive or manipulative).
of other federal laws, and argued that the similarities were close enough.\textsuperscript{3} Specifically, the SEC pointed to the Computer Fraud and Abuse Act, federal mail and wire fraud statutes, and the Model Penal Code.\textsuperscript{4}

Under the Computer Fraud and Abuse Act, a defendant who gains access to a protected computer without authorization and subsequently uses the unauthorized access to commit a fraud is culpable if the defendant acquires "anything of value."\textsuperscript{9} Under federal mail and wire fraud statutes, the government must show: (1) the defendant executed a "scheme to defraud"; (2) the defendant made material misstatements or omissions; (3) the defendant intended to defraud; (4) the scheme results in a loss of property; (5) the United States mail, interstate or international wires, or private courier, were used in furtherance of the scheme to defraud; and (6) the defendant used the mail or wires.\textsuperscript{9}

The SEC also contended that Model Penal Code section 223.3, relating to theft by deception, supports the assertion that hacking constitutes deception.\textsuperscript{7} Subsection 223.3(1) provides that a defendant is guilty of theft by deception if he "creates or reinforces a false impression, including false impressions as to law, value, intention or other state of mind."\textsuperscript{9} Subsection (2) provides that a defendant is guilty if he "prevents another from acquiring information which would affect his judgment of a transaction." Finally, subsection (3) provides that the defendant is guilty if he "fails to correct a false impression which the [defendant] . . . knows to be influencing another to whom he stands in a fiduciary or confidential relationship."\textsuperscript{10}

\textbf{C. Why the SEC's Argument Is Problematic}

An in-depth analysis shows that the authors of the Computer Fraud and Abuse Act, federal mail and wire fraud statutes, and the Model Penal Code did not contemplate that a computer would be the victim of deception. Rather, the statutes seem to apply solely to humans. Breaking down each statute is illustrative.

A look at how courts have interpreted the Computer Fraud and Abuse Act shows that the SEC's analogy is mistaken. In \textit{Shurgard Storage Centers, Inc. v.}
Safeguard Self Storage, Inc., the court held "to defraud," in the context of the Computer Fraud and Abuse Act, simply means to "wrong[] one in his property rights by dishonest methods or schemes." The court adopted this broad definition of fraud rather than the common law definition.

The court's ruling is informative for two reasons. First, looking at the language, the definition is not referring to a computer. The words "one" and "his" support this assertion. Second, the origin of this definition also illustrates that the statute is not referring to computers. The Shurgard court adopted this definition from Hammerschmidt v. United States. There, the Supreme Court created this definition in a case which involved deception of the U.S. government. Thus, the concept of deceiving a computer did not exist anywhere in the concept of this definition.

Similarly, mail and wire fraud statutes do not provide a convincing analogy. The typical mail and wire fraud case occurs when the defendant uses the mail or a wire as a means to deceive a person on the other end of the communication. For example, in Lustiger v. United States, the defendant mailed advertisements to potential buyers containing misrepresentations. The defendant was using the mail as means for deceiving the potential buyers. Conversely, in Dorozhko, Dorozhko did not use the Internet as a means to deceive a person. If he had done so, the mail and wire fraud statutes would be analogous. However, Dorozhko used the Internet to gain access to the information on Thomson Financial's website. Dorozhko never made contact with a human being.

The fact that some courts require that the victim reasonably rely on the deception supports the inference that mail and wire fraud statutes apply solely to humans. This reliance element indicates that there must be a victim—a human—who is deceived. Arguing that hacking involves fraud in the same manner as mail and wire fraud is similar to claiming that the mail (such as a parcel) or wire (such as physical phone line) is literally being deceived.

102. Id. at 1125–26.
103. See id. at 1125 (taking the definition of "to defraud" from Hammerschmidt).
105. See, e.g., Lustiger v. United States, 386 F.2d 132, 134-35 (9th Cir. 1967) (deciding a mail fraud case).
106. Id. at 134–35.
107. Id. at 135.
108. See generally SEC v. Dorozhko, 574 F.3d 42 (2d. Cir. 2009) (mentioning no facts that Dorozhko even communicated with a person).
109. Id. at 44 (noting that Dorozhko hacked into Thomson Financial's server).
110. See generally id. at 44–45 (mentioning no facts that Dorozhko communicated with a human).
111. See, e.g., United States v. Brown, 79 F.3d 1550, 1557 (11th Cir. 1996) (describing the circuit court split and citing cases).
Instead, mail and wire fraud is more akin to phishing. A typical phishing scheme begins when a computer user receives an email from a phisher that seems to be "from a reputable company." After clicking the link, the user is taken to another webpage or a pop-up page, also purporting to be reputable. This new window asks the user for personal information. If provided, the phisher uses this information to make purchases, apply for credit cards, or simply steal the user's identity. The user believed he or she was dealing with the reputable company, when in reality, the user was not. The phisher deceived the user, not the computer. Thus, the SEC's attempted analogy proves inadequate.

Concerning the SEC's alleged support from the Model Penal Code, a careful reading shows that the Code does not contemplate computer hacking. Looking at section 223.3(1), for example, the text explicitly uses the term "other state of mind." This suggests that the one being deceived must have a state of mind. Similarly, subsection (2) requires a detrimental effect on the victim's "judgment of a transaction." It can be reasonably inferred that the Model Penal Code assumes that the one being deceived is human, unless the code assumes computers can make judgments. For subsection (3) to be applicable, a person must be able to have a "fiduciary or confidential relationship" with a computer. Fiduciary and confidential relationships only exist between humans. Thus, the Model Penal Code presumes a human is being deceived, not a computer. The SEC's flawed arguments highlight the need for the courts to make a determination of whether computers can be deceived.

IV. CAN A COMPUTER BE DECEIVED?

To violate Section 10(b), a computer hacker must engage in deception. It is crucial for the courts to determine whether a hacker can deceive a computer. If the courts rule that a computer cannot be deceived, then a hacker does not engage in deception simply by hacking into a computer. Since the hacker has not engaged in deception, the hacker cannot be tried as an inside trader. But the

113. Id.
114. Id.
115. Id.
116. Id.
117. Id.
118. MODEL PENAL CODE § 223.3(1) (1980).
119. Id. § 223.3(2).
120. Id. § 223.3(3).
121. BLACK'S LAW DICTIONARY 1401 (8th ed. 2004) (defining "relationship" as "[t]he nature of the association between two or more people") (emphasis added).
123. Id.
first step is to determine whether a computer can be deceived. In the first instance, it may seem that hacking into a computer is clearly deceptive. However, analogizing a computer to a simple mechanism, such as a door lock, demonstrates the weakness of that assertion.

A. Door-Lock Hypothetical

Assuming that a computer’s security system is merely a sophisticated door lock highlights the issue that many courts and commentators have overlooked. The hypothetical is as follows: accessing the information stored on a computer is analogous to accessing a room behind a closed door. A computer which is password-protected can only be accessed by one who has the correct username and password. Similarly, a door may be locked, making the room behind the door only accessible by key. Hacking into a computer—in the sense that an unauthorized hacker uses the username and password of an authorized person—is similar to gaining access to a room by using a key without the owner’s permission. Both cases would involve mere theft and unlawful access, and the user would only be liable for those offenses. Alternatively, hacking into a computer by such means as a buffer overflow attack would be more akin to picking a lock. The hacker gains access to the information in the computer, but uses an alternative method. Similarly, a door lock is picked when the lock’s inner-workings are manipulated in a manner that results in the door becoming unlocked as if a key was used.

No one would argue that a lock is deceived when an unauthorized person uses the key of an authorized person, or when a lock-pick is used. A door lock does not “think” an authorized person is using a key to unlock the door. Equally, a door lock does not “think” someone is using a key, when in fact someone is using a lock-pick. Burglary, for example, which can involve breaking into a lock,
does not frame the entry element as deceiving a lock. In this line of reasoning, a computer would not be deceived when a user employs a username and password without authorization, or uses a buffer overflow attack to gain the information inside a computer.

Thus, if the courts find that a computer cannot think, in the same way as a door lock cannot think, then a hacker will not be liable as an inside trader. Breaking into a computer and stealing information would then be mere theft. While some commentators argue that "mere thieves" should be liable for insider trading, courts have generally been firm in holding the contrary. The only way hackers could be prosecuted is if courts refrain from using an analogy similar to the lock-pick, and find that computers have the capacity to think. This way, the computers would be deceived—when a hacker uses either a username and password without authorization, a buffer overflow attack, or an alternative hacking method—and all the elements of Section 10(b) would be met. This raises the dispositive question: Do computers have the capacity to think?

B. Thinking Is Beyond a Computer’s Capacity

As the following discussion will show, theorists, scientists, and philosophers have long debated whether a computer can think. This Comment certainly will not provide a definitive answer to that question. However, if experts could show that computers think in a way similar enough to that of a human, then courts will have adequate support to rule that hackers can deceive computers for Section 10(b) purposes.

Some theorists argue that computers cannot think because thinking requires something more than just computation. A number of assertions have been offered, allegedly identifying what exactly it is that will never allow computers to have the capacity to think. The idea of "consciousness" requires something that is manifested in an immaterial capacity, and computers are made-up only of

129. See, e.g., CAL. PENAL CODE § 459 (providing no deception element).
130. See, e.g., Steinbuch, supra note 40, at 578 (laying out a theory that those who acquire material nonpublic information and trade upon it are culpable under current insider trading principles).
131. SEC v. Dorozhko, 606 F. Supp. 2d 321, 339 (S.D.N.Y. 2008) (“No federal court has ever held that those who steal material nonpublic information and then trade on it violate § 10(b).”).
133. Mitchell Waldrop, Can Computers Think?, in THE AGE OF INTELLIGENT MACHINES 63 (Raymond Kurzweil ed., 1990) (“[T]hinking is something going on in the brain all right, but it is not computation at all, thinking is something holistic and emergent—and organic and fuzzy and warm and cuddly and mysterious.”) (quoting Daniel C. Dennett, philosopher).
134. Dennett, supra note 132, at 186–91. These theorists view “thinking” as the ability to have consciousness. Id.
Consciousness requires an organic brain, whereas computers are inorganic by definition. Only naturally born entities can exhibit consciousness, which computers are not. Further, consciousness requires complexity, which computers cannot attain. The view that computers have the inability to think is also demonstrated by the difference in intelligence between a computer and a human brain.

1. Difference in Intelligence

"Intelligence" is defined by breaking it down into its individual components: "learning, reasoning, and the ability to manipulate symbols." "Learning" is defined as the acquiring of facts, the understanding of the relationship between those facts, and the implication of those facts. A computer’s ability to learn is different than a human’s ability to learn. While computers have the ability to remember billions of facts, computers lack the ability to understand the relationship between those facts. Conversely, humans cannot remember considerable amounts of facts with the same accuracy that computers demonstrate. Humans, however, do have the ability to comprehend the relationships between those facts. For instance, humans are able to understand the fine relationship between characters in a novel—an ability computers lack.

"Reasoning" is defined as "the ability to draw deductions and inferences from knowledge with the purpose of achieving a goal or solving a problem." Compared to computers, humans have a superior ability to make inferences and deductions from incomplete knowledge. From there, humans make decisions. Generally, a computer uses "hard rules," which means that a computer has a predetermined conclusion to a specific antecedent.

135. Id. at 187–88.
136. Id. at 187.
137. Id. at 188.
138. Id. at 190.
141. Id. at 17.
142. Id.
143. Id.; GLYNN, supra note 139, at 246 (stating that computers are better at “long or complex arithmetical problems” than the human brain is).
144. Kurzweil, supra note 140, at 17.
145. Id.
146. Id.
147. Id.
148. Id.
149. Id.
150. Id.
The capacity to manipulate symbols also differentiates humans from computers. Rather than being listed, symbols are usually arranged in complex patterns. Humans can understand patterns made up of symbols they are aware of, even if they learned the symbol in a different context. In contrast, computers have difficulty performing such tasks.

2. The Chinese Room

John Searle’s famous “Chinese Room” hypothetical demonstrates the view that computers have the inability to think. The hypothetical begins with a person (David), an English speaker with no understanding of Chinese, secluded in a room. By sliding slips of paper under the door, the experimenter gives David a story and a number of questions pertaining to the story; both the story and the questions written in Chinese. David also receives a description, written in English, supplying “an algorithmic way of answering the question as a native [Chinese] speaker might.” David uses the description to form new answers to the questions and then passes those answers on. Looking at David’s answers, one might think that he understands Chinese. But in reality, David does not understand a word of Chinese.

Similarly, Searle argues, a computer does not understand, even if it can answer questions. A computer simply “uses formal rules to manipulate abstract symbols.” And like David, who responded to questions in Chinese without understanding the language, the computer does not understand. However, if the language was English instead of Chinese, and David was an English speaker,
then the hypothetical would be analogous to what a human does.\footnote{166} The words suddenly have meaning, and David understands what is being said.\footnote{167}

Commentators have offered several counterarguments to Searle's Chinese Room hypothetical.\footnote{168} One argument claims the hypothetical is misleading.\footnote{169} Shuffling through the sheer number of slips of paper, which could number in the billions, to devise one answer could take years.\footnote{170} Searle responds by noting that David could just memorize all the information on the slips of paper.\footnote{171} But if that were the case, David would understand Chinese.\footnote{172}

Another counterargument is that, while David alone may not understand Chinese, the whole system (the room, the process of slipping questions and answers back and forth, the algorithmic way to answer questions, \textit{and} David) understands the language.\footnote{173} Similarly, a computer's central processing unit itself does not think, but is instead a component of a thinking system.\footnote{174}

Computers may not have that extra something that provides the same level of consciousness as humans, or consciousness at all. Clearly, a computer's intelligence is different from a human's intelligence. Searle's Chinese room hypothetical, however flawed, is informative. Relying on theories such as the Chinese Room, it seems a computer is akin to a door lock, unable to think.

C. Computers Can Think

1. The Turing Test

Other theorists suggest that computers do have the capacity to think. One of those theorists was the mathematician, Alan Turing, whose Turing Test was purported to determine whether something has the ability to think.\footnote{175} The concept behind the test is rather simple. Suppose there are two people and one computer.\footnote{176} The humans, A and B, and the computer, C, are all in separate rooms.\footnote{177} A, the judge in the exercise, asks B and C the same questions, and B

\begin{itemize}
\item \footnote{166} Id.
\item \footnote{167} Id.
\item \footnote{168} See id. at 64–66 (examining some of those counterarguments).
\item \footnote{169} Id. at 65.
\item \footnote{170} Id.
\item \footnote{171} Id.
\item \footnote{172} Id.
\item \footnote{173} Id.
\item \footnote{174} Block, \textit{supra} note 132, at 164.
\item \footnote{175} Id. at 127.
\item \footnote{177} Id. (explaining that a man and a computer are physically separated from an interrogator).
\end{itemize}
and C provide responses to these questions.\textsuperscript{178} If A cannot distinguish between B and C, then C, the computer, is intelligent and has the ability to think.\textsuperscript{179}

ELIZA was a program created to pass the Turing Test, and, in one of its versions, was designed to emulate a psychiatrist.\textsuperscript{180} The following provides a description of how ELIZA mimics a person:

[ELIZA] employs a group of simple but effective strategies. For example, it looks for "key words" on a list supplied by the programmer, e.g., "I", "you", "alike", "father", and "everybody". The words are ordered; for example, "father" comes before "everybody", so if you type in "My father is afraid of everybody", the machine will spit back one of its "father" responses, such as "WHAT ELSE COMES TO MIND WHEN YOU THINK OF YOUR FATHER?" If you type in "Everybody laughed at me", you will get one of its responses to "everybody", such as "WHO IN PARTICULAR ARE YOU THINKING OF?" It also has techniques that simultaneously transform "you" into "I", and "me" into "you" so that if you type in "You don’t agree with me", it can reply: "WHY DO YOU THINK THAT I DON’T AGREE WITH YOU?"\textsuperscript{181}

One program that passed the Turing Test was PARRY.\textsuperscript{182} PARRY used prearranged responses like ELIZA, and was programmed to answer as if it were a paranoid patient.\textsuperscript{183} When given PARRY’s responses, psychiatrists were unable to distinguish PARRY from real human patients.\textsuperscript{184} However, critics say the Turing Test is flawed, because whether a computer passes the test depends on the judge’s knowledge of computers.\textsuperscript{185} On the one hand, if the judge is exceedingly knowledgeable of intelligent computers, it will be more difficult for a computer program to pass the Turing Test.\textsuperscript{186} On the other hand, if the judge has no knowledge of computers whatsoever, a computer program will have a much better chance to pass the test.\textsuperscript{187} Whether the Turing

\begin{footnotes}
\textsuperscript{178}. \textit{Id.}
\textsuperscript{180}. Block, \textit{supra} note 132, at 128.
\textsuperscript{181}. \textit{Id.} at 128–29.
\textsuperscript{182}. See CREVIER, \textit{supra} note 179, at 137 (noting that psychiatrists were unable to distinguish PARRY from human patients). It is important to note that it is debatable as to whether what PARRY was able to accomplish actually amounts to passing the Turing Test. See FRANKLIN, \textit{supra} note 157, at 101 (arguing that "[t]o date, no machine has even come close to passing Turing’s test in its full glory").
\textsuperscript{183}. CREVIER, \textit{supra} note 179, at 137.
\textsuperscript{184}. \textit{Id.}
\textsuperscript{185}. Block, \textit{supra} note 132, at 127–28.
\textsuperscript{186}. \textit{Id.} ("A judge who was a leading authority on genuinely intelligent machines might know how to tell them apart from people.").
\textsuperscript{187}. See \textit{id.} at 128 ("A stupid judge, or one who has had no contact with technology, might think that a radio was intelligent.").
\end{footnotes}
Test actually measures a computer’s ability to think is questionable. Therefore, the Turing Test does not seem to provide courts with evidence necessary to conclude that computers can think for insider trading purposes.

2. Computing is Thinking

The support the courts need arises from the fact that a computer is analogous to a human brain in that they both process information. The practicality of the analogy depends on how in-depth one takes it. An in-depth analysis of how a computer functions compared to how a brain functions reveals how different both systems truly are. However, a simple analogy of the two systems offers courts the needed support to give computers legal consciousness. If computers can think, they can be deceived for insider trading purposes.

a. Detailed Processing Analogy

A computer consists of (1) a central processing unit, which, simply put, controls what goes on in the computer; (2) a collection of pigeon holes, each containing an address and capable of holding a number; (3) computer programs that direct the central processor to do specific acts at specific times; and (4) a screen, which displays what the central processing unit instructs it to do. This design, common in the majority of computers, operates one step at a time. This type of processing is called serial processing.

The human brain, however, performs parallel processing. This means that the human brain does not process in a linear manner or take single steps sequentially. While the term “hardware” is fitting for the computer, because the properties of the computer are static, there is no corresponding concept when it comes to the human brain. The synapses of the human brain may change their properties, and the complex circuitry of the human brain may change as well. The term “software,” which dictates the actions of the central processing unit, also does not have an equivalent in the human brain.

188. See GLYNN, supra note 139, at 245–46 (describing how both human brains and computers process information).
189. Id. (highlighting the differences between the processing of a computer and that of a human brain).
190. Id. at 245.
191. Id.
192. Id.
193. Id. at 246.
194. Id. at 245.
195. Id. at 246.
196. Id.
197. Id.
Another difference between the human brain and a computer is processing speed. While the precise processing speed of the human brain is unknown, it can process roughly 10 quadrillion calculations per second. The fastest computer in the world as of this writing, China's Tianhe-1A, can process 2.57 quadrillion calculations per second. Thus, even supercomputers have a ways to go before their processing speed equals that of the human brain. Additionally, the average personal computer is dwarfed in comparison to the human brain. A high-end home computer can only perform 111 billion calculations per second.

b. Simple Processing Analogy

A comprehensive comparison between a human brain and a computer, which focuses on the distinctions between the two, is clearly problematic. However, courts can adopt a simpler analogy which focuses on the fact that both computers and the human brain process information. How each processes information, whether serial or parallel, and the processing power of each is immaterial.

Theorists known as computationalists suggest a line of inferences to support their argument that computers have the ability to think. They argue that processing information is synonymous with thinking. "[I]nformation processing is computation, which is the manipulation of symbols . . . ." Therefore, contend computationalists, computers have
artificial intelligence. In other words, computers have the capacity to think, and thus can be deceived.

This simple line of inferences provides the courts with the support needed for a ruling that computers have the capacity to think for insider trading purposes. In other words, that computers have legal consciousness. Because computers have this capacity to think, in that they can process information, computers are distinguished from a door lock. When a person inserts a key or a lock-pick into a door lock, the lock does not process any information. However, when a person inputs information into a computer, the computer processes that information.

This is akin to a human brain.

V. SATISFYING THE DECEPTIVE DEVICE ELEMENT

When an inside trader conveys information to the human information source, the human receives and processes that information. The inside trader can deceive the human by making the human think one reality when another reality is true. The human falsely believes the insider will not trade on the information. The deception is complete when the insider actually trades on the information, as it was in O'Hagan.

When a hacker conveys information to a computer information-source, the computer likewise receives and processes the information. The hacker can deceive the computer by making the computer think that an authorized user is gaining access to the information, when in fact the hacker is an unauthorized user, or by using an alternative hacking method, such as a buffer overflow attack.

A human brain processes information, and thus thinks. A door lock does not process information, and thus does not think. Since a computer processes information, it thinks. Therefore, Section 10(b) will be satisfied because computer hacking will involve a deceptive device: deceiving the computer. This in itself gives courts enough ammunition to rule that computer hackers, who deceive computers to gain inside information, can be prosecuted under Section 10(b). Now, instead of having to analogize to other statutes, such as the Computer Fraud and Abuse Act, the SEC has a clear argument that computer hacking amounts to deception.

209. Crevier, supra note 179, at 9 (Artificial intelligence can be defined as the “science of making machines do things that would require intelligence if done by men.”).
210. See Glynn, supra note 139, at 245 (explaining how a computer operates).
211. Id.
212. See id. (describing how the human brain processes information).
214. See Glynn, supra note 139, at 245.
It is unquestioned that courts assume humans have the capacity to be deceived. Thus, if courts give computers personhood, computers will likewise have the capacity to be deceived. Giving personhood to computers, in the context of hacking and trading, is not wholly implausible. Non-human entities have had legal rights for centuries. Although it may be a legal fiction, courts have been open to bestow legal rights on non-human entities; one of the most well-known and debated entities with legal rights is the corporation.

A. Corporate Personhood

In 1947, Congress enacted 1 U.S.C. § 1, which provides, “In determining the meaning of any Act of Congress, unless the context indicates otherwise . . . the word[] ‘person’ . . . include[s] corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals . . . .” To the dismay of some, corporations have gained rights previously only conferred on individual humans. Corporations can own property, enter into contracts, act as trustees, and pay taxes. Corporations even have

216. JOHN CHIPMAN GRAY, THE NATURE AND SOURCES OF THE LAW 46 (Roland Gray ed., The Macmillan Co. 1972) (“Inanimate things may be regarded as the subject of legal rights, and, as such, entitled to sue in the courts. Such perhaps, were some of the temples in pagan Rome, and such seem often to have been church buildings and the relics of the saints in the early Middle Ages.”).
217. See id. at 53 (“[E]ven if a corporation be a real thing, it is yet a fictitious person . . . .”).
218. Christopher D. Stone, Should Trees Have Standing?—Toward Legal Rights for Natural Objects, 45 S. CAL. L. REV. 450, 452 (1972) (“The world of the lawyer is peopled with inanimate right-holders: trusts, corporations, joint ventures, municipalities, Subchapter R partnerships, and nation-states, to mention just a few.”).
219. Lawrence B. Solum, Legal Personhood for Artificial Intelligences, 70 N.C. L. REV. 1231, 1239 (1992) (“The most familiar examples of legal persons that are not natural persons are business corporations and government entities.”).
221. See generally Wheeling Steel Corp. v. Glander, 337 U.S. 562, 576–81 (1949) (Douglas, J., dissenting) (arguing that the Supreme Court should not have extended Fourteenth Amendment protections to corporations).
223. See Solum, supra note 219, at 1259 (“[T]he property of corporations is protected from taking without just compensation.”).
224. See generally Trustees of Dartmouth College v. Woodward, 17 U.S. 518 (1819) (holding that the Contracts Clause applies to corporations).
225. RESTATEMENT (THIRD) OF TRUSTS § 33(1) (2003) (“A corporation has capacity to take and hold property in trust . . . .”).
constitutional rights. Recently, the Supreme Court expanded corporations' First Amendment rights by allowing corporations to engage in political speech.228

Aside from giving corporations rights, courts have implicitly held that corporations can be deceived as well.229 In fact, some insider trading cases involve a defendant deceiving a corporation instead of an individual human.230 For example, in O'Hagan, the defendant had to have engaged in deception to be liable as an inside trader.231 The Court held that the defendant deceived his law firm, the source of the information, when the defendant traded on the confidential information.232 Thus, the defendant did not deceive a human being, but instead deceived his law firm.233

Similarly, in Dorozhko, if Dorozhko had not hacked the information, but instead had talked directly to a human representing IMS, he would have deceived the information supplier, IMS.234 Once again, a defendant deceived a corporation, not an individual human.

The doctrine of corporate personhood makes clear that the courts are willing to give legal rights to non-humans.235 If courts are willing to view corporations as "persons," it is no stretch for the courts to take the same view regarding computers.

B. Extending Personhood to Computers

As previously explained, a computer and human brain can both process information.236 While one may view a corporation as a system with working components, the system does not process information in the way a human brain or a computer does. Thus, a computer is much more analogous to a human brain

227. See Range Resources-Appalachia, LLC v. Blaine Township, 649 F. Supp. 2d 412, 417 (W. D. Pa. 2009) ("The United States Supreme Court has repeatedly recognized that corporations have the right to assert the very sort of constitutional claims alleged . . . ."); see also Fong Foo v. United States, 369 U.S. 141, 143 (1962) (applying Fifth Amendment protections to a corporation); Hale v. Henkel, 201 U.S. 43, 76 (1906) ("[A corporation] can only be proceeded against by due process of law, and is protected, under the Fourteenth Amendment, against unlawful discrimination.").

228. Citizens United v. FEC, 130 S. Ct. 876, 904 (2010) ("Political speech is indispensable to decisionmaking in a democracy, and this is no less true because the speech comes from a corporation rather than an individual."") (quoting First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 777 (1978))).

229. See United States v. O'Hagan, 521 U.S. 642, 648 (1997) ("[A] person who trades in securities for personal profit, using confidential information misappropriated in breach of a fiduciary duty to the source of the information" is guilty of violating § 10(b) and Rule 10b-5).

230. See, e.g., id. (describing how O'Hagan deceived his law firm, Dorsey & Whitney).

231. Id. at 650-51, 653-54.

232. Id. at 648.

233. Id.

234. GRAY, supra note 216, at 51 ("The powers granted by the State are not the rights of the men whose wills put them in motion, for it is not the interests of those individual men that are protected; but, by a dogmatic fiction, their wills are attributed to the corporation, and it is the corporation that has the rights.").

235. Stone, supra note 218, at 452.

236. GLYNN, supra note 139, at 245.
than a corporation is. In fact, scholars have explored the concept of providing rights to entities besides corporations previously.\textsuperscript{237} For instance, Christopher Stone, in his essay \textit{Should Trees Have Standing}, argued that natural objects should have rights.\textsuperscript{238} While his concern was the environment, Stone highlights a movement, however slight, towards providing legal rights to physical non-human objects.\textsuperscript{239} Further, the discussion of providing those rights to computers is already underway.\textsuperscript{240}

Opponents of personhood for computers offer a number of objections for their position.\textsuperscript{241} The objections mirror those arguments that computers lack the capacity to think.\textsuperscript{242} One argument is that only humans should be given personhood, computers are not humans, and thus computers should not be given personhood.\textsuperscript{243} However, computers are much more analogous to the human brain than corporations, in that both can process information.\textsuperscript{244} Since corporations have personhood, there is no reason computers should be denied personhood merely because they are not human. Another argument is that computers lack a "critical element of personhood."\textsuperscript{245} This element may be a soul, consciousness, intentionality, feelings, interests, or free will.\textsuperscript{246} But a corporation does not have a conscious, intentionality, feelings, interest, or free will. Further, legal reasoning should not depend on concepts that belong in the religious or philosophical realm.\textsuperscript{247}

It may be safe to say that computers one day will have personhood in the form of a number of rights.\textsuperscript{248} At the moment, however, and in the context of insider trading, computer personhood is not absolutely necessary. Yet, giving computers very limited personhood may provide an alternative means to prosecute inside traders under Section 10(b). Courts need not provide any specific rights to computers. Instead, courts should rule that computers have

\begin{itemize}
\item \textsuperscript{237} Stone, supra note 218, at 456 (arguing that legal rights should be given to non-humans).
\item \textsuperscript{238} \textit{Id.} ("I am quite seriously proposing that we give legal rights to forests, oceans, rivers and other so-called 'natural objects' in the environment—indeed, to the natural environment as a whole.").
\item \textsuperscript{239} \textit{Id.;} Soskis, supra note 176 ("At some point in the not-too-distant future, we might actually face a sentient, intelligent machine who demands, or who many come to believe deserves, some form of legal protection.").
\item \textsuperscript{240} Soskis, supra note 176 (presenting several arguments offered by others concerning legal rights for computers and robots).
\item \textsuperscript{241} Solum, supra note 219, at 1258–79.
\item \textsuperscript{242} Dennett, supra note 132, at 186–91; Solum, supra note 219, at 1258–62.
\item \textsuperscript{243} Solum, supra note 219, at 1258–62.
\item \textsuperscript{244} GLYNN, supra note 139, at 245.
\item \textsuperscript{245} Solum, supra note 219, at 1262.
\item \textsuperscript{246} \textit{Id.} at 1262–74.
\item \textsuperscript{247} \textit{Id.} at 1262–63 ("Political and legal decisions ought to be made in accord with the requirement of public reason. The requirement of public reasons is that political and legal decisions must be justified on grounds that are public. Public reason cannot rely on particular comprehensive religious and philosophical conceptions of the good.").
\item \textsuperscript{248} Soskis, supra note 176.
\end{itemize}
personhood in the sense that, like corporations, they can be deceived. This is not too fanciful of an idea in light of the fact that corporations do not have the same rights as humans—the courts have given them only a small number. If Dorozhko received the inside information from an agent of IMS, the courts would find that IMS, the corporation, was deceived. In a similar vein, courts can hold that a computer, given personhood like a corporation, is deceived if a hacker receives information from it.

VII. CONCLUSION

Computer hacking as a means for traders to gain inside information raises a novel issue for the courts. To prosecute hackers under Section 10(b), the hackers must act in a way that involves deception. Hacking into a computer only involves deception if the computer has the capacity to think.

For many years, theorists have argued about just that: whether computers have the capacity to think. One group of theorists, the computationalists, provides an argument that supplies a foundation for holding that computers can think, and thus can be deceived. Because computers process information, computers have the capacity to think. How information is processed, whether serial or parallel, is of no consequence. The result is a positive one. If computers have legal consciousness, inside traders who use computer hacking as an instrument to gain inside information can be prosecuted under Section 10(b).

For added support, courts can go one step further and grant computers personhood. This form of personhood will be very limited; computers will only be persons in that they can be deceived like corporations. If courts adopt the proposals set forth in this Comment, hackers like Dorozhko will not be able to evade prosecution under Section 10(b) simply because they gained their information through computer hacking.

249. GRAY, supra note 216, at 51.
252. See supra Part. IV (presenting the arguments of theorists on both sides of the debate).
253. Waldrop, supra note 133, at 63 (noting Allen Newell and Herbert Simon as proponents of this doctrine).
254. Id.