FROM THE OUTSIDE IN: A LAW AND ECONOMICS PERSPECTIVE ON INSIDER TRADING CASES INVOLVING CYBERCRIME

Jaclyn Collier*

I. Introduction

"It is doubtful whether any other type of public regulation of economic activity has been so widely admired as the regulation of the securities markets by the Securities and Exchange Commission."[1]

To many people, and certainly the Securities and Exchange Commission ("SEC"), it is categorically unfair for insiders who have access to material nonpublic information to trade on it for their own personal gain.[2] On the other side of the argument, the idea that insider trading is "just wrong" is generally not accepted by many law

* J.D. Candidate, Suffolk University Law School, 2017.

[1] George J. Stigler, *Public Regulation of the Securities Markets*, 37 J. BUS. 117, 117 (1964) (discussing the importance of regulating securities markets).

[2] *See, e.g.*, STEPHEN M. BAINBRIDGE, INSIDER TRADING LAW AND POLICY 166 (Found. Press 2014) (explaining the SEC's interests in having a powerful enforcement program to combat insider trading); Stephen Clark, *Insider Trading and Financial Economics: Where Do We Go From Here?*, 16 STAN. J.L. BUS. & FIN. 43, 48 (2010) (describing a renewed interest in insider trading by the SEC in response to the financial scandals of the early 2000s); Ronald J. Colombo, *Buy, Sell, or Hold? Analyst Fraud from Economic and Natural Law Perspectives*, 73 BROOK. L. REV. 91, 93 (2007) (arguing against law and economics approach to securities regulation as deficient for not taking social goals into consideration and being too heavily focused on wealth maximization)*; see also* Kim Lane Scheppele, *"It's Just Not Right": The Ethics of Insider Trading*, 56 L. & CONTEMP. PROBS. 123, 124 (1993) (arguing for regulation of insider trading). Scheppele recounts a passage from

 ISSN 1536-7983.

and economics intellectuals.[3] Despite the lack of agreement about whether insider trading should be illegal, hacking into another company's system in order to access the material nonpublic information that is then used to trade is itself a crime.[4] But is it insider trading?[5]

Insider trading has long been a significant element of the enforcement regime of the SEC.[6] In 2009, the *Dorozhko* decision in the Second Circuit opened the door to the SEC to seek enforcement against company outsiders who traded on material nonpublic information obtained through cybercrime;[7] however, the question remains whether it should.[8] Hackers are an interesting species for the SEC because the activities they engage in to obtain the material nonpublic information do not easily fit into the traditional definitions of insider trading.[9]

Through a law and economics analysis, this Note will discuss insider trading cases where traders traded on material nonpublic information obtained through commission of a cybercrime and whether the SEC should pursue those kinds of insider trading cases. Part II

Henry Manne's well-known book, *Insider Trading and the Stock Market*, where Manne minimizes ethical arguments against insider trading. *Id.* at 123.

[3] *See* Stephen Bainbridge, *The Insider Trading Prohibition: A legal and Economic Enigma*, 38 U. FLA. L. REV. 35, 49 (1986) (describing the deregulators' argument that Insider Trading actually benefits society and promotes market efficiency).

[4] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2015) (describing the unauthorized access to a computer system as a crime).

[5] *See* Michael D. Wheatley, *Apologia for the Second Circuit's Opinion in SEC v. Dorozhko*, 7 J.L. ECON. & POL'Y 25, 56 (2010) (questioning why the SEC pursued hackers for insider trading instead of the DOJ or aggrieved party pursuing the defendants for the other crimes (e.g., theft) leading up to the trades).

[6] *See* Jeffrey D. Bauman, *Loss and Seligman on Securities Regulation: An Essay for Don Schwartz*, 78 GEO. L.J. 1753, 1759 (1990) (reviewing LOUIS LOSS AND JOEL SELIGMAN, SECURITIES REGULATION (1989)) (describing the rise of insider trading brought by the SEC starting in 1961 with *In re Cady Roberts*). *See* Clark, *supra* note 2, at 48 (noting that despite a decline in prosecution of insider trading cases in the 1990s, SEC insider trading prosecutions have otherwise trended upward).

[7] *See* SEC v. Dorozhko, 606 F. Supp. 2d 321, 341 (S.D.N.Y. 2008), *vacated*, 574 F.3d 42, 51 (2d Cir. 2009) (holding that hackers may be liable under the misappropriation theory).

[8] *See* Wheatley, *supra* note 5, at 55 (arguing availability of private causes of action and criminal causes of action under cybercrime statutes).

[9] *See* Wheatley, *supra* note 5, at 56 (reasoning that these cases could have been brought effectively under other criminal statutes).

will provide historical background on insider trading law and the evolution of cybercrime as it relates to insider trading.[10] It will also discuss the classical law and economics arguments related to the regulation of insider trading. Part III will discuss the SEC's recent complaint in Dubovoy to give substance to the law and economics arguments around prosecution of insider trading cases involving hacking.[11] Part IV will argue that the existing law is not designed or intended to bring actions against company outsiders trading on material nonpublic information obtained though cybercrime.[12] Using economic efficiency analysis, Part V will show that the SEC should not focus on these cases because it is not a good use of resources for a government agency that has a limited budget.[13] Instead, these cases should be prosecuted as a cybercrime by the Department of Justice ("DOJ") and other law enforcement agencies, leaving the SEC to focus on investigating and prosecuting cases where its finite resources could be more effectively deployed.

II. History

A. Background on the Mandate of the SEC

The SEC's mandate is to protect investors through the maintenance of fair and orderly securities markets.[14] The Securities Exchange Act of 1934 ("Exchange Act"), a federal law that was implemented after the great 1929 stock market crash, was designed to

[10] *See infra* Part II.
[11] *See infra* Part III.
[12] *See infra* Part IV.
[13] *See infra* Part IV.B.
[14] *See The Investors Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, U.S. SEC. & EXCH. COMM'N, (June 10, 2013), *archived at* https://perma.cc/9B8C-BRNC (explaining the mission of the SEC to protect investors and provide access to "certain basic facts" about securities through public disclosure); Michael Geeraerts, *Hackers Who Steal and Trade on Inside Information Finally Fear the Securities and Exchange Commission and Section 10(b)*, 17 NO. 3 PIABA B.J. 253, 255 (2010) (pronouncing the essence of Section 10(b) as to "assure orderly and fair securities markets").

regulate the securities exchanges (e.g., the New York Stock Exchange).[15] The congressional hearings and reports preceding the passage of the Exchange Act demonstrate that in the wake of the 1929 crash there was public concern that market abuses caused the crash.[16] The Exchange Act established the SEC,[17] which was empowered through the act to regulate all aspects of the securities industry.[18] This broad authority is divided amongst numerous divisions and offices within the SEC.[19]

The Division of Enforcement is responsible for prosecuting insider trading cases.[20] It works closely with the Office of Compli-

[15] *See* BAINBRIDGE, *supra* note 2, at 25 (describing the Exchange Act as a response to the crash).

[16] *See* DUNCAN FLETCHER, STOCK EXCHANGE PRACTICES, S. REP. NO. 73-1455, at 5 (1934) (reporting "[i]n retrospect, the fact emerges with increasing clarity that the excessive and unrestrained speculation which dominated the securities markets in recent years, has disrupted the flow of credit, dislocated industry and trade, impeded the flow of interstate commerce, and brought in its train social consequences inimical to the public welfare"). Later, the report goes on to state: "[t]he exposures before the subcommittee of the evils and abuses which flourished on the exchanges, and their disastrous effects upon the entire Nation, finally compelled the conclusion, even among partisan advocates of the exchanges themselves, that Federal regulation was necessary and desirable." *Id.* at 81. *See also* George C. Nnona, *International Insider Trading: Reassessing the Propriety and Feasibility of the U.S. Regulatory Approach*, 27 N.C. J. INT'L L. & COM. REG. 185, 205 (2001) (outlining the scope of discussion in Congress leading up to the passage of the Exchange Act).

[17] *See* Securities Exchange Act of 1934, 15 U.S.C. § 78d (2015) (establishing the SEC and describing the requirement that is be composed of five commissioners appointed by the President).

[18] *See The Investors Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, *supra* note 14 (describing the SEC's authority to regulate the securities market as "includ[ing] the power to register, regulate, and oversee brokerage firms, transfer agents, and clearing agencies as well as the nation's securities self-regulatory [sic] organizations (SROs)").

[19] *See The Investors Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, *supra* note 14 (detailing the divisions and offices of the SEC, which are Corporate Finance, Trading and Markets, Investment Management, Enforcement, and Economic and Risk Analysis). The Offices are far more numerous and include the Office of the General Counsel, the Office of Compliance Inspections and Examinations, and the Office of Administrative Law Judges. *Id.*

[20] *See The Investors Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, *supra* note 14 (explaining the role of the Division of Enforcement as the law enforcement arm of the SEC which has the authority to prosecute cases and work closely with other enforcement agencies).

ance Inspections and Examinations and other areas of the SEC to obtain evidence of potential violations of securities laws.[21] The SEC is required to provide reports annually to Congress on its enforcement effort, the success of which is critical to the SEC's ability to maintain political support, which in turn allows the agency to get increases in funding.[22] In its fiscal year 2014, the SEC reported an all-time record in enforcement; however, serious questions have been raised about the methodology used to create those reports.[23] Despite the availability of information from the SEC on its enforcement program, it remains difficult to measure with any degree of accuracy the actual success of the program.[24]

B. SEC Insider Trading Theories

Insider trading is a term used to describe the act of trading a security for illicit gains based on information not known to others that has the potential to significantly impact the price of that security.[25] That information is typically referred to as material nonpublic

---

[21] *See The Investors Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, *supra* note 14 (noting that the Division of Enforcement obtains evidence from a variety of sources and conducts private investigations).

[22] *See* Urska Velikonja, *Reporting Agency Performance: Behind the SEC's Enforcement Statistics*, 101 CORNELL L. REV. 901, 908 (2016) (reviewing the requirements of the SEC to testify before Congress, report on enforcement performance and leverage enforcement successes to justify budget increases).

[23] *See* Velikonja, *supra* note 22, at 976 (arguing that the SEC's process for calculating enforcement statistics is deeply flawed). Velikonja also asserts that SEC often double-counts enforcement actions, which in turn inflates its enforcement numbers. *Id.* at 931.

[24] *See* Velikonja, *supra* note 22, at 948-49 (explaining that the SEC reports on the amount of monetary penalties it ordered, as opposed to the penalties it actually collected). In 2014, the SEC only collected approximately half of what it ordered. *Id.*

[25] *See* BAINBRIDGE, *supra* note 2, at 1 (illustrating examples and providing detail on the definition of insider trading); *SEC Enforcement Actions: Insider Trading Cases*, U.S. SEC. & EXCH. COMM'N, (Jan. 28, 2015), *archived at* https://perma.cc/326Z-M6ED (describing insider trading as "when a security is bought or sold in breach of a fiduciary duty or other relationship of trust and confidence while in possession of material, nonpublic information").

information.[26] Insider trading has its roots in state corporate law,[27] but insider trading as we know it today has its roots in federal securities law.[28] In addition to creating the SEC, the Exchange Act also created the primary law governing the regulation of insider trading.[29] The Exchange Act was intended to protect investors and increase the public's confidence in the securities markets by promoting fairness and transparency in the purchase and sale of securities.[30] For the most part, the SEC is empowered to prosecute insider trading cases from section 10(b) from the Exchange Act, a catchall provision that

[26] *See SEC Enforcement Actions: Insider Trading Cases*, *supra* note 25 (calling the information used to trade material nonpublic information).

[27] *See* BAINBRIDGE, *supra* note 2, at 11 (providing background on the history of insider trading common law found in state corporate law). Under late nineteenth century state corporate law, liability arose in instances of actual fraud, which include fraudulent concealment of a material fact and misrepresentation. *Id.* at 11-12. An important state case, *Goodwin v. Agassiz*, 186 N.E. 659 (Mass. 1933), is still included in most casebooks for corporation law. *Id.* at 14. *Goodwin* is reflective of most of the state law at the time, which held that company directors and officers have no duty of disclosure if they are trading on an impersonal stock exchange, unless special circumstances exist that give the directors a responsibility to communicate facts. *Id.*

[28] *See* BAINBRIDGE, *supra* note 2, at 25 (providing historical overview of the implementation of federal insider trading laws).

[29] *See* BAINBRIDGE, *supra* note 2, at 25 (stating that the Exchange Act encapsulates the principal law covering insider trading).

[30] *See* DUNCAN FLETCHER, STOCK EXCHANGE PRACTICES, S. REP. NO. 73-1455, at 54 (1934) (pronouncing the purpose of the Exchange Act was to provide a "free and honest market" that would not be brought down by deceptive practices and calling attention to the Exchange Act specifically prohibiting devices that would otherwise be used to "artificially" inflate or depress prices of securities traded on exchanges)*; see also* BAINBRIDGE, *supra* note 2, at 25 (describing the circumstances and legislative history that led to the passage of the Exchange Act); Robert Bailey, Jr., *SEC v. Cuban: The Misappropriation Theory and its Application to Confidentiality Agreements Under Section 10(b) and Rule 10b5-2 of the Securities Exchange Act of 1934*, 35 DEL. J. CORP. L. 539, 540 (2010) (explaining the driving force for the Exchange Act was to promote fairness and transparency in the market).

prohibits "any manipulative or deceptive device or contrivance",[31] and Rule 10b-5,[32] and Rule 10b5-1, promulgated thereunder.[33]

The SEC has historically focused on prosecuting insider trading cases under two main theories of liability: the "classical theory" and the "misappropriation theory".[34] It is a violation of section 10(b) and Rule 10b-5 under the classical theory when a corporate insider[35]

---

[31] *See* 15 U.S.C. § 78j(b) (2015); Chiarella v. United States, 445 U.S. 222, 235 (1980) (pronouncing Section 10(b) as "a catchall provision, but what it catches must be fraud"); BAINBRIDGE, *supra* note 2, at 26 (articulating the nature of section 10(b) as a catchall provision intended to capture securities fraud not covered anywhere else in the regulation).

[32] *See* 17 C.F.R. § 240.10b-5 (2015) (codifying the prohibition against using interstate commerce, mails or facility of national securities exchanges to commit fraud). Rule 10b-5 states:

> 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 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.

[33] *See* 17 C.F.R. § 240.10b5-1 (2015) (defining when a trade is considered trading on the basis of material nonpublic information).

[34] *See* Howard J. Kaplan et al., *The Law of Insider Trading*, A.B.A. SEC. LITIG. ANN. CONF. 3 (2012), *archived at* https://perma.cc/8WW8-P3G2 (articulating the two theories of insider trading liability under section 10(b)); *Insider Trading*, BLACK'S LAW DICTIONARY (9th ed. 2009) (defining classical insider trading as "[t]he use of material, nonpublic information in trading the shares of a company by a corporate insider or other person who owes a fiduciary duty to the company"). The misappropriation theory of insider trading is defined as "deceitful acquisition and misuse of information that properly belongs to persons to whom one owes a duty." *Id.* This Note will focus primarily on the misappropriation theory of insider trading as it relates to hackers.

[35] *See* Kaplan, *supra* note 34, at 3 (defining a corporate insider as an officer or director who owed a duty to the corporation and its shareholders).

trades the corporation's securities based on material nonpublic information about the corporation.[36] Under the classical theory, the Supreme Court has imposed a requirement to abstain from trading or disclosing the information.[37] The misappropriation theory expands insider trading liability.[38] Under the misappropriation theory, a corporate outsider misappropriates material nonpublic information he received from a source to whom he owed a duty and then uses that information to trade.[39] In this instance the trader has deceived the source of the information and breached his duty to the source.[40] The SEC promulgated Rule 10b5-2 in 2000, which provides detail about certain circumstances when a "duty of trust or confidence" arises for

---

[36] *See* Kaplan, *supra* note 34, at 3 (outlining the classical theory of insider trading)*; see also SEC Enforcement Actions: Insider Trading Cases*, *supra* note 25 (describing the areas of authority provided to the SEC under the Exchange Act); *The Laws That Govern the Securities Industry*, U.S. SEC. & EXCH. COMM'N, (Oct. 1, 2013), *archived at* https://perma.cc/6MJM-EB26 (describing insider trading laws under the Securities Exchange Act of 1934). The SEC explains:

> The securities laws broadly prohibit fraudulent activities of any kind in connection with the offer, purchase, or sale of securities. These provisions are the basis for many types of disciplinary actions, including actions against fraudulent insider trading. Insider trading is illegal when a person trades a security while in possession of material nonpublic information in violation of a duty to withhold the information or refrain from trading.

Id.

[37] *See Chiarella*, 445 U.S. at 228-29 (imposing a duty to abstain from trading or disclose material nonpublic information on corporate insiders); Elizabeth A. Odian, *SEC v. Dorozhko's Affirmative Misrepresentation Theory of Insider Trading: An Improper Means to a Proper End*, 94 MARQ. L. REV. 1313, 1315-16 (2011) (discussing the Supreme Court's historical interpretation of 10(b) and Rule 10b-5); Kaplan, *supra* note 34, at 3 (reviewing how, in the *Chiarella* case, the Court also held that if a trader does not owe the duties that a corporate insider does, then it could not be successfully convicted of insider trading).

[38] *See* United States v. O'Hagan, 521 U.S. 642, 652 (1997) (holding that a company outsider violates § 10(b) when he trades on material nonpublic information in violation of a duty owed to the source of the information); Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 SW. J. INT'L L. 259, 267 (2011) (elucidating how *O'Hagan* expanded insider trading liability).

[39] *See O'Hagan*, 521 U.S. at 652 (holding that using confidential information to trade securities is a breach of duty to the source of the information).

[40] *See id.* (holding that a fiduciary's use of confidential information to trade securities in breach of a duty to the source defrauds the source because it is in contradiction of the purpose for which the fiduciary has the information).

which a breach would be considered a misappropriation of information in violation of section 10(b).[41]

Over the years, the SEC continuously tries to broaden its span of control under the insider trading laws.[42] More recently, the SEC has attempted to expand insider trading theory to prohibit people with no fiduciary duty to the company or a third party from trading on the

---

[41] *See* 17 C.F.R. § 240.10b5-2 (2015). Section (b) of Rule 10b5-2(b) states:

> (b) Enumerated "duties of trust or confidence." For purposes of this section, a "duty of trust or confidence" exists in the following circumstances, among others:
>
> (1) Whenever a person agrees to maintain information in confidence;
>
> (2) Whenever the person communicating the material nonpublic information and the person to whom it is communicated have a history, pattern, or practice of sharing confidences, such that the recipient of the information knows or reasonably should know that the person communicating the material nonpublic information expects that the recipient will maintain its confidentiality; or
>
> (3) Whenever a person receives or obtains material nonpublic information from his or her spouse, parent, child, or sibling; provided, however, that the person receiving or obtaining the information may demonstrate that no duty of trust or confidence existed with respect to the information, by establishing that he or she neither knew nor reasonably should have known that the person who was the source of the information expected that the person would keep the information confidential, because of the parties' history, pattern, or practice of sharing and maintaining confidences, and because there was no agreement or understanding to maintain the confidentiality of the information.

Id.

See also Kaplan, *supra* note 34, at 5 (providing background on Rule 10b5-2). Despite the promulgation of Rule 10b5-2, the parameters of the duty and relationship have been tricky for courts to define. *See e.g.* S.E.C. v. Cuban, 634 F. Supp. 2d 713, 730-31 (N.D. Tex. 2009), *vacated*, 620 F.3d 551 (5th Cir. 2010) (finding no liability for Cuban because there was no breach of his contractual duties to the corporation).

[42] *See Odian*, *supra* note 37, at 1316 (asserting that the SEC continues to increase its regulatory authority to prosecute all trades made based on informational advantages).

basis of material nonpublic information.[43] In the *Cuban* case, the SEC alleged that Cuban breached his contractual obligation to maintain the confidentiality of certain information.[44] The case, which was decided in the Fifth Circuit, culminated in a jury trial finding for Cuban.[45] In the *McGee* case, the SEC alleged that McGee had an agreement, as a member of Alcoholics Anonymous ("AA"), to keep information another member discussed with him confidential.[46] The court agreed that McGee breached his duty to his fellow AA member by trading on material nonpublic information gleaned from that member.[47]

Over the last several years the SEC has also pursued insider trading cases against company outsiders with no duty to the company or its shareholders who are even further removed – hacker who break into computer systems, steal material nonpublic information, and then trade on it.[48] In *Dorozhko,* the Second Circuit directly addressed insider trading by hackers, holding that the hacker must have lied or

[43] *See Cuban*, 620 F.3d at 557 (disputing the S.E.C.'s position on prohibiting people with no fiduciary duty from trading on the basis of material nonpublic information); *Dorozhko*, 574 F.3d at 48 (explaining that District Courts have concluded that fiduciary duty is required); S.E.C. v. McGee, 895 F. Supp. 2d 669, 682 (E.D. Pa. 2012) (stating that a history of sharing and maintaining confidences gives to a duty). The criminal case was appealed and decided by the Third Circuit in *United States v. McGee*, 763 F.3d 304 (3d Cir. 2014) *cert. denied*, 135 S. Ct. 1402 (2015). The court found that there was a relationship of trust between the defendant and the person from whom he received the material nonpublic information. *Id.* at 317. *See also* BAINBRIDGE, *supra* note 2, at 170 (discussing the *Cuban* case and the SEC's attempt to broaden the scope of duty under the misappropriation theory to include contractual agreements imposing a duty of confidentiality).

[44] *See* Bailey, *supra* note 30, at 541 (describing the Cuban case).

[45] *See* Christopher G. Green et al., *The Mark Cuban Verdict and What It Means for Misappropriation and Insider Trading Law*, 27 INSIGHTS 9, 13 (2013) (stating that the jury found for Cuban because the SEC had not proven the disputed elements).

[46] *See McGee*, 895 F. Supp. 2d at 681 (describing the allegations that members of AA had a history of sharing confidential information and an agreement to keep personal or business related information confidential).

[47] *See id.* at 684 (stating that the allegations would demonstrate that McGee had a duty keep the information he learned from another member about a pending merger confidential).

[48] *See, e.g.*, *Dorozhko*, 574 F.3d at 51 (holding that hackers may be liable under the misappropriation theory if there was some deception in the gaining access to the system from which the hacker obtained the information); S.E.C. v. Lohmus, Haavel & Viiesemann et al., SEC Litigation Release No. 20134, 2005 WL 3309748 (Nov. 8, 2005) (announcing complaint against defendants who stole confidential press releases through hacking and traded on the information in the releases in advance of

committed some fraud to find an affirmative misappropriation.[49] It may strain credulity to label computer hacking a lie, but the misappropriation theory is the only theory that even remotely suits insider trading cases for hackers.[50] Although the court found that it is a violation of Rule 10b-5 for a hacker to misrepresent his identity to gain access to the information, it also indicated that a hacker who gains access to a system without any misrepresentation does not violate the Rule.[51]

C. Second Circuit Decides Section 10(b) Captures (Some) Hackers

In the complaint against Dorozhko, the SEC alleged that Dorozhko violated Section 10(b) and Rule 10b-5 by hacking into systems and computer networks that contained information about a company's pending earning announcement, thereby gaining access to material nonpublic information.[52] That same day, Dorozhko used the

---

their public dissemination); S.E.C. v. Blue Bottle Ltd., SEC Litigation Release No. 20018, 2007 WL 580798 (Feb. 26, 2007) (describing complaint against defendants where defendants hacked into computer systems to obtain news releases before public issuance in order to trade on the information in advance of issuance)*; see also* Wheatley, *supra* note 5, at 39-41 (defining cases where defendants gained unauthorized access to material nonpublic information stored electronically as a "nonmanipulative intrusion").

[49] *See Dorozhko*, 574 F.3d at 51 (holding that it is deceptive for a hacker to misrepresent his identity to gain access to a system and the information contained in that system and then to steal that information); BAINBRIDGE, *supra* note 2, at 172 (explaining the decision in *Dorozhko* and the requirement that the hacker somehow lied in order to find an affirmative misrepresentation)*; see also* John C. Coffee, Jr., *Mapping the Future of Insider Trading Law: Of Boundaries, Gaps, and Strategies*, 2013 COLUM. BUS. L. REV. 281, 285 (2013) (arguing that the Second Circuit ignored the broader definition of the word "deception" and as such construed the term unnecessarily narrowly in the opinion).

[50] *See* BAINBRIDGE, *supra* note 2, at 171-72 (outlining the lack of other law under which hacker insider trading cases can be prosecuted and noting that defining hacking as a lie is "a rather considerable stretch").

[51] *See Dorozhko*, 574 F.3d at 51 (pointing out that it is not clear whether "exploiting a weakness in an electronic code to gain unauthorized access is 'deceptive,' rather than being mere theft").

[52] *See* Complaint at ¶ 3, *Dorozhko*, 574 F.3d at 44 (describing the allegations against defendant). The complaint does not explain in any detail how Dorozhko actually hacked into the systems from which he improperly obtained material nonpublic information. *Id.*

information obtained by hacking to buy put options ("puts") on the company's stock.[53] The purchases Dorozhko made represented about 90% of all puts purchased in the company's stock in the six weeks leading up to the date Dorozhko purchased the puts.[54] By buying these puts, Dorozhko was betting that the company's stock price would decline before the puts expired.[55] Later that day, the company announced that its earnings were 28% below the consensus expectations of Wall Street analysts.[56] At the open of the market the next morning, the company's stock price dropped roughly 28%, making the puts much more valuable.[57] Almost immediately, Dorozhko sold all of the puts he bought the previous day and realized $286,456.59 in net profits.[58] The broker Dorozhko used to execute these trades detected the unusual trading activity and notified the SEC.[59]

[53] *See id.* (detailing the conduct of the defendant in purchasing out-of-the-money and at-the-money put options). An option is a derivative, meaning it derives its value from an underlying asset, such as the price of a stock. *See Investor Bulletin: An Introduction to Options*, U.S. SEC. & EXCH. COMM'N (Mar. 18, 2015), *archived at* https://perma.cc/D7AJ-UFAK (providing definitions and descriptions of how derivatives work). A put option contract provides the buyer with the right (but not the obligation), for a specified period of time, to sell shares of an underlying stock at the strike price for a specified period of time. *Id.* The buyer expects that the price of the underlying stock will decrease during the time of the contract. *Id.* The seller of the put "is obligated to buy those shares from the buyer of the put option who exercises his or her option to sell on or before the expiration date." *Id.* A put option is "out-of-the-money" when the strike price (i.e., the price at which the buyer of the put can purchase the underlying stock) is lower than the stock's actual price. *Id.* A put option is "at-the-money" when the strike price for the stock is the same as the stock's actual price. *Id.* Out-of-the-money puts trade typically at a discount because unless something happens that would cause the stock price to drop to match the strike price, the puts will not be exercised and will be worthless upon expiration. *See also* John W. Labuszewski, CME GROUP, *Managing Currency Risks with Options* 7 (2010), *archived at* https://perma.cc/5X4W-9LDE (describing economics of out-of-the-money puts).

[54] *See Dorozhko*, 574 F.3d at 44 (explaining the magnitude of the defendant's purchases in comparison to historical market activity for the company's puts).

[55] *See id.* (citing the SEC's brief, which indicated that the purchase of these options was very risky).

[56] *See id.* (noting that the earnings announcement was 28% below expectations).

[57] *See id.* (describing defendant's actions to sell all of the puts he owned within six minutes of the market open).

[58] *See id.* (stating defendant's net profit on the put sales).

[59] *See id.* at 44 (explaining that defendant's brokerage firm notified the SEC).

The SEC sought a preliminary injunction to freeze the proceeds of the put transaction in Dorozhko's brokerage account.[60] The District Court decided that Dorozhko did not violate Section 10(b) because computer hacking did not meet the definition of "deceptive" as characterized by the Supreme Court, and there was no breach of fiduciary duty.[61] On appeal, the SEC argued that Dorozhko committed fraud in violation of Section 10(b) by affirmatively misrepresenting himself to access the system from which the material nonpublic information was obtained, regardless of whether he owed or breached a fiduciary duty.[62] The Second Circuit held that fiduciary duty is not a required element of every Section 10(b) violation.[63]

The Second Circuit court also held that depending on the conduct in which the hacker engaged, computer hacking could be construed as a "deceptive device".[64] In dicta, the Second Circuit court

---

[60] *See Dorozhko*, 574 F.3d at 45 (detailing the SEC's request for a preliminary injunction).

[61] *See id.* (reciting the District Court's holding that there could not be a violation of Section 10(b) without deceptive conduct including a breach of fiduciary duty).

[62] *See id.* at 45-46 (explaining the SEC's theory that the fraud violating Section 10(b) was computer hacking). The court also noted that the SEC did not argue that the defendant breached any fiduciary duty as part of this scheme. *Id.* at 48.

[63] *See id.* at 48 (holding that the Supreme Court decisions the District Court relied upon did not establish that a fiduciary duty was a requirement of every Section 10(b) violation). This decision prompted a large amount of commentary on whether this decision was consistent with existing Supreme Court precedent. *See, e.g.*, James A. Jones, *Outsider Hacking and Insider Trading: The Expansion of Liability Absent a Fiduciary Duty*, 6 WASH. J. L. TECH. & ARTS 111, 119-20 (2010) (explaining that the Second Circuit split from the Fourth, Fifth, and Seventh Circuits in deciding that a fiduciary breach is not required to violate Section 10(b) or Rule 10b-5); Cohen, *supra* note 38, at 268 (explaining that *O'Hagan* showed the Supreme Court's willingness to protect the marketplace and its participants through the imposition of broader liability); Wheatley, *supra* note 5, at 25 (describing the controversial nature of the Second Circuit's decision, despite the fact that it may have reached the "right" result); Steven M. Bainbridge, *The Second Circuit's Egregious Decision in SEC v. Dorozhko*, PROFESSORBAINBRIDGE.COM (July 29, 2009), *archived at* https://perma.cc/G5Q5-BSFM (reviewing leading authorities and commentary that support the District Court's conclusion that a fiduciary duty is a required element of a violation of Section 10(b)).

[64] *See Dorozhko*, 574 F.3d at 51 (holding a hacker misrepresenting his identity to gain unauthorized access "off limits" information is "plainly 'deceptive,'" but it is not clear whether gaining unauthorized access by exploiting a flaw in the electronic code is "deceptive"); *see also* Robert T. Denny, *Beyond Mere Theft: Why Computer Hackers Trading on Wrongfully Acquired Information Should Be Held Accountable Under the Securities Exchange Act*, 2010 UTAH L. REV. 963, 969-70

addresses the SEC's arguments about the two ways that hacking can be deceptive.[65] The court states that a hacker stealing information otherwise unavailable to him by misrepresenting his identity to access the information is "plainly deceptive".[66] However, the court was not willing to go so far as saying that identifying a weakness in computer code and then exploiting it could be more than theft and meet the requirements of being a "deceptive device".[67]

The case was remanded to the District Court to determine whether the computer hacking Dorozhko engaged in to obtain access to the material nonpublic information on which he subsequently traded included a fraudulent misrepresentation considered "deceptive" per Section 10(b).[68] On remand, the District Court granted summary judgment to the SEC, ordering Dorozhko to disgorge gains of $286,456.59, pay prejudgment interest of $6,930.94, and pay a civil penalty of $286, 456.59.[69] The motion was unopposed because by the time the case made its way back to District Court, Dorozhko had vanished.[70] As a result, there was no resolution to the question of

(considering the Second Circuit reasoning in Dorozhko that fiduciary duty was a sufficient, but not a necessary condition for the court to find deception under Section 10(b)).

[65] *See Dorozhko*, 574 F.3d at 50-51 (describing the SEC's description of computer hacking as tricking, circumventing, or bypassing computer security for the purpose of gaining unauthorized access to information and computer systems and networks in order to steal data).

[66] *See id.* at 51 (declaring misrepresentation of identity in order to obtain information that is off limits and then stealing the information meets the ordinary meaning of the word deceptive).

[67] *See id.* (expressing uncertainty as to whether other types of hacking such as breaking source code would be considered deceptive).

[68] *See id.* (remanding for consideration of whether the hacking involved a "deceptive" fraudulent misrepresentation in violation of Section 10(b)).

[69] *See Order SEC v. Dorozhko, S.D.N.Y., No. 07 Civ. 9606 (NRB), 3/24/10*, UNIVERSITY OF DENVER: STURM COLLEGE OF LAW 2 (Mar. 23, 2010), *archived at* https://perma.cc/A4KE-8JHN (granting the SEC's motion for summary judgment, which went unopposed); *see also* Kaplan et al., *supra* note 34, at 15 n.79 (noting SEC was granted summary judgment); Cohen, *supra* note 38, at 264 n.43 (describing the judgment and order for defendant to pay a civil penalty, pay prejudgment interest and disgorge gains).

[70] *See Order SEC v. Dorozhko, S.D.N.Y., No. 07 Civ. 9606 (NRB), 3/24/10*, *supra* note 69, at 2 (indicating that defendant's counsel had not received any communication from defendant and thus did not submit any opposition to the SEC's motion for summary judgment); Kaplan et al., *supra* note 34, at 15 n.79 (noting the defendant disappeared and the SEC was granted summary judgment).

whether hacking is "deceptive" within the meaning of Section 10(b).[71]

D. Insider Trading Crimes

Insider trading laws also carry the potential for criminal liability and penalties.[72] The criminal cases are prosecuted by the DOJ.[73] Although the DOJ uses the same securities fraud provisions of the exchange act to prosecute insider trading, it can add on or include other pertinent criminal statutes in its prosecution.[74] The DOJ often indicts for wire fraud and conspiracy to commit wire fraud in connection with an insider trading case.[75] In a case where a computer was used

[71] *See* Odian, *supra* note 37, at 1329 (explaining that unopposed summary judgment left the question of whether computer hacking is "deceptive" unanswered). Thomson Financial, the newswire service that was hacked by the defendant, decided to refrain from exploring the details of how the defendant hacked into its system in order to protect "certain trade secrets". *Id.* at 1329 n.126.

[72] *See* 15 U.S.C. § 78(u)(d)(1) (2015) (describing the power of the SEC to refer criminal cases to the Department of Justice).

[73] *See id.* (providing discretion to the DOJ to prosecute criminal insider trading cases without a referral from the SEC)*; see also* BAINBRIDGE, *supra* note 2, at 141 (explaining the autonomy of the DOJ to bring its own insider trading cases).

[74] *See* United States v. Turchynov, No. 15-CR-390(MCA), 2015 WL 4764144, ¶ 112-121, 122-23 (D.N.J. Aug. 6, 2015) [hereinafter New Jersey Indictment] (declaring allegations against defendants for: (1) conspiracy to commit wire fraud and (2) wire fraud).

[75] *See* 18 U.S.C. § 1343 (2015) (making it a crime for anyone who "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice"). 18 U.S.C. § 1349 (2002) criminalizes attempts and conspiracies to commit wire fraud. *Id. See also* Gerald A. Polcari, *A Comparative Analysis of Insider Trading Laws*, 13 SUFFOLK TRANSNAT'L L.J. 167, 176 (1989) (describing the ability of the DOJ to prosecute insider trading activity under wire fraud statutes); Joel Seligman, *A Mature Synthesis: O'Hagan Resolves "Insider" Trading's Most Vexing Problems*, 23 DEL. J. CORP. L. 1, 12 (1998) (highlighting the Supreme Court's affirmance of the DOJ's ability to prosecute insider trading activity under wire fraud statutes).

to commit fraud, the DOJ may also leverage certain crimes promulgated under the Computer Fraud and Abuse Act ("CFAA").[76]

The criminal sanctions in the Exchange Act allow for monetary penalties and jail time.[77] On the criminal side of insider trading, there is also a push to increase penalties, including jail time.[78] For example, in the *Galleon* case, hedge fund manager Raj Rajaratnam was convicted of insider trading in the then-highest sentence ever given for insider trading.[79] The SEC and DOJ worked closely together on this case, which has been touted as a great success by both groups.[80]

---

[76] *See* New Jersey Indictment, *supra* note 74, ¶ 1 (alleging that the Defendants engaged in conspiracy to commit fraud and related activity in connection with computers, and fraud and related activity in connection with computers in violation of the Computer Fraud and Abuse Act).

[77] *See* 15 U.S.C. § 78ff(a) (2015), which states:

> Any person who willfully violates any provision of this chapter . . . shall upon conviction be fined not more than $5,000,000, or imprisoned not more than 20 years, or both, except that when such person is a person other than a natural person, a fine not exceeding $25,000,000 may be imposed.

Id.

[78] *See* Peter J. Henning, *Punishments for Insider Trading Are Growing Stiffer*, N.Y. TIMES: WHITE COLLAR WATCH (Sept. 9, 2014), *archived at* https://perma.cc/GKV9-UJXV (describing the increases in penalties for insider trading).

[79] *See* Henning, *supra* note 78 (describing Rajaratnam's sentence as one of the heaviest prison terms ever given for insider trading); Press Release, U.S. Dep't of Justice, Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Insider Trading Charges Against Former Galleon Portfolio Manager Rengan Rajaratnam (Mar. 21, 2013) (on file with the United States Department of Justice) (explaining the results of the case and publicizing the cooperation between the SEC and DOJ).

[80] *See* Press Release, U.S. Dep't of Justice, *supra* note 79 (lauding the agencies' collaborative work on the Galleon case)*; see also* Han Shen, *A Comparative Study of Insider Trading Regulation Enforcement in the U.S. and China*, 9 J. BUS. & SEC. L. 41, 61 (2008) (outlining the process by which the SEC will work in conjunction with the DOJ on an insider trading case through referrals to the DOJ for investigation and parallel investigations).

E. Cybercrime Statutes

At least for now, the "traditional theft" of hacking into a computer system sans the Second Circuit's narrowly-defined interpretation of misrepresentation does not give rise to insider trading liability.[81] Insider trading notwithstanding, hacking into a system and taking information does give rise to liability and criminal sanctions under cybercrime statutes and regulations.[82] United States cybercrime statutes include inchoate crimes as well.[83] These are often referred to as access offenses because the conduct involves accessing another computer to commit the crime.[84] An access crime such as

---

[81] *See* BAINBRIDGE, *supra* note 2, at 172 (reiterating district court's comments in Dorozhko that the Supreme Court has considered a breach of fiduciary duty to disclose or abstain an essential element of a section 10(b) violation); Brian A. Karol, *Deception Absent Duty: Computer Hackers & Section 10(b) Liability*, 19 U. MIAMI BUS. L. REV. 185, 208 (2011) (noting that traditional theft is not normally deceptive and thus falls outside of Section 10(b)).

[82] *See* Computer Fraud and Abuse Act, 18 U.S.C § 1030(a)(2) (2015). This section of the code punishes anyone who:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer;

Id.

The term "protected computer" includes a computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B) (2015); s*ee also Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATORS (June 2, 2015), *archived at* http://perma.cc/2239-PY9Z (providing list of all state statutes relevant to computer crimes).

[83] *See* 18 U.S.C. § 1030(b) (providing that "whoever conspires to commit or attempts to commit an offense" under 18 U.S.C. § 1030(a) can also be punished under the statute).

[84] *See* JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME 48 (Cambridge Univ. Press, 2d ed. 2015) (describing instances where a hacker gains access to a computer

hacking into a non-governmental system is considered a misdemeanor if the hacker intentionally accesses a computer, either without authorization or in excess of authorization, to obtain information from a protected computer.[85] This type of crime rises to the level of a felony when it is "committed for commercial advantage or private financial gain, or committed in furtherance of any criminal or tortious act, or the value of the information obtained exceeds $5,000."[86] The punishments can be severe and range from a fine up to imprisonment for up to twenty years.[87]

F. Law and Economics of Insider Trading

Since the publication of Henry Manne's groundbreaking book, *Insider Trading and the Stock Market*,[88] the law and economics debate has continued to impact securities regulation and enforcement.[89] The majority of law and economics discussion on insider trading focuses on whether it should be regulated at all.[90] Over the

as target intentionally and without rights to do so); Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 2 (2014) (describing typical cybercrimes).

[85] *See* H. Marshall Jarrett et al., *Prosecuting Computer Crimes*, U.S. DEP'T JUST. 16, *archived at* https://perma.cc/8P2P-Y7X9 (summarizing 18 U.S.C. § 1030(a)(2) and providing information about what constitutes a misdemeanor under the statute).

[86] *See id.* (describing elements of a felonious violation of 18 U.S.C. § 1030(a)(2)).

[87] *See* 18 U.S.C. § 1030(c) (citing the punishments for an offense of committing fraud and related activity in connection with computers or an attempt or conspiracy to do so).

[88] HENRY G. MANNE, INSIDER TRADING AND THE STOCK MARKET (Free Press, 1966).

[89] *See* BAINBRIDGE, *supra* note 2, at 175 (explaining impact of Manne's book on the law and economics debate about insider trading); Alexandra Padilla, *How Do We Think About Insider Trading? An Economist's Perspective on the Insider Trading Debate and Its Impact*, 4 WASH. & LEE J.L. ECON. & POL. 239, 242 (2008) (elucidating how Manne's book revolutionized the debate on insider trading, particularly from a law and economics perspective).

[90] *See e.g.*, Colombo, *supra* note 2, at 93 (arguing against law and economics approach to securities regulation as deficient for not taking social goals into consideration and being too heavily focused on wealth maximization); Padilla, *supra* note 89, at 240 (indicating no consensus among law and economics scholars regarding insider trading prohibitions); Colombo, *supra* note 2, at 124 (explaining the argument that the only reason under a pure law and economics theory to regulate trade would be to maximize societal wealth)*; see also* Jie Hu & Thomas H. Noe, *The Insider Trading Debate*, FEDERAL RESERVE BANK OF ATLANTA 37 (1997), *archived at* https://perma.cc/D2N9-3QZZ (describing the focus of the bulk of insider trading literature on whether it should be regulated at all).

years there has been significant discussion about whether the Exchange Act was even intended to prohibit insider trading.[91] Regardless, prohibitions against insider trading are now deeply ingrained in securities jurisprudence and enforcement.[92] Some pro-regulation arguments are non-economic and focus on the social costs and concerns over the fairness of insider trading.[93] Others argue that insider trading is not a cost effective way to promote market efficiency because it harms investors and issuers.[94]

[91] Legislative history shows that Congress has considered the idea of whether insider trading should be more specifically defined, but declined to do so. *See* John P. Anderson, *Greed, Envy, and the Criminalization of Insider Trading*, 2014 UTAH L. REV. 1, 3 Fn.6 (2014) (describing Congressional hearings on insider trading and decision to avoid adding specific language to further define insider trading); BAINBRIDGE, *supra* note 2, at 25-26 (positing that diligent inspection of the legislative history of the Exchange Act does not suggest that regulation of insider trading was part of the Act's original purpose).

[92] *See* BAINBRIDGE, *supra* note 2, at 29 (pointing out that modern insider trading jurisprudence is based on judicial opinions and SEC administrative actions, and somewhat removed from the legislative history and statutes).

[93] *See* Bainbridge, *supra* note 3, at 49 (noting that pro-regulation arguments underscore insider trading as unfair and having high social costs). The fairness argument revolves around the idea that "insider trading causes rational investors to refrain from trading, to incur search costs to avoid the insider's informational advantage, and to demand premiums as compensation for the risk of insider trading. Both the individual investor and society as a whole are therefore injured by insider trading." *Id.* at 55. *See also* BAINBRIDGE, *supra* note 2, at 190 (describing non-economic arguments used to justify regulation of insider trading).

[94] *See* Bainbridge, *supra* note 3, at 49 (highlighting arguments for regulation, namely that insider trading lacks cost effectiveness in relation to promoting market efficiency). There are other economic pro-regulation arguments that pertain to the breach of fiduciary duty. *Id.* These arguments will not be discussed here because hackers who are corporate outsiders are unlikely to have a fiduciary duty to the company. *See also* BAINBRIDGE, *supra* note 2, at 190 (describing economic arguments for the regulation of insider trading).

Many law and economics theories have been applied to the insider trading question, including the Coase theory,[95] Kaldor-Hicks efficiency theory,[96] property analysis,[97] cost-benefit analysis of regulation.[98] Under the Coase theorem, economists argue that in a world with zero transaction costs, insider trading could be regulated through private contracting between the firm and the insiders, which would allow for optimal allocation of the property right.[99] For example, a corporation could implement a compensation scheme that allows for the corporate agent who created the innovation that would cause the stock price to recover the value of her innovation through a purchase of company stock while that innovation is still material nonpublic information.[100] Consequently, when the successful innovation was announced, the stock price would rise, and the corporate agent would be able to reap her reward.[101] Kaldor-Hicks looks at whether the party who is made better off by the transaction could compensate any party

[95] *See* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 29 (1960) (positing that in a world of zero transaction costs, property rights will be allocated according to their most efficient uses).

[96] *See* Bainbridge, *supra* note 3, at 65 (describing the normative "Chicago School" claims of allocative efficiency). Kaldor-Hicks efficiency occurs if those whose position increases could fully compensate those whose position diminishes with a net gain in wealth. Jules L. Coleman, *Efficiency, Utility, and Wealth Maximization*, 8 HOFSTRA L. REV. 509, 513 (1980).

[97] *See* Wheatley, *supra* note 5, at 52-53 (describing the property rights approach to insider trading regulation models).

[98] *See* John C. Coates, *Cost-Benefit Analysis of Financial Regulation: Case Studies and Implications*, 124 YALE L.J. 882, 888 (2015) (reiterating that cost-benefit analysis is and has been part of administrative law analysis).

[99] *See* Laura Nyantung Beny, *Insider Trading Laws and Stock Markets Around the World: An Empirical Contribution to the Theoretical Law and Economics Debate*, 32 IOWA J. CORP. L. 237, 252-54 (2007) (applying the Coase theorem to insider trading in a world without government regulation). This theory is not applied in the "real world" because there is governmental regulation of insider trading. *Id.* at 253-54. Even if there were no government regulation of insider trading, there still would be difficulty in negotiating insider trading contracts because of the effect of transaction costs. *Id.* at 254. Two main transaction costs are enforcement costs and negotiation costs. *Id.*

[100] *See* Bainbridge, *supra* note 3, at 46 (explaining Manne's application of the Coasian theory of law and economics to a compensation scheme that permits insider trading).

[101] *See* Bainbridge, *supra* note 3, at 46 (concluding that in this compensation scheme a successful innovation that causes the stock price to rise will allow the corporate agent to recover the value of their innovation through insider trading).

who is made worse off.[102] This theory also focuses on the value of the "thing," such as material nonpublic information that the stock price will decrease, and measures efficiency based on whether or not the person who trades on that information would be in a position to compensate the person who was made worse off by trading later when the stock price was lower.[103]

A property rights analysis looks at the company's information as its exclusive property for which misappropriation of that information constitutes fraud.[104] This theory, which is based on older insider trading law, focuses on a property right in the material nonpublic information which would make it illegal for an investor to trade for her own benefit on that information.[105] This theory does not require that the person trading for her own benefit have a duty to the company.[106]

Another law and economics question examines cost benefit analysis and which prosecutorial authority should handle insider trading cases.[107] From a law and economics perspective, prosecuting insider trading cases is costly to the SEC in time and resources, the costs of which ultimately trickle down to the investing public.[108] The

---

[102] *See* Coleman, *supra* note 96, at 513 (describing Kaldor-Hicks efficiency and the concept that the "winner" must only have the ability to pay the "loser," not that he actually must do so).

[103] *See* Coleman, *supra* note 96, at 513-14 (explaining how the Kaldor-Hicks efficiency depends on the ability of the person who was made better off to have been made sufficiently better off such that he could compensate anyone who was made worse off by the transaction).

[104] *See* Wheatley, *supra* note 5, at 53 (explaining the property rights approach in the context of the corporation's nonpublic information being property for its exclusive use and benefit.)

[105] *See* Odian, *supra* note 37, at 1345 (reviewing the property rights approach to insider trading, stemming from *In re Cady Roberts & Co.*, 40 S.E.C. 907 (1961)).

[106] *See* Odian, *supra* note 37, at 1345 (asserting that removing the fiduciary duty requirement would allow for a property rights theory to prosecute insider trading hackers).

[107] *See* Jill E. Fisch, *Start Making Sense: An Analysis and Proposal for Insider Trading Regulation*, 26 GA. L. REV. 179, 232-33 (1991) (discussing outcomes of insider trading suits if those cases were relegated to derivative suits under state law and positing outcomes in the absence of insider trading enforcement by the SEC).

[108] *See* BAINBRIDGE, *supra* note 2, at 175 (describing the considerable resources expended to investigate and prosecute insider trading); Harvey L. Pitt & Karen K. Shapiro, *Securities Regulation By Enforcement: A Look Ahead At the Next Decade*, 7 YALE J. ON REG. 149, 171 (1990) (discussing the limited nature of governmental resources and the need to be efficient in selection of cases to pursue and prosecute,

SEC can also maintain efficiency through settlements,[109] and maintaining a high profile or visibility for its enforcement program.[110] The SEC's activity in this area implies that it can keep a laser-like focus on insider trading cases, continually broadening the scope of insider trading under new and novel theories and more aggressively prosecuting those cases.[111]

III. Facts

A. The Case Against Dubovoy et al.

In August 2015, the SEC filed a complaint and the DOJ filed criminal charges in one of the largest computer hacking insider trading schemes ever prosecuted.[112] Defendants engaged in this scheme for at least five years, with hackers and traders working together to gather the information and then trade on it for profits alleged to be

---

focusing on deterrence); Marleen A. O'Connor, *Toward a More Efficient Deterrence of Insider Trading: The Repeal of Section 16(b)*, 58 FORDHAM L. REV. 309, 363 (1989) (concluding that the use of public resources to pursue insider trading cases is more efficient as a deterrence strategy).

[109] *See* Pitt & Shapiro, *supra* note 108, at 179 (explaining SEC's reliance on settlements as an integral part of an efficient enforcement regime).

[110] *See* Pitt & Shapiro, *supra* note 108, at 184 (describing the visibility of the SEC's enforcement program as essential, creating an illusion that the Commission is omnipresent and more likely than not to identify illegal activity).

[111] *See* Patrick Craine & Lashon Kell, *Prosecuting Insider Trading: Recent Developments and Novel Approaches*, 59 THE ADVOC. (TEXAS) 45, 46 (2012) (explaining the SEC's commitment to pursuing "new and novel theories" that go well beyond the traditional definitions and legal foundations of liability for insider trading); Press Release, Sec. & Exch. Comm'n, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015) (on file with the United States Securities & Exchange Commission) (quoting Andrew Ceresney, Director of the SEC's Division of Enforcement, "[o]ur use of innovative analytical tools to find suspicious trading patterns and expose misconduct demonstrates that no trading scheme is beyond our ability to unwind").

[112] *See* Press Release, U.S. Dep't of Justice, Nine People Charged In Largest Known Computer Hacking And Securities Fraud Scheme (Aug. 11, 2015) (on file with the United States Department of Justice) (announcing criminal indictments of nine people for hacking into newswire services to obtain material nonpublic information and then using the information to make trades for illicit profit); Press Release, Sec. & Exch. Comm'n, *supra* note 111 (announcing civil fraud charges against 32 defendants for the scheme taking place over a five year period, using advanced techniques to hack into newswire services, steal material nonpublic information and then use the information to trade).

over $100 million.[113] Hacking to obtain the information was a departure from the methods used in traditional insider trading schemes, but the trades they used to make a profit were what likely tipped off the SEC in the first place: short-dated out-of-the-money options.[114]

B. The SEC's Complaint

The SEC complaint divides the Defendants into two groups: hacker Defendants and trader Defendants.[115] The SEC alleges that over the span of five years, the Defendants hacked into newswire services, obtained material nonpublic information, and then worked with the network of traders all over the world to trade on that information for profit.[116]

Newswire services publish press releases for companies that are publicly traded.[117] These press releases contain important infor-

---

[113] *See* Press Release, Sec. & Exch. Comm'n, *supra* note 111 (describing the scheme as taking place over a five-year timeframe and amassing more than $100 million in illicit profits). Interestingly, the DOJ press release alleges approximately $30 million in illegal profits. Press Release, U.S. Dep't of Justice, *supra* note 112.

[114] *See* Matt Levine, *Why Not Insider Trade on Every Company?*, BLOOMBERG VIEW (Aug. 11, 2015), *archived at* https://perma.cc/Z4FZ-5ACW (describing the common insider trading scheme of buying short-dated out-of-the-money call options, which is a strategy that the SEC monitors for insider trading, and noting that the traders in this case traded in out-of-the-money put options); U.S. SEC. & EXCH. COMM'N, *supra* note 53 (giving a description of how puts and calls work).

[115] *See Complaint for Violations of the Federal Securities Laws*, SEC. & EXCH. COMM'N 5-6 (Aug. 10, 2015), *archived at* https://perma.cc/Q4HC-UFPA (introducing the Defendants as "hacker defendants" and "trader defendants"). The complaint is against 17 people and 15 companies. *Id.* at 1. The companies' purported businesses range from construction and real estate to hedge funds and proprietary trading funds. *Id.* at 12-17.

[116] *See id*. at 5 (summarizing the complaint). As of January 20, 2016, two of the trader Defendants have pleaded guilty to one count of conspiracy to commit wire fraud. *Id. See* Jonathan Stempel, *New Guilty Plea in Big U.S. Insider Trading Hacking Case*, REUTERS (Jan. 20, 2016), *archived at* https://perma.cc/HZ8G-RZXF (relaying the guilty pleas of trader Defendants Igor Dubovoy and Alexander Garkusha)*; see also* Levine, *supra* note 114 (citing the indictment as describing the traders using puts to profit from the material nonpublic information).

[117] *See Complaint for Violations of the Federal Securities Laws*, *supra* note 115, at 6 (describing the activities of newswire services as editing and publishing press releases on behalf of publicly-traded companies in the United States). Newswire services are considered repositories for material nonpublic information. *Id.* at 21.

mation about the company's business, such as quarterly earnings announcements and major personnel or business changes.[118] The publicly-traded company provides the draft press release to the newswire services in advance of publishing.[119] The newswire service stores the press release until it is time for it to be issued.[120] Until the press release is issued, the information contained in press releases is material nonpublic information.[121]

The hackers and traders did the majority of their work in the window of time between when the newswire service receives the press release from the publicly-traded company and when the newswire service issues the press release.[122] The hackers hacked into the computer systems of the newswire services to access the press releases before they were published.[123] Although the complaint does not contain much information about how the hackers actually did the hacking, it alleges that they used "deceptive means" to access the newswire system, including using stolen usernames and passwords to pose as authorized users, employing malicious computer software that could delete evidence of the hacking, concealing their identity and location when hacking into the newswire services' systems, and use of "back-door access-modules."[124] After obtaining the material

[118] *See id*. (defining the types of information typically contained in press releases).
[119] *See id.* (describing the process for press release drafting, distribution, and storage).
[120] *See id.* (illustrating the press release process after drafting but before issuance).
[121] *See id.* (explaining that the information in press releases is made up of material nonpublic information.)
[122] *See Complaint for Violations of the Federal Securities Laws*, *supra* note 115, at 21-22 (describing the window of time for the Defendants to take advantage of and trade on material nonpublic information). This window of time could be anywhere between several minutes and several days. *Id.* at 21.
[123] *See id.* at 22 (providing detail on how the Defendants took advantage of the time window by hacking in and obtaining material nonpublic information from press releases that were not yet issued). The complaint alleges that the hackers stole over 100,000 press releases before they were issued. *Id.* at 24.
[124] *See id.* at 22 (describing means of hacking). The complaint contains relatively little information about how the actual hacking was committed, containing only two paragraphs about how the hacker Defendants gained access to the newswire services systems. *Id.* at 22, 55. The complaint does not provide any specifics on how these tactics were used by the Defendants to perpetrate the hacking. *Complaint for Violations of the Federal Securities Laws*, *supra* note 115, at 22. By comparison, the complaint includes eleven detailed examples how the material nonpublic information from stolen press releases was used and the trading activity in

nonpublic information from the unpublished press releases, the hackers provided the information to traders through various secret means in exchange for a flat fee or a percentage of the profits the traders made on the trading.[125]

C. Department of Justice Indictments

The criminal charges are more expansive than the SEC's case.[126] The indictments charge the Defendants with a series of securities related and computer hacking related crimes.[127] While the alleged facts are the same, the indictments also get into much more detail about how the hackers obtained the information from the newswire services.[128] The hackers used several techniques to hack into the newswires.[129] The hackers engaged in programming attacks, which allowed the hackers to gain unauthorized access to a network

---

those eleven securities. *Id.* at 38-55. None of the examples contain any information on how the press releases were stolen. *Id.* The criminal indictments include more information about the hacker Defendants' activities. *See* United States v. Korchevsky, No. 15-CR-381, 2015 WL 4749247, ¶ 31 (Aug. 5, 2015) [hereinafter New York Indictment] (alleging hackers used malware, phishing attempts and other "surreptitious infiltration of [the newswires'] servers"); New Jersey Indictment, *supra* note 74, ¶¶ 45, 56 (describing alleged use of malware, phishing, stolen login credentials to obtain the press releases).

[125] *See* New Jersey Indictment, *supra* note 74, ¶ 65 (explaining the way that the hacker Defendants provided the information to and were compensated by the trader Defendants). The traders employed various trading schemes to take advantage of the material nonpublic information. *Id.* at ¶ 119.

[126] *See* Press Release, U.S. of Dep't Justice, *supra* note 112 (describing the charges stated in the indictments). There are two indictments, one for the District of New Jersey and one for the Eastern District of New York. *Id.* The Department of Justice case is more expansive because it brought charges for other crimes in addition to securities fraud. *Id.*

[127] *See* New York Indictment, *supra* note 124, ¶¶ 45-59 (presenting charges against the Defendants). The charges include wire fraud and securities fraud. *Id.* at ¶¶ 50-51, 52-53. *See also* New Jersey Indictment, *supra* note 74, ¶ 112-48 (presenting charges against the Defendants). The Defendants are charged with wire fraud, securities fraud, fraud and related activity in connection with computers, and aggravated identity theft. *Id.*

[128] *See* New Jersey Indictment, *supra* note 74, ¶¶ 40-64 (detailing the methods by which the hacker Defendants were able to illegally enter the newswire services' networks).

[129] *See* New Jersey Indictment, *supra* note 74, ¶ 16 (alleging that the hackers stole confidential press releases by gaining unauthorized access through various methods).

by using a series of programming instructions.[130] They also used malware,[131] phishing,[132] and "bruted" or stolen usernames and passwords.[133] The hacker Defendants repeatedly accessed the newswire services through these methods and then provided the information to trader Defendants through a "stolen release server".[134]

---

[130] *See* New Jersey Indictment, *supra* note 74, ¶¶ 40-42 (describing Structured Query Language ("SQL") and SQL Injection Attacks as using the programming language SQL to gaining unauthorized access to computers that are connected to the internet); New York Indictment, *supra* note 124, ¶ 34 (explaining Defendants' use of SQL Injection Attacks to steal over 900 press releases). SQL is a programming language designed to manage and retrieve data stored in network databases. New York Indictment, *supra* note 124, ¶ 18.

[131] *See* New Jersey Indictment, *supra* note 74, ¶¶ 16, 32-33 (defining malware and explaining how Defendants used malware to access the newswire services' networks); New York Indictment, *supra* note 124, ¶¶ 17, 32 (explaining that the use of malware like "PHP scripts" allowed the hackers to move freely through the newswire's network and access press releases)*; see also* New Jersey Indictment, *supra* note 74, ¶ 25 (describing malware as malicious software designed to obtain unauthorized access to computers, gather information from those computers, and evade detection); New York Indictment, *supra* note 124, ¶ 32 (noting the hackers also used unauthorized "PHP scripts" to retrieve press releases on the newswire's network).

[132] *See* New Jersey Indictment, *supra* note 74, ¶¶ 26, 45 (explaining phishing and the details of the phishing scheme); New York Indictment, *supra* note 124, ¶ 22 (defining phishing as an attempt to obtain unauthorized access to computers by sending emails that appeared legitimate and from trustworthy sources, but in fact contained malware).

[133] *See* New Jersey Indictment, *supra* note 74, ¶¶ 23, 58 (defining "bruting" and the use of "bruted" login credentials); New York Indictment, *supra* note 124, ¶¶ 21, 33 (explaining "bruting" and describing how the hackers use a file containing user IDs and associated hashed passwords)*;* New Jersey Indictment, *supra* note 74, ¶ 23 (stating Brute Force Attacks or "bruting" refer to running programs to decrypt data and check each potential or password until the correct password is divulged). This information may then be used to decrypt strings of encrypted data that were generated when a word passed through an algorithm that was designed to encrypt the information. *Id.* The strings of encrypted data are called "password hashes." *Id.* The hackers stole login usernames and passwords of several employees of one of the newswire services. *Id*. at ¶ 143.

[134] *See* New Jersey Indictment, *supra* note 74, ¶ 36 (describing how hacker Defendants shared the press releases by creating servers that allowed the trader Defendants to access the press releases before they were released so that the traders could use the material nonpublic information to trade ahead of the release's issuance). The traders were instructed to conceal their IP addresses and other information that would identify their network providers to avoid detection. *Id.* at ¶ 67*; see also* New York Indictment, *supra* note 124, ¶ 35 (claiming hackers also used email, phone calls, and internet messaging to disseminate information to the traders).

IV. Analysis

A. Duty, Deception, and Devices in Dubovoy

The SEC's decision to pursue the hacker Defendants in the *Dubovoy* case raises substantial questions about long-standing interpretations of insider trading law. Computer hacking and fraudulently obtaining information through cybercrime are certainly crimes;[135] however, the securities law as it exists today does not clearly support making hackers liable under Section 10(b).[136] The two generally accepted theories of insider trading – the classical and misappropriation theories – each require a duty either to the company or the person from whom the material nonpublic information was obtained.[137] If the Defendants in *Dubovoy* had a duty, it would have been to either the newswire services or the companies whose press releases were being published by the newswire services,[138] and the complaint does not indicate that the Defendants owed a duty to either.[139]

Absent a duty, the most meaningful precedent the SEC can leverage is the Second Circuit holding in *Dorozhko* indicating that a

---

[135] *See* Odian, *supra* note 37, at 1333 (noting that computer hacking may be characterized as fraudulent conduct, although not necessarily securities fraud); Geeraerts, *supra* note 14, at 278 (noting that hackers can be punished under a number of other statutes, like the Computer Fraud Abuse Act, for crimes such as computer fraud as well as the more traditional crimes of wire and mail fraud that are not specifically designed to address insider trading).

[136] *See* Denny, *supra* note 64, at 969-70 (reviewing the circuit split and describing it as a disagreement on whether it is possible for a "deceptive device" to exist under Section 10(b) without a fiduciary duty); Geeraerts, *supra* note 14, at 255-56 (stating that technology has tested the regulatory power of the SEC, despite its authority being adaptable to changing technology). Before *Dorozhko*, insider trading under Section 10(b) had not been applied to a computer hacker who was a corporate outsider owing no fiduciary duty. *Id.* at 256.

[137] *See Dorozhko*, 574 F.3d at 45 (explaining that the SEC's argument against the defendant did not rely on either of the two existing theories of insider trading, both of which required a duty).

[138] *See id.* (reviewing the district court's opinion, which reasoned that if a fiduciary duty were owed, it would have been to the newswire service or the company whose securities were traded based on material nonpublic information).

[139] *See Complaint for Violations of the Federal Securities Laws*, *supra* note 115, at 5-6 (summarizing the complaint, which does not mention a duty to anyone on the part of the trader Defendants or hacker Defendants).

fiduciary duty may not be required for every Section 10(b) violation.[140] The difficulty with *Dorozhko*, and what makes it risky for the SEC, is court's decision to parse the definition of "deceptive device" down to such a level of detail that it has the potential to make every hacking case into a technology assessment for the judge.[141] The hacker Defendants are likely to argue long-standing Supreme Court precedents which have looked for some duty, if not a fiduciary duty, in order to find insider trading.[142] The hacker Defendants may leverage the circuit split and argue cases from the Fifth Circuit requiring breach of a duty.[143] Another case that could end up being influential in *Dubovoy* is the *McGee* decision in the Third Circuit because, although it does not address hacking, it delves deeply into the duty concept under Section 10(b) and the contours of Rule 10b5-2(b)(2).[144]

If the court is swayed in the SEC's favor and holds that a duty is not required, the SEC will then need to prove that the conduct the hacker Defendants engaged in was a "deceptive device."[145] The issue of what types of cybercrime may be deemed a "deceptive device"

---

[140] *See Dorozhko*, 574 F.3d at 45 (noting that the SEC's claim is a claim of fraud). The court discusses this in further detail later in the opinion when it reviews the existing Supreme Court opinions on insider trading. *Id.* at 48-49. The court reasons that while a breach of a fiduciary duty satisfies the "deceptive device" requirement under Section 10(b), it is not always required. *Id.* at 49. Rather there is always an affirmative duty not to mislead in commercial dealings. *Id. See also* Odian, *supra* note 37, at 1328-29 (describing the *Dorozhko* decision as an affirmative misrepresentation case for which there has been no contravening Supreme Court case requiring a duty and distinguishing the Supreme Court decisions that addressed fraud by nondisclosure).

[141] *See* Odian, *supra* note 37, at 1344 (arguing that either Congress or the Supreme Court needs to adopt a new theory of insider trading involving hacking, or "deceptive theft" to capture insider trading hackers).

[142] *Supra* Section II.B.

[143] *See Cuban*, 620 F.3d at 557 (finding no duty for Cuban); *see also* Denny, *supra* note 64, at 969 (reviewing the Fifth Circuit holding in Regents v. Credit Suisse First Boston, Inc. that there must be some breach of fiduciary duty for a deceptive device to exist under Section 10(b)).

[144] *See* United States v. McGee, 763 F.3d at 312-13 (stating that the Court disagreed with the *Chevron* interpretation of fiduciary duty in rule 10(b) and 10b5-2(b)(2)*; see also McGee*, 895 F. Supp. 2d at 681-82 (defining "duty" as not necessarily having to meet the threshold of fiduciary-level of duty).

[145] *See Dorozhko*, 606 F. Supp. 2d at 328 (granting the SEC's unopposed motion for summary judgment); Denny, *supra* note 64, at 970 (pointing out that even if a court finds that a duty is not required, the hacker's conduct still must be found to be a deceptive within the meaning of Section 10(b) and Rule 10b-5).

was never reached in *Dorozhko*,[146] but will necessarily need to be reached in *Dubovoy* to find the Defendants guilty.[147] As the SEC has done in other cases where it attempted to expand its authority,[148] it will likely use this as an opportunity to shape the definition of "deceptive device" to its advantage.[149] This case could give the SEC the opportunity to create a low bar for what hacking activities are considered a deceptive device.[150]

The activities of the hacker Defendants in *Dubovoy* seem even further attenuated from existing insider trading law, which does not clearly support making hackers with no duty being liable under Section 10 and Rule 10b-5, because according to the complaint, they did not engage in any trading.[151] In *Dorozhko*, the court looked at the

[146] *See Dorozhko*, 574 F.3d at 50-51 (noting that the district court never reached the question of whether "deceptive" in its ordinary meaning includes computer hacking, or whether the computer hacking involved any misrepresentation)*; see also* Geeraerts, *supra* note 14, at 271 (indicating that the Second Circuit was unsure if exploiting a system's security weakness could be "deceptive").

[147] *See Dorozhko*, 574 F.3d at 51 (stating that the court would need to determine whether the Dorozhko's hacking activities met the definition of a "deceptive device or contrivance" under Section 10(b) and Rule 10b-5).

[148] *See* Odian, *supra* note 37, at 1316 (describing the SEC's ongoing push to whittle away at the Supreme Court's narrow interpretations of insider trading rules); Clark, *supra* note 2, at 48-50 (detailing the SEC's continued and increased interest in insider trading enforcement and the methods by which the SEC has broadened its authority).

[149] *See* BAINBRIDGE, *supra* note 2, at 172 (indicating that the Second Circuit's decision in *Dorozhko* encouraged the SEC's "end run" around the "carefully established" fiduciary duty requirement).

[150] *See* BAINBRIDGE, *supra* note 2, at 172 (conjecturing that the *Dorozhko* case sets an important precedent for the SEC to work with courts in circumventing Supreme Court jurisprudence on insider trading); Geeraerts, *supra* note 14, at 267 (surmising that the Second Circuit intended to broaden the SEC's power when it held that hacking, even without a breach of fiduciary duty, could meet the definition of a "deceptive, affirmative misrepresentation").

[151] *See Complaint for Violations of the Federal Securities Laws*, *supra* note 115, at 5-6 (delineating the two groups of Defendants as "hacker defendants" and "trader defendants"). Throughout the complaint, the SEC separates the activities of the hacker Defendants and trader Defendants. *Complaint for Violations of the Federal Securities Laws*, *supra* note 115, at 22, 25, 26. *See also* Denny, *supra* note 64, at 970 (reiterating scholarly arguments that hackers are thieves and should not necessarily be liable for insider trading). *But see* Geeraerts, *supra* note 14, at 272-73 (discussing the open-endedness of the Dorozkho decision regarding what types of hacking are deceptive, but concluding that hacking is like "trickery, misrepresentation, and deceit", and misrepresentation such that the hacker's conduct is deceptive within the meaning of Section 10(b)).

ordinary meaning of deceptive and then applied it to some basic assumptions about hacking.[152] The *Dubovoy* complaint alleges that the hackers used stolen passwords to gain access to the newswires' systems,[153] which was enough to be considered "plainly deceptive" by the *Dorozhko* court.[154] The SEC will have to prove that the stolen passwords were actually used in the process of obtaining material nonpublic information that was then used to place a trade.[155] This means the SEC will need to chain together evidence from each trade to prove how the material nonpublic information was sourced, namely that the password was not in fact used by the person to whom it belonged and was used by the hacker defendant.[156] With respect to the other methods by which the hacker Defendants obtained information, the path forward is less clear.[157] The court is going to have to

[152] *See Dorozhko*, 574 F.3d at 50 (pointing out that the ordinary meaning of deceptive can encompass a wide array of conduct comprised of "cheating or trading in falsehoods").

[153] *See* New Jersey Indictment, *supra* note 74, ¶ 42 (alleging that the hacker Defendants stole login credentials of several newswire service employees and then used the stolen credentials to access the newswire's networks); New York Indictment at 8-9 (alleging the hackers used a file containing user IDs and associated hashed passwords to access the newswire's network).

[154] *See Dorozhko*, 574 F.3d at 51 (opining that gaining access to information by misrepresenting one's identity plainly meets the definition of "deceptive").

[155] *See* Odian, *supra* note 37, at 1337 (explaining that the second element of Section 10(b) requires the conduct to be "in connection with" a purchase or sale of a security); Geeraerts, *supra* note 14, at 268 (declaring that the "in connection with" requirement was met in *Dorozhko* because the deception does not need to be specifically related to the trade to purchase or sell the security).

[156] *See* Odian, *supra* note 37, at 1339 (examining the potential issues that could have arose in a trial of the *Dorozhko* case). Odian suggests that according to language from O'Hagan, there would not have been any securities fraud in *Dorozhko* until the information obtained through hacking was used to purchase or sell securities. *Id.* This means SEC would have to demonstrate that the defendant hackers' fraud coincided with the later purchase or sale of securities by the trader defendants. *Id. See also* Geeraerts, *supra* note 14, at 268-69 (stating that the "in connection with" test can be met in a hacking case provided that the hack in some way is related to or coincides with the purchase of securities).

[157] *See* Denny, *supra* note 64, at 970 (stating that there is a considerable amount of disagreement about what types of hacking should be considered deceptive). Some argue that burglary and theft are not ordinarily deceptive, while others argue that theft of information used to purchase or sell securities is essentially a fraud on the party from which the information was stolen. *Id.*

decide whether they meet the definition of a deceptive device,[158] which will inevitably be modelled to some degree by the SEC's theories.[159] If the court holds that the hacker Defendants were not engaged in insider trading because they did not actually execute any trades, it would be a setback to the SEC's push to broaden insider trading law because it will effectively curtail future cases where the hackers defendants are not engaged in the trading itself.[160]

B. The Law and Economics of Pushing the Envelope

The question remains as to whether pursuing hacker defendants who did not engage in any insider trading is a productive use of SEC resources. This can be difficult to measure because of the lack of transparency in publicly available reporting for insider trading enforcement makes it nearly impossible to provide an assessment on the effectiveness of the action.[161] The SEC expended considerable resources to pursue the hacker Defendants in *Dubovoy* based on relatively rarefied case law.[162] If the SEC is able to expand the law through cases like *Dubovoy*, it ensures that an economic efficiency analysis will not be conducted, and the SEC will not be held accountable for explaining whether the resources it expended on this case and others like it outweighed the costs in time and money.[163]

---

[158] *See* Denny *supra* note 64, at 973 (noting that the issue of whether exploiting a weakness in a computer code was never reached in the *Dorozhko* decision).
[159] *See* BAINBRIDGE, *supra* note 2, at 57 (describing the Second Circuit's willingness to help the SEC eschew the duty requirement); Denny, *supra* note 64, at 971 (concluding that the SEC's pursuit of hackers like Dorozhko demonstrates that the SEC is looking to establish deceptive conduct under Section 10(b) without relying on a fiduciary duty).
[160] *See* Odian, *supra* note 37, at 1344 (arguing that new theories must be adopted by the courts to capture insider trading hackers).
[161] *See* Velikonja, *supra* note 22, at 913 (asserting that the flaws in the SEC's reporting do not accurately reflect the landscape of regulatory violations and are an obstacle to providing an accurate assessment of the agency's performance).
[162] *See* Press Release, Sec. & Exch. Comm'n, *supra* note 111 (announcing that the trading scheme ensued over a five-year period and indicating that at least nineteen SEC employees worked on the case).
[163] *See* Velikonja, *supra* note 22, at 922 (breaking down the SEC's process for reporting enforcement statistics, and explaining the change in 1987 to stop reporting on case outcomes and instead reporting on performance indicators). The SEC does include information in its annual report to highlight major enforcement cases. *See* U.S. SEC. AND EXCH. COMM'N, AGENCY FINANCIAL REPORT, FISCAL YEAR 2015, at

If the SEC is unsuccessful against the hacker Defendants in *Dubovoy*, it still may be able to use this case as a guidepost to update insider trading laws. Administrative agencies like the SEC have broad authority for rulemaking.[164] For example, the SEC could consider pulling in elements of cybercrimes in which hackers engage, such as accessing a computer knowingly and without authorization to obtain information and then communicating that information.[165] It can also try to codify in Rule 10b-5 that a duty is not required if the material nonpublic information was obtained during the commission of a cybercrime such as computer fraud.[166]

One consideration for the SEC is the efficiency of its insider trading enforcement regime, which is a required component of SEC rulemaking.[167] Although the SEC is required to conduct economic

---

147-59, *archived at* https://perma.cc/7LKX-8AHR. The *Dubovoy* case was mentioned in this section:

> In August 2015, the SEC announced fraud charges and an asset freeze against 34 defendants for allegedly taking part in a massive international cyber-hacking scheme to profit from nonpublic information about corporate earnings announcements. Since filing the emergency action, the SEC has obtained a $30 million settlement from two defendants who made approximately $25 million buying and selling CFDs on the basis of the hacked press releases. The SEC's litigation continues against the remaining 32 defendants.

Id. at 153 (citations omitted). Note that it does not include any information about the costs of prosecuting this case.

[164] *See* Pitt & Shapiro, *supra* note 108, at 165-66 (explaining the authority of administrative agencies like the SEC, although operating under the delegation of Congressional authority, to create rules that have the same force and effect of law as laws passed by Congress).

[165] *See* Clough, *supra* note 84, at 109 (describing the elements of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(1)) that focus on harmful intent and the harm that results).

[166] *See* Denny, *supra* note 64, at 977-78 (suggesting updates should be made to insider trading statutes to alleviate the need for a duty). Denny also notes that Congress has been reluctant to make modifications to the Securities Exchange Act, despite its many deficiencies. *Id.* at 976.

[167] *See* 15 U.S.C. §§ 78c(f) (2012). "Whenever pursuant to this chapter the [SEC] is engaged in rulemaking . . . and is required to consider or determine whether an action is necessary or appropriate in the public interest, the [SEC] shall also consider . . . whether the action will promote efficiency, competition, and capital formation"; Coates, *supra* note 98, at 912-13 (European Corp. Governance Inst., Law

efficiency analysis in the rulemaking process,[168] there is a lack of economic analysis information available from the SEC about the SEC's insider trading program.[169] Instead of pushing a change like removal of the duty requirement through case law, a promulgated rule change would require the SEC to conduct an economic efficiency analysis and therefore be held accountable to some degree for proving that it is economically efficient.[170]

Assuming that the SEC can provide additional transparency on the costs and benefits of pursuing these hacker cases, it would bring legitimacy to its approach not only by leveraging the rulemaking process, but by requiring it to quantify the resources used in these cases.[171] A case like *Dubovoy* demonstrates not only substantial, but

---

Working Paper No. 234, 2014) (explaining that securities regulations require the SEC to consider efficiency with respect to regulatory action); PAUL ROSE & CHRISTOPHER J. WALKER, THE IMPORTANCE OF COST-BENEFIT ANALYSIS IN FINANCIAL REGULATION 8-9 (Ctr. for Capital Mkts. Competitiveness) (2013) (describing successful efficiency-based legal arguments against SEC rulemaking).

[168] *See* Memorandum from the Division of Risk, Strategy, and Financial Innovation and the Office of the General Counsel to Staff of the Rulewriting Divisions and Offices, Sec. & Exch. Comm'n 1 (Mar. 16, 2012) (on file with the United States Securities and Exchange Commission) (declaring "high-quality economic analysis" a critical part of the SEC's rulemaking process).

[169] *See* Hu & Noe, *supra* note 90, at 41 (calling for an analysis of the key insider trading variables to define policy and create efficient regulation); Eric A. Posner & E. Glen Weyl, *The Case for Cost-Benefit Analysis of Financial Regulations*, 124 YALE L.J. F. 246, 262 (Jan. 2015) (concluding that cost-benefit analysis of financial regulation would improve the performance of financial regulators). The requirement for economic analysis is focused on legislative rulemaking, rather than backward-looking analysis of rulemaking through case law. *See* Memorandum from the Division of Risk, Strategy, and Financial Innovation and the Office of the General Counsel to Staff of the Rulewriting Divisions and Offices, Sec. & Exch. Comm'n, *supra* note 168, at 4.

[170] *See* Coates, *supra* note 98, at 914 (noting that the SEC considered economic efficiency); Memorandum from the Division of Risk, Strategy, and Financial Innovation and the Office of the Counsel to Staff of the Rule writing Divisions and Offices, Sec. & Exch. Comm'n, *supra* note 168, at 1 (highlighting the importance of economic analysis in rulemaking); Bainbridge, *supra* note 3, at 66 (postulating that insider trading law and the SEC's desire to pursue insider traders is based more on fairness than efficiency).

[171] *See* Coates, *supra* note 98, at 890-91 (extrapolating the effects that a law can have on an agency's actions in tracking its own expenses and conduct in relation to the law); Velikonja, *supra* note 22, at 949 (arguing the SEC has the information it needs to assess performance and that better assessment of performance is needed to measure the effectiveness of the agency's actions).

measurable losses that can be incurred through these insider trading schemes involving hackers.[172] The SEC can position the *Dubovoy* case as the bellwether for the future insider trading cases that have the potential to cause the most significant damage, bolstering an efficiency analysis.[173] The key is for the SEC to quantify how the rule would benefit market integrity and how much it would cost for the SEC it enforce it.[174]

Looking at the prosecution of insider trading from the perspective of traditional law and economics theories, the property theory provides a clear path toward prosecuting hackers for insider trading.[175] From the perspective of the SEC, leveraging the property theory by updating the rules to penalize insider trading where there is no duty gives the agency bandwidth to target hackers, which is consistent with the concerns brought forth in recent enforcement actions.[176] The property rights theory is also consistent with the other statutes that the DOJ can leverage, such as the fraud and related activity in connection with computers, and would provide clear statutory direction for prosecution of insider trading hackers.[177]

In lieu of a rule change, the SEC could also work more closely with the DOJ and refer insider trading cases involving hack-

---

[172] *See* Press Release, Sec. & Exch. Comm'n, *supra* note 111 (alleging that the insider trading scheme generated illegal profits of more than $100 million over a five-year period).

[173] *See* Denny, *supra* note 64, at 977-78 (positing that if courts do not recognize computer hacking as a "deceptive device" Section 10(b) should be changed to incorporate computer hacking as a deceptive device).

[174] *See* O'Connor, *supra* note 108, at 363 (stating that the advantages of the deterrence strategy for insider trading must be weighed against the costs).

[175] *See* Odian, *supra* note 37, at 1345 (describing how a property rights approach opens the door to prosecuting insider trading defendants without a duty).

[176] *See Dorozhko*, 574 F.3d at 51 (holding that hackers may be found guilty for insider trading absent a duty to the company or its shareholders); S.E.C. v. Lohmus, Haavel & Viiesemann, et al., SEC Litigation Release No. 20134, 2005 WL 3309748 (Nov. 8, 2005) (announcing complaint against hacker defendants who traded material nonpublic information); S.E.C. v. Blue Bottle Ltd., SEC Litigation Release No. 20018, 2007 WL 580798 (Feb. 26, 2007) (announcing litigation against hackers who used material nonpublic to trade for illicit gains).

[177] *See* JARRETT ET AL., *supra* note 85, at 16 (describing the various cybercrime statutes).

ers to the DOJ for prosecution under existing wire fraud and computer fraud statutes.[178] The Galleon case is instructive on this point because it showed the power of the SEC and DOJ working together to prosecute a major insider trading ring, winning a large number of convictions and some of the harshest prison sentences for insider trading to date.[179] This approach allows both groups to create efficiencies by working together to detect, investigate, and punish insider traders.[180] If the DOJ and SEC work together they may also be able to better leverage bargaining power on hacker defendants to testify against the trading defendants in the same case.[181] The SEC has specialized expertise in detecting and identifying trades that could potentially be indicative of a hacking scheme resulting in insider trading, and it can refer this information about hacker defendants to the DOJ to decide whether to prosecute.[182] This is more efficient because the DOJ can leverage existing statutes designed specifically to prosecute cybercrimes, and it would not have to solely rely on insider trading law, which is what the SEC would have to do.[183]

V. Conclusion

The SEC has broad authority to interpret its own statutes, and based on the ground that it covered in the *Dorozhko* case, it certainly has the potential to be successful in the *Dubovoy* case. If this type of case is the future of insider trading enforcement for the agency, then

---

[178] *See* Shen, *supra* note 80, at 61 (explaining that the existing relationship between the SEC and DOJ is already collaborative and that the sharing of information creates efficiencies in investigation and prosecution of insider trading cases).
[179] *See* Press Release, U.S. Dep't of Justice, *supra* note 79 (explaining the actions taken in the case, including use of non-traditional methods such as wiretaps, leading to the successful prosecution in the case).
[180] *See* Press Release, U.S. Dep't of Justice, *supra* note 79 (highlighting the substantial benefit of civil and criminal enforcement working together to prosecute the Galleon defendants).
[181] *See* Henning, *supra* note 78 (describing the DOJ's ability to use various bargaining tools to garner cooperation and as leverage against those who do not cooperate).
[182] *See* Shen, *supra* note 80, at 61 (explaining the way that the SEC and DOJ can work together on parallel investigations, whereby the DOJ will make use of the evidence that the SEC uncovers during its investigation).
[183] *See* Shen, *supra* note 80, at 61 (illustrating how the SEC and DOJ can work together and the DOJ can use evidence obtained through the SEC's investigation to increase efficiency and effectiveness).

it should be thoughtful in its approach by conducting a cost-benefit analysis of these enforcement actions and consider taking steps to proactively enhance rules to clarify that a duty is not required. If hacker insider trading cases are not where the SEC intends to spend its enforcement budget, then these cases would best be left to the DOJ, which has the additional statutory authority to prosecute hackers for fraud through computer-related offenses and the wire fraud statute.