Preliminary Draft: August 31, 2014 (please do not quote or cite without author's consent)

Outsider Trading

Caroline Bradley*

The US Supreme Court for many years insisted that a securities trader would only be liable for insider trading if she was acting in breach of a fiduciary duty[1] or if she obtained the information knowingly from a fiduciary in breach of a duty.[2] For many years the SEC argued for a vision of insider trading law focusing on the idea of a level playing field for investors in which asymmetric information was problematic,[3] but the Supreme Court refused to adopt this approach, insisting on the importance of fiduciary duties as a component of insider trading liability.[4]

In US v O'Hagan the Supreme Court accepted that outsiders to the issuer could be liable for insider trading based on the misappropriation theory,[5] but the Court's version of this theory

---

* Professor of Law, University of Miami School of Law, PO Box 248087, Coral Gables, FL, 33124, cbradley@law.miami.edu ; http://blenderlaw.umlaw.net/ .

[1] *See, e.g.*, Donald C. Langevoort, *Insider Trading and the Fiduciary Principle: A Post-Chiarella Restatement*, 70 CALIF. L. REV. 1, 3 (1982) (noting that "Chiarella has made the fiduciary principle a consideration of utmost importance.")

[2] Dirks v SEC 463 U.S. 646 (1983).

[3] *Cf.* James D. Cox, *Insider Trading and Contracting: A Critical Response to the "Chicago School",* (1986) DUKE L. J. 628, 631 (noting that the "utopian dream of information parity among investors was short-lived.")

[4] See, e.g., Jonathan R. Macey, *From Judicial Solutions to Political Solutions: The New, New Direction of the Rules Against Insider Trading*, 39 ALA. L. REV. 355, 358 (1988) ("During the 1980s, the Supreme Court, philosophically opposed to the SEC's position on insider trading, rejected the notion that those possessing material nonpublic corporate information owe a general duty to the marketplace that requires them to disclose that information. In its place, the Supreme Court established a theory of insider trading liability defined by property law.") For an argument that the current Supreme Court is not very interested in securities regulation see A.C. Pritchard, *Securities Law in the Roberts Court: Agenda or Indifference?*, 37 J. CORP. L. 105 (2011-2012).

[5] 521 U.S. 642, 652 (1997) ("The "misappropriation theory" holds that a person commits fraud "in connection with" a securities transaction, and thereby violates § 10(b) and Rule 10b-5, when he misappropriates confidential information for securities trading purposes, in breach of a

requires the misappropriator to breach a duty of confidentiality which is either fiduciary or like a fiduciary duty.[6] The misappropriation theory's invocation of fiduciary-like duties, however, is different from the invocation of the duties in the context of the classical theory of insider trading liability, as it focuses on the right of the true owner of the information in question to control its use[7] rather than on the idea that a fiduciary of an issuer owes obligations to investors.[8] The original conception of the function of fiduciary duty in US insider trading law involved the fiduciary taking advantage of information in breach of duty in circumstances where the indirect beneficiaries of the fiduciary duties would be harmed by being deprived of the information their fiduciary had. Outsiders who happened to have valuable information were not constrained in the same way as fiduciaries were. Misappropriation theory shifts the focus to the duties a person owes to the "source"of information, but the Supreme Court has remained clear that fiduciary (or fiduciary-like) duties are a component of liability under section 10(b) and Rule 10b-5.

The SEC and the lower courts seem to be less clear that the idea of fiduciary duty remains

---

duty owed to the source of the information.... Under this theory, a fiduciary's undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information. In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information.')

[6] *See, e.g.*, Donna M. Nagy, *Insider Trading and the Gradual Demise of Fiduciary Principles*, 94 IOWA L. REV. 1315, 1318 (2009).

[7] See, e.g., Jonathan R. Macey, *From Fairness to Contract: The New Direction of the Rules Against Insider Trading*, 13 HOFSTRA L. REV. 9 (1984) (articulating a property rights approach to insider trading regulation).

[8] SEC v Texas Gulf Sulphur 401 F.2d 833, 848 (2d. Cir. 1968) ("anyone in possession of material inside information must either disclose it to the investing public, or, if he is disabled from disclosing it in order to protect a corporate confidence, or he chooses not to do so, must abstain from trading in or recommending the securities concerned while such inside information remains undisclosed.")

(or should remain) a part of US insider trading law.[9] Commentators express differing views as to whether insider trading law should remain true to the Supreme Court's precedents, espouse a property rights view wholeheartedly, be rationalized in new legislative rules,[10] or be reconceived as the regulation of private corruption.[11] US insider trading law has never been completely coherent: it has developed rather erratically through SEC rule-making under a rather ambiguous statutory provision with occasional Congressional adjustments. And the Supreme Court expressed views about fiduciary duties and the common law of fraud that commentators have challenged.[12] Securities law seems to take a formalistic view of fiduciary duty and contract law that experts in those areas of law would dispute. There is little certainty as to the precise contours of insider trading liability. Some commentators see this lack of certainty as benefiting the SEC. [13] From a European perspective US insider trading law seems overly complex.[14]

Much of the SEC's enforcement effort with respect to insider trading has focused on

---

[9] See Nagy, *supra* note 6, at 1319 ("Despite the Supreme Court's explicit dictate that fiduciary principles underlie the offense of insider trading, there have been recent repeated instances in which lower federal courts and the Securities and Exchange Commission ("SEC") have disregarded these principles.")

[10] *See, e.g.*, Nagy, *supra* note 6

[11] Sung Hui Kim, *Insider Trading as Private Corruption*, 61 UCLA L. REV. 928 (2014). Cf. Alan Strudler & Eric W. Orts, *Moral Principle in the Law of Insider Trading*, 78 TEX. L. REV. 375, 376 (1999) ("insider trading is wrong because it is a kind of fraud").

[12],,, *See, e.g.*, Kim Lane Scheppele, *"It's Just Not Right": The Ethics of Insider Trading*, 56 L. & CONTEMP. PROBS. 123, 132 (1993) ("Justice Powell's argument in Chiarella rests heavily on his interpretation of what the common law of fraud requires....But courts have often construed equity rules to require disclosure in many situations not involving specific, preexisting fiduciary relationships or active deception.")

[13] *See, e.g.*, Macey, *supra* note 4 at 365 ("To the extent that the law remains vague, the SEC's services and regulatory forbearance are in demand.")

[14] *See, e.g.*, Marco Ventoruzzo, *Comparing Insider Trading in the United States and in the European Union: History and Recent Developments*, European Corporate Governance Institute (ECGI) - Law Working Paper No. 257/2014; Bocconi Legal Studies Research Paper No. 2442049 (May 26, 2014).

people whose access to material non-public information derives from their employment by financial firms which provide services to issuers and to the markets.[15] Employees of financial printers, accounting firms,[16] banks,[17] and investor relations firms[18] have access to information that is not generally available to investors. But targeting only those people who are linked to these firms by employment, or by familial or friendly relationships does not satisfy the SEC. Even people who have obtained information without such links have been targeted. Thus the SEC has brought enforcement actions against hackers on the theory that the theft constitutes obtaining information by deception.[19] In SEC v Dorozhko the Second Circuit held that a computer hacker not subject to a fiduciary duty could be considered to be "deceptive" for the purposes of insider trading liability.[20] The court stated:

> "the SEC has not alleged that defendant fraudulently remained silent in the face of a "duty to disclose or abstain" from trading. Rather, the SEC argues that defendant affirmatively misrepresented himself in order to gain access to material, nonpublic information, which he then used to trade. We are aware of no precedent of the Supreme Court or our Court that forecloses or prohibits the SEC's straightforward

---

[15] For example the Galleon insider trading ring. *See, e.g.*, US v. Goffer, 721 F. 3d 113 (2nd. Cir. 2013).

[16] SEC Press Release, SEC Charges Atlanta-Based Accountant With Insider Trading on Confidential Information From Client (Aug. 14, 2014).

[17] SEC Press Release, SEC Charges Former Bank Executive and Friend With Insider Trading Ahead of Acquisition (Aug. 18, 2014).

[18] SEC Press Release, SEC Charges Investor Relations Executive With Insider Trading While Preparing Clients' Press Releases (Jul. 22, 2014)

[19] Nagy, *supra* note 6, at 1340 ff.

[20] SEC v. Dorozhko, 574 F. 3d 42 (2d. Cir. 2009). After the decision of the Second Circuit the District Court granted a motion for summary judgment to the SEC. SEC, Litigation Release No. 21465 / March 29, 2010, SEC v Oleksandr Dorozhko, Civil Action No. 07 Civ. 9606 (NRB) (S.D.N.Y.) (filed October 29, 2007), SEC Obtains Summary Judgment Against Computer Hacker for Insider Trading.

theory of fraud."[21]

This theory of non-fiduciary liability for deceptive behaviour distinguishes between the Supreme Court's fiduciary theories of insider trading liability in cases where the deceptive behaviour is non-disclosure of the material non-public information to the market (the traditional theory of insider trading liability) or to the information source (misappropriation theory of insider trading liability) and cases where the material non-public information is obtained by deception.[22] The Second Circuit suggested that there would be a difference between exploiting weaknesses in electronic code (which would not be deceptive) and "misrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information" which "is plainly "deceptive" within the ordinary meaning of the word."[23] Misrepresenting one's identity, or lying to the owner of information in order to acquire it and trade in securities to which the information relates is, according to the Second Circuit, prohibited by Section 10(b) and Rule 10b-5.

Whether it makes sense to characterize Dorozhko's actions as deceptive in this sense is not clear. The SEC's complaint in the case does not specify exactly how Dorozhko obtained

[21] See 574 F. 3d 42, 51 (" In our view, misrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly "deceptive" within the ordinary meaning of the word. It is unclear, however, that exploiting a weakness in an electronic code to gain unauthorized access is "deceptive," rather than being mere theft. Accordingly, depending on how the hacker gained access, it seems to us entirely possible that computer hacking could be, by definition, a "deceptive device or contrivance" that is prohibited by Section 10(b) and Rule 10b-5.")

[22] Note that in the disclosure of the intent to trade was not treated as precluding liability under the misappropriation theory but rather as rendering

[23] At 51. The SEC had argued that hackers either "(1) `engage in false identification and masquerade as another user['] . . . or (2) `exploit a weakness in [an electronic] code within a program to cause the program to malfunction in a way that grants the user greater privileges.'" Appellant's Br. 22-23 (quoting Orin S. Kerr, Cybercrime Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L.Rev. 1596, 1645 (2003))." *Id.*

access to the information he used in trading.[24] The decision of the district court in Dorozhko's case states:

> The SEC presented computer logs that showed that at 2:15:28 p.m., an unauthorized user gained access to IMS Health's soon-to-be-released negative earnings announcement, which was scheduled to be released to the public later that day at around 5:00 p.m. The SEC further showed that approximately 35 minutes after the hack occurred, and just a matter of hours before the information was to be released to the public, Dorozhko, who had recently opened an online brokerage account but had not yet used the account, purchased $41,670.90 worth of October 25 series and October 30 series put options in IMS Health stock.[25]

The District court refers to a hacker "probing" the issuer's website at Thompson Financial. The SEC argued that his use of "electronic means to trick, circumvent, or bypass computer security in order to gain unauthorized access to computer systems, networks, and information stored or communicated therein, and to steal such data" was deceptive for the purposes of the statute. The district court, reviewing case law and academic commentary concluded that there was no basis for treating Dorozhko's behaviour as deceptive.[26] And nothing in the decision of the District Court seems to suggest that the Second Circuit's distinction between exploiting weaknesses in electronic code (which would not be deceptive) and "misrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information" makes sense in the context of what Dorozhko seems to have done.

Many commentators have argued that Dorozhko is wrongly decided because Dorozhko was not a fiduciary, and he was not consciously entrusted with information by one who owned or

---

[24] Complaint in SEC v Dorozhko available at http://www.sec.gov/litigation/complaints/2007/comp20349.pdf .

[25] SEC v. Dorozhko 606 F.Supp.2d 321 (SDNY 2008).

[26] *Cf.* Stephen M. Bainbridge, *Ruling on Hackers as Inside Traders: Right in Theory, Wrong on the Law*, Washington Legal Foundation Legal Backgrounder Vol. 24, No. 32 (Oct. 9, 2009) (critiquing the Second Circuit's decision along the lines of the District Court's analysis).

had the right to use it.[27] In a world where regulators worry about the risks cyber attacks and hacking create for financial firms and infrastructures, it makes sense for the regulators to encourage financial firms to be diligent about controlling access to their information.[28] Singling out a hacker as a securities law violator may have helped to emphasize the security risks.[29] And the SEC may worry that there are more hackers out there planning to exploit vulnerabilities in the computers of the US financial sector. In one sense the debate about the case is a rather narrow debate, but if there is an increase in such activity it would be useful for the SEC to have tools to address it.

Advocates for the misappropriation theory before O'Hagan had argued for a vision of misappropriation that focused on the importance of being able to sanction people who cheated others into entrusting information to them. For example, Barbara Aldave wrote:

> an agent or employee who is given custody of nonpublic information, with the understanding that he will keep the information confidential and refrain from

---

[27] Kim, *supra* note 11, at 999 ("Even though the hacking-and-trading does not fit the definition of corruption, does it raise corruption costs seriously enough to reconsider the initial judgment? Because he betrayed no entrusted position, there are no obvious temptation or distraction costs. But what about legitimacy costs? Although the hacker's advantage was unfair, he garnered it not through privilege or special connections but through the much rarer combination of superior technologies, risk-taking, and criminal bravado. Hence, the hacker's conduct, though universally condemned and proscribed by other law, is unlikely to be perceived as being systemic in a way that might raise serious legitimacy costs to the securities markets. In the end, most investors will not see the hacker's actions as evidence that the entire system is rigged.")

[28] *See, e.g.*, New York State Department of Financial Services, Report on Cyber Security in the Banking Sector (May 2014); The Joint Forum, Outsourcing in Financial Services (Feb. 2005). Cf. David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L. J. 1091, 1100 (2012) ("The risks posed by hackers are likely underreported because they are effective at covering their tracks.")

[29] Regulators exercising enforcement powers may care as much about the message their actions send as about sanctioning violators. *Cf.* Ezra Ross & Martin Pritikin, *The Collection Gap: Underenforcement of Corporate and White-Collar Fines and Penalties*, 29 YALE L. & POL'Y REV. 453 (2011); Margaret H. Lemos & Max Minzner, *For-Profit Public Enforcement*, 127 HARV. L. REV. 853 (2014).

> using it for personal profit, "dupes" those who entrusted the information to him when he conveys it to others or trades on the basis of it....the misappropriation of confidential information by one to whom it was entrusted is fraudulent conduct.[30]

The author, like the Supreme Court in O'Hagan, was clearly imagining interactions between human beings with respect to the entrusting of information rather than interactions between a human being and a computer system.

Although the Court in O'Hagan suggested that a misappropriator could avoid liability by disclosing to the source of this information that he intended to trade in securities, in SEC v Rocklage, where this argument was deployed, the First Circuit refused to accept it.[31] Mr Rocklage, the CEO of a corporation, shared information with his wife about adverse clinical trial results for one of the corporation's drugs. When he passed the information to his wife he emphasised that the information was confidential, but, unknown to him, his wife had previously agreed to share useful information with her brother, who owned shares in the corporation. Before informing her brother Mrs Rocklage told her husband that she intended to do so. She later tried to rely on this disclosure to avoid liability, but the First Circuit held that the circumstances in which she had obtained the information meant that she had been guilty of deception.[32] Although Mr and Mrs Rocklage had a relationship that had in the past involved expectations of confidentiality, at the time Mr Rocklage communicated the material information about the clinical trial to his wife she was acting as a faithless, rather than faithful, fiduciary. A faithless fiduciary who uses or even plans to use information for her own benefit that she should only use

---

[30] Barbara Bader Aldave, *Misappropriation: A General Theory of Liability for Trading on Nonpublic Information*, 13 HOFSTRA L. REV. 101, 119 (1984). Although *cf. id.* at 122 ("When one simply steals information from a stranger, his trading on the information does not involve deception or fraud, and therefore should not be held to violate Rule l0b-5.")

[31] SEC v Rocklage, 470 F. 3d 1 (1st Cir. 2006).

[32] The Court stated: "In light of her disclosure to her husband, Mrs. Rocklage's mechanism for "distributing" the information to her brother may or may not have been rendered non-deceptive by her stated intention to tip. But because of the way in which Mrs. Rocklage first acquired this information, her overall scheme was still deceptive: it had as part of it at least one deceptive device. Thus as a matter of the facts alleged in the complaint, and taking all facts and inferences in favor of the plaintiff, a § 10(b) claim is stated."

for the benefit of her employer is deceptive in the same sense — she pretends to be faithful although she is in fact faithless.

In SEC v Dorozhko the defendant had hacked into the systems of Thomson Financial, Inc. which was providing investor relations services for the issuer, including the online release of its earnings reports.[33] If the hacker had misrepresented his identity he would have induced Thomson to provide access to confidential information in a manner that was similar to Mrs Rocklage's behaviour. Dorozhko accessed information which Thompson only intended to make available to people who were subject to obligations of confidentiality. In the same way Mrs Rocklage induced her husband to give information to her which he would not have communicated had he known what she was planning to do. In both cases the recipients of the information purported to be subject to obligations of confidentiality when they either were not subject to those obligations or were but did not intend to behave as if they were. In both cases one could say that the communicator of the information reposed trust and confidence — misplaced though they were — in the person to whom the information was given or made available. But the contexts are very different. Mrs Rocklage actively induced her husband to trust her whereas Thompson failed to control access to its confidential information. Nevertheless both cheated in the context of obtaining the information that made tipping and trading profictable.[34]

Insisting on a traditional fiduciary component of insider trading law tends to assume that fiduciary type duties are less than usual rather than being pervasive. Employees are agents of their employers and are therefore fiduciaries. It is true that scholars of insider trading and the courts have in the past tended to suggest that only certain employment relationships involving access to information should be characterized as fiduciary relationships, but employers often assert a broader view of the fiduciary, or at least confidential, characteristics of the employment relationship. As information has become recognized as an increasingly important business asset, and trade secrets law protect information which is treated as secret, employers subject a wide

[33] 574 F. 3d 42, 44 (2d. Cir. 2009).

[34] *Cf.* Scheppele, *supra* note 12.

range of employees to obligations of confidentiality.[35]

Employers may seek to have employees disgorge secret profits they make in violating their fiduciary duties of loyalty. And employers have also asked courts to require employees to disgorge their compensation during periods when they breach their duty of loyalty, including, for example engaging in sexual harassment,[36] and even insider trading.[37] But courts have characterized faithless servant doctrine as being based in contract.[38] In August 2014, Michael Lucarelli, the Director of Market Intelligence at Lippert/Heilshorn & Associates, Inc., an investor relations firm, was arrested for insider trading.[39] The Complaint alleged that Lucarelli made profits from trading in securities after reading draft press notices produced by the firm for clients,[40] that Lucarelli had signed a contract with the firm which required him to sign a

---

[35] *See, e.g.*, Almeling, *supra* note 28.

[36] Charles A Sullivan, *Mastering the Faithless Servant?: Reconciling Employment Law, Contract Law, and Fiduciary Duty*, WISC. L. REV. 777, 777 (2011); Consolidated Edison Co. v. Zebler 2013 NY Slip Op 51354 (NY Sup Ct. 2013) ("The faithless servant doctrine does not consider criminal culpability, nor does it require the Court to value the loss of honest services. Under the faithless servant doctrine, the act of being disloyal to one's employer is itself sufficient grounds for disgorging all compensation received during the period of disloyalty, and does not depend on actual harm to the employer.")

[37] Morgan Stanley v. Skowron (SDNY 2013).

[38] Carco Group, Inc. v. Maconachy, 718 F. 3d 72, 84 (2nd Cir. 2013) ("The faithless servant doctrine arises out of an agency or employment relationship, and New York courts have repeatedly and consistently used the rules and terminology of contract law in evaluating faithless servant claims. ")

[39] US Attorney's Office for the Southern District of New York, Manhattan U.S. Attorney And FBI Assistant Director-In-Charge Announce Insider Trading Charges Against Director Of Market Intelligence At Investor Relations Firm (Aug. 26, 2014). See also U.S. Securities and Exchange Commission, Securities and Exchange Commission v. Michael Anthony Dupre Lucarelli, Civil Action No. 14-Civ-6933 (NRB) (S.D.N.Y.), Litigation Release No. 23074 (Aug. 26, 2014).

[40] Complaint in US v Lucarelli available at http://www.justice.gov/usao/nys/pressreleases/August14/LucarelliArrestPR/Lucarelli,%20Michael%20Complaint.pdf .

confidentiality agreement and the firm's code of conduct which prohibited trading in the securities of clients or non-clients involved in transactions with clients.[41] If the allegations in the Complaint are substantiated, Lucarelli, as an employee who obtained access to information he did not have authority to see, would be liable as a faithless servant.

A non-employee hacker is, in contrast, clearly not a servant and is not liable as a faithless servant. At the same time, requiring the faithless servant to disgorge the compensation they received as an employee during a period of faithlessness does in a sense unravel the employment relationship. And arguably the sort of deception as to identity the Second Circuit imagined in the Dorozhko case as the basis for deception is not unlike the sort of promise which, accompanied by detrimental reliance, might give the promisee the basis for a claim for a remedy.

Whether or not Dorozhko did what can reasonably be characterized as lying to Thompson, his unauthorized access to Thompson's computers was likely criminal.[42] Criminal computer hacking is surely more morally and legally problematic than a breach of fiduciary duty. And, in the EU a person who obtains inside information by breaching the criminal law can be liable for insider trading.[43] There is no need to distinguish between deceptive and non-deceptive hacking under the Market Abuse Directive — the question is merely whether the information was obtained in breach of the criminal law. The neatness of the EU rule contrasts dramatically with the messiness of the US position on this question.[44]

A doctrinal comparison between the different US and the EU rules on insider trading seems therefore to contrast a chaotic American approach to the development of the law with an orderly European one. It is a story both Americans and Europeans might like: Americans might congratulate themselves on the effectiveness of their messy approach and Europeans may feel

---

[41] *Id.*

[42] The Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, makes it a criminal offence to access a computer intentionally without authorization.

[43] The EU Market Abuse Regulation treats a person as violating the rules against insider trading who "possesses inside information as a result of ... being involved in criminal activities." Regulation (EU) No 596/2014 on Market Abuse, Art. 8(4), O J No. L 173/1 (Jun. 12, 2014).

[44] *Cf.* Ventoruzzo, supra note 14.

happy in the aesthetic advantages of theirs. But this doctrinal focus also avoids thinking about the harder questions about how prevalent insider trading is in the US and the EU and how energetically and effectively the regulators in both regions are enforcing the rules.