ALTERNATIVE DATA AND INSIDER TRADING: ARE INVESTMENT MANAGERS ASSLEEP AT THE WHEEL ON BIG DATA USE?

William Montemarano

Follow this and additional works at: https://brooklynworks.brooklaw.edu/bjcfcl

Part of the Air and Space Law Commons, Business Organizations Law Commons, Civil Law Commons, Internet Law Commons, Law and Economics Commons, and the Securities Law Commons

Recommended Citation

William Montemarano, *ALTERNATIVE DATA AND INSIDER TRADING: ARE INVESTMENT MANAGERS ASSLEEP AT THE WHEEL ON BIG DATA USE?*, 15 Brook. J. Corp. Fin. & Com. L. 263 (2021).
Available at: https://brooklynworks.brooklaw.edu/bjcfcl/vol15/iss1/11

ALTERNATIVE DATA AND INSIDER TRADING: ARE INVESTMENT MANAGERS ASLEEP AT THE WHEEL ON BIG DATA USE?

ABSTRACT

The rapid rise of "big data" has transformed the way that professional investors make investment decisions. In addition, the intersection of the United States federal securities laws and the use of "big data" to inform securities trading lies in uncharted waters. The nuanced and factually-dependent securities laws are far behind industry practices, and the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) have remained largely silent on the issue to date. This Note argues that this combination of murky laws and rapidly evolving business practices gives rise to legal and regulatory risk, and that investment managers leveraging "big data" sources may be paying insufficient attention. It is therefore critical that to protect their business and ensure compliance with the laws, investment managers implement robust compliance programs to guard against the risk that their use of "big data" violates the securities laws.

INTRODUCTION

The generation, collection, and monetization of so-called "big data" has become a matter of national discussion. We are living in what the New York Times called "the world's most advanced surveillance system."[1] Every day, each one of our transactions, geo-location tags, internet searches, social media visits, and numerous other data points are scrupulously documented by private companies.[2] The data can be used for a variety of purposes from personally-targeted advertising to tracking the spread of an infectious disease.[3] It can also be used to understand what is happening inside corporations: for example, Dataminr, an "advanced AI [artificial intelligence] platform that detects the earliest signals of high-impact events and emerging risks,"[4] applied analytics to Twitter data to uncover Volkswagen's emissions scandal three days before the market reacted to the news.[5]

For investment managers and other professional investors, these "big data" sources, referred to collectively as "alternative data" in industry parlance, represent a potential gold mine of information that can be used to

---

1. Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell- phone.html?searchResultPosition=3.

2. *Id.*

3. *Id.*

4. DATAMINR, https://www.dataminr.com/ (last visited Dec. 20, 2019).

5. Shaw Horton, *A Fund Manager's Roadmap to Big Data: Its Acquisition and Proper Use*, HEDGE FUND L. REP. 2 (Jan. 11, 2018), https://www.lowenstein.com/media/4297/hflr_a-fund-manager-s-roadmap-to-big-data_its-acquisition-and-proper-use.pdf.

inform securities trading.[6] Alternative data is not exhaustively defined, but it is generally understood to include any data which may be useful for understanding the financial condition of a particular company or industry which is not included in traditional data sources such as public financial filings or analyst reports.[7] It includes information such as geo-location tags, satellite and drone imagery, credit card and consumer transactions, social media data, email monitoring, website scraping, internet search data, and many other types of data points.[8] Most alternative data leveraged by investment managers is purchased from third-party specialty vendors who source, process, and sell datasets to buyside purchasers via subscription services.[9]

Although the use of alternative data to inform trading decisions is nothing new, modern technologies such as high-definition satellite imagery, drones, and sophisticated IT systems capable of identifying patterns in large unlinked data sets have led to an explosion of growth in the quantity and types of alternative data available.[10] For example, where an investment manager in the past might have sent an analyst to count the number of cars in a McDonald's parking lot to gauge the performance of the business, today that same manager can purchase a dataset specifying the number of cars in every McDonald's parking lot across thousands of square miles based on an analysis of real-time satellite images.[11] Indeed, alternative data is an evolving legal landscape because of the rapid pace of technological change and the types of alternative data available, and changes in how data is sourced, analyzed, and sold.[12] In addition, the relevant securities laws are imprecise and factually-dependent, there is minimal case law, and the SEC has not brought any enforcement action to date where a buyer purchased alternative data from a vendor.[13] Additionally, the SEC announced in January 2020 that its examinations priorities for the year will include a focus on alternative data use.[14]

---

6. Kara M. Stein, Comm'r, SEC, From the Data Rush to the Data Wars: A Data Revolution in Financial Markets, Georgia-State University College of Law – Henry J. Miller Distinguished Lecture Series (Sept. 27, 2018) (available at https://www.sec.gov/news/speech/speech-stein-092718).

7. Horton, *supra* note 5 at 1.

8. *Id*.

9. *Id*. at 3.

10. *Id*. at 1.

11. *See infra* note 37 and accompanying text.

12. Horton, *supra* note 5, at 5.

13. *See infra* note 59 and accompanying text.

14. SEC Rel. No. 2020-4, *SEC Office of Compliance Inspections and Examinations Announces 2020 Examination Priorities* (Jan 7, 2020) ("OCIE recognizes that advancements in financial technologies, methods of capital formation and market structures, as well as registered firms' use of new sources of data (often referred to as 'alternative data'), warrant ongoing attention and review.").

This Note will argue that this evolving landscape gives rise to legal and regulatory risks, and that investment managers may be giving these risks insufficient weight when trading on the basis of alternative data sources. Part I begins by discussing the alternative data marketplace, including explaining what alternative data is and how it is sourced, processed, sold, used, and by whom. Part II then highlights the most prominent United States federal securities laws that may be applicable to alternative data use, specifically insider trading and the parallel provisions of Section 204A of the Investments Advisers Act of 1940 (204A) and Section 15(g) of the Securities Exchange Act of 1934 (15(g)). Part III then discusses the current state of the mosaic theory of materiality and argues that alternative data use is analogous to the use of expert networks, which experienced widespread adoption in the investment management industry, followed by a crash after Raj Rajaratnam's 2011 conviction for insider trading, and a subsequent resurgence after firms implemented compliance controls. Finally, Part IV argues that managers should perform careful due diligence in order to manage the legal and regulatory risks presented by alternative data use, and lays out suggested compliance practices.

It is important to caveat that this Note focuses exclusively on the intersection of alternative data and the U.S. federal securities laws, most especially insider trading law. As is explained in further detail below, U.S. insider trading laws do not include a general prohibition on using any given information as a basis for securities trading decisions, absent some breach of duty to the source of that information.[15] Thus, in effect, it is legal to trade in securities on the basis of alternative data so long as that alternative data has not been improperly obtained.[16] Of course, there are many other laws, as well as ethical, societal, and privacy-related concerns implicated by the "big data" marketplace both in the context of securities trading and in other areas.[17] Indeed, it may or may not be legal or ethical to disseminate or use a particular "big data" source for some other purpose. As such situations are far too numerous and context-dependent to be addressed in this Note, they will be left for another day.

I.   ALTERNATIVE DATA MARKETPLACE

According to the Wall Street Journal, when Tesla CEO Elon Musk announced that employees were working "around the clock" to increase deliveries of Tesla's new mid-size Model 3 sedan, Thasos Group, a New York City-based alternative data vendor which converts "real-time location data from mobile phones into actionable information,"[18] decided to see for

---

15. *See infra* notes 88-98 and accompanying text.

16. *Id.*

17. *See* discussion *infra* note 57.

18. THASOSGROUP, http://thasosgroup.com/ (last visited Oct. 12, 2019).

themselves.[19] Thasos used their real-time database of geographic location coordinates collected by over 1,000 smartphone apps from over 30 million smartphones[20] to determine that the number of smartphones in Tesla's factory in Fremont California during the overnight hours had increased 30% from June to October of 2018.[21] Then, in late October 2018, "Tesla disclosed a rare quarterly profit, the result of Model 3 production that had nearly doubled in three months. Shares shot up 9.1% the next day."[22]

Thasos, founded in 2011 by Greg Skibiski, offers a variety of analytical reports based on smartphone location data.[23] One of the firm's offerings, MallStreams, which Thasos describes as "everything you ever wanted to know about your competitor's property but were afraid to ask," provides real-time information on mall visitation data, distance traveled to the property, average customer median household income, key census information based on the mall's location and surrounding areas, and customer cross-shopping patterns (i.e., what stores nearby were also visited by mall customers) for over 4,000 malls across the United States.[24] Thasos does not disclose its clients, but according to the Wall Street Journal, Thasos "sells its data to dozens of hedge funds, some of which pay more than $1 million a year."[25] In addition to datasets generated by smartphone location, there are numerous other types of alternative datasets available from many different vendors. Eagle Alpha, a New York-based firm helping owners of datasets monetize their data, groups alternative data into 24 different categories ranging from social media to internet-of-things, to satellite and weather data, thus illustrating the broad spectrum of data types available.[26] Most investment managers acquire data through third-party vendors like Thasos and do not pursue data collection in-house because of the expense and expertise required to build the requisite infrastructure.[27] Instead, "the overwhelming majority of managers are acquiring data through vendors," according to Peter Greene, a partner at Lowenstein Sandler.[28]

The investment insights gained from these datasets are as expansive as the types of datasets available. For example, Eagle Alpha's Consumer

---

19. Ryan Dezember, *Your Smartphone's Location Data Is Worth Big Money to Wall Street*, WALL ST. J. (Nov. 2, 2018), https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260.

20*. Id.*

21. *Id.*

22. *Id.*

23*. Id.*

24*. Interested in Powerful Real-Time Retail Analytics?,* THASOSGROUP, http://thasosgroup.com/blog/interested-retail-analytics/ (last visited Oct. 12, 2019).

25. Dezember, *supra* note 19.

26*. Alternative Data: Applications & Case Studies*, EAGLE ALPHA 10-14 (Sept. 8, 2017), https://s3-eu-west-1.amazonaws.com/ea-pdf-items/Alternative_Data_Report_Version_2.pdf.

27. Horton, *supra* note 5 at 3 ("Subscription costs for many of the services offered by data vendors are often lower than building the requisite structure internally.").

28*. Id*.

Discretionary datasets, which "provide near real-time insight, and longer-term trends, into spending at retailers and on specific products," offer investment managers insight into issuers' performance before the issuer releases earnings publicly. [29] In the municipal-bond space, investment managers have leveraged alternative datasets to understand the economic performance of state, local, and federal governments.[30] IHS Markit, which is "one of the largest data, insights and analytics firms in the world, [which] leverages 1,500+ traditional and non-traditional datasets to provide unique and timely insights to better inform investment decisions,"[31] used real-time ship tracking technology to analyze the number of cruise ships at port in Puerto Rico from 2014 to 2017. [32] The company found that there was a correlation between the cruise ship data and the island's gross revenues. From this correlation, IHS Markit was able to deduce that small declines in cruise ship traffic were predictive of a decline in tax collections over the subsequent months.[33] IHS Markit also leveraged its database of automotive ownership to track changes in luxury vehicle registrations in the United States in order to understand capital and population migration across states.[34] IHS Markit notes that its database allows for tracking the model and year of each vehicle leaving a state, as well as its destination state, which "is one potential gauge for the movements of higher income and net worth individuals among states."[35] Tracking the movements for certain "vehicle owners could be a proxy for the number of executives following companies to states with fast-growing industries" or could signify "owners moving or expanding to more business-friendly states."[36]

Matthew Granade, Chief Market Intelligence Officer at Point72, an asset management firm led by former S.A.C. Capital CEO Steven A. Cohen, summarized the disruptive impact of alternative data on the market research process:

> [I]t is a real change from how investing used to work . . . if you want to understand what is going on with McDonald's, you are going to have to look at credit card transactions data, you are going to look at geo-location data, at app downloads and handful of other things. And suddenly you are

---

29. Alternative Data: Applications and Case Studies, *supra* note 26, at 15, 21.

30*. See* Alternative Data: Applications & Case Studies, *supra* note 26, at 17-18; *see also* Chris Fenske, *Boats, Quotes, and Automobiles: Alternative Data for Municipal Bond Investors*, FACTSET (July 14, 2017), https://insight.factset.com/boats-quotes-and-automobiles-alternative-data-for-municipal-bond-investors.

31. IHS MARKIT, https://ihsmarkit.com/topic/alternative-data-and-insights.html (last visited Oct. 12, 2019).

32. Fenske, *supra* note 30.

33*. Id.*

34*. Id.*

35*. Id.*

36*. Id.*

going to have a very robust picture of how McDonald's is going and you are not going to have to talk to McDonald's about that.[37]

Evan Schnidman, founder and CEO of Prattle, an alternative data vendor which uses machine learning to analyze linguistical patterns in corporate and governmental disclosures,[38] noted, "in many ways, alternative data is what we used to think of as research."[39] Nevertheless, the use of alternative data still plays a supplementary role in the research process for many, especially smaller, investment managers. As of 2019, 80% of investment managers with assets under management (AUM) over $10 billion surveyed in the 2019 EY Global Alternative Fund Survey indicated that they were purchasing datasets from alternative data vendors (among other sources).[40] In contrast, just 48% of investment managers with AUM of $2 billion to $10 billion and 33% of investment managers with AUM of under $2 billion indicated that they were currently obtaining data from alternative data vendors.[41]

This discrepancy is largely due to the high signal-to-noise ratio of many alternative datasets, and the degree of effort and capability required to separate the proverbial needles from the haystack.[42] Indeed, there are many ways in which a dataset can fail to be useful (timeliness, completeness, business need, statistical correlation/predictive power, etc.), and failing in any manner can render the dataset useless.[43] To make matters worse, some datasets are delivered in unstructured, non-traditional formats, such as satellite images or voice recordings, which makes them difficult to incorporate into trading models.[44] For investment managers, and for alternative data vendors themselves, this means dedicating resources to

---

37. Alternative Data: Applications & Case Studies, *supra* note 26, at 21-22.

38. Horton, *supra* note 5 at 2.

39. *Id.* at 1.

40. *2019 Global Alternative Fund Survey*, EY, 40 (2019), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/wealth-and-asset-management/ey-global-alts-fund-survey-final.pdf.

41. *Id.*

42. Tamer Kamel, *So Much Data, So Little Alpha*, QUANDL (July 11, 2019), https://blog.quandl .com/monetize-data-for-finance-with-care?utm_source=google   &utm_medium=organic&utm campaign=&utm content=category /alternative-data ("More data is, of course, a good thing. But the signal to noise ratio is deteriorating. Finding a powerful alternative dataset has always been a needle in a haystack problem. But now the volume of hay is growing faster than needle count. For data driven investors, the opportunity set is growing but so too is the work required to process it all.").

43. *Id.* (Arguing that datasets are subject to the Anna Karenina principle, which states, "happy families are all alike; every unhappy family is unhappy in its own way." In other words, useful data sets share certain uniform, objective criteria: "Data is not like antiques on eBay. One man's data trash is not another's data treasure. Beauty is not in the eye of the beholder; data is objectively good or bad." Thus if a data set fails on any one of those criteria, it becomes useless, in its own way).

44. *Alternative Data: Application and Best Practices for Investment Management Firms*, DOW JONES NEWSWIRE 11 (2019), https://images.dowjones.com/wp-content/uploads/sites/35/2019/ 02/25200135/Alternative-Data-Application-and-Best-Practices-for-Investment-Management-Firms.pdf ("Alternative data comes in many different formats. Drawing these data sets into a form that can be applied to analytical trading and investment models can be challenging. Alternative data is often unstructured, and there is no general-purpose messaging middleware or other platform solution for this kind of data, as there is for real-time data or historical/reference data.").

attempting to distinguish between useful and useless datasets; a process which is neither quick nor easy.[45] In order to come up with one or two useful datasets, analysis of approximately fifty datasets is needed;[46] and assessing the value of each dataset (should be) a comprehensive process which includes back-testing, reviewing data hygiene, collection, transfer, and storage procedures, assessing legal and regulatory risks including privacy concerns such as whether data contains personally identifiable information (PII), whether the dataset can be integrated into trading models, and other tests.[47] In summary, "[r]eliable data is hard work."[48]

As a result, "the most prominent consumers of this data on Wall Street are managers of 'quant' funds, which devour massive quantities of data and translate that data into investment decisions via complex algorithms."[49] However, traditional investment managers are also increasingly incorporating alternative data and other quantitative strategies into their investment decisions,[50] and many use alternative datasets to validate hypotheses or conclusions based on traditional research.[51] Even private equity funds, which have traditionally lagged behind hedge funds in using alternative data as part of their investment process, are increasingly experimenting with alternative data.[52] According to the 2019 EY Global Alternative Fund Survey, 56% of private equity managers surveyed either use alternative data or expect to, an increase from 52% in 2018.[53] According to Alternative Data Insider, an alternative data industry group which tracks alternative data vendors and maintains a public database of vendor firms,[54]

---

45. *Id.* at 2 ("But sourcing, evaluating, integrating, and using alternative data is a non-trivial exercise. Many providers of alternative data are experts in their field, but inexpert when it comes to data provision. Alternative data sets may be incomplete or unverifiable; they may be unstructured in format and difficult to integrate; they may include data that isn't permitted for redistribution under new privacy rules. And there may be limited or no archive available for back-testing.").

46. *Id.* at 10.

47. *Id.* at 10-14.

48. *Id.* at 14.

49. *See* Peter Altman, Kelly Handschumacher, & Jennifer Hustwitt, *Big Data and the Risks of Insider Trading*, BLOOMBERG L. SEC. L. DAILY (Mar. 14, 2018), https://www.akingump.com/images/content/6/5/v2/65585/spBigData-SRLR-March-19-2.pdf.

50. *Id.*

51. Horton, *supra* note 5, at 3 ("[W]hile SpaceKnow has traditionally provided data to quantitative hedge funds, they are working with an increasing number of traditional, fundamental-driven investors who are looking to overlay their fundamental investment processes with alternative data insights.").

52. 2019 Global Alternative Fund Survey, *supra* note 40, at 39 ("For years, private equity managers have trailed their hedge fund peers in using next generation data as part of the investment process. The gap is closing as year over year more private equity managers are using advanced data in the front office. Use case examples among private equity include identifying potential investment targets and using new financial metrics to determine valuations.").

53. 2019 Global Alternative Fund Survey, *supra* note 40, at 39.

54. Sanford Bragg, *Free Database of Alternative Data Sources Launched*, INTEGRITY RESEARCH ASSOCS. (Aug. 23, 2017), http://www.integrity-research.com/free-database-alternative-data-sources-launched/.

there are currently 445 alternative data provider firms, and the group projects that total buy-side spending on alternative data will be $1.7B by 2020, up from $232M in 2016.[55] Despite the proliferation of alternative data across the investment management industry, returns remain surprisingly difficult to quantify—only about 30% of managers have attempted to quantify the benefits of alternative data use and those who have not are increasingly facing questions about the ROI of data acquisitions.[56]

II. LEGAL OVERVIEW: FEDERAL SECURITIES LAWS

Where Part I discussed several of the business risks posed by the use of alternative data, Part II reviews an equally important risk posed by alternative data use: legal and regulatory risk.[57] Although alternative data users should be cognizant of all relevant legal risks, the most critical are violations of the United States federal securities laws discussed below, which represent an existential threat to investment managers.[58] Jeffrey Neuburger, a partner at Proskauer, cautions:

> The most important legal concerns relate to violations of the securities laws . . . Commercial issues can be worked out quietly, but issues with the SEC or the DOJ are in another league. While the SEC and DOJ haven't brought any cases yet in the alternative data space, they've been active in breach of duty cases and hacking cases, so I expect them to begin to focus on it more.[59]

Derek Steingarten, a partner at K&L Gates, agrees: "The big brand-killer for any manager is a regulatory investigation that is alleging a breach of securities law in pursuing trading strategies. The fund will long be out of business before a determination has been made as to whether the actions were appropriate or not."[60] SEC and DOJ investigations also expose investment

---

55. ALTERNATIVE DATA.ORG, https://alternativedata.org/stats/ (last visited Oct. 27, 2019).

56. 2019 Global Alternative Fund Survey, *supra* note 40, at 40.

57. Although outside the scope of this Note, in addition to risks posed by violations of the United States federal securities laws, alternative data use also may expose firms to a litany of contractual, intellectual property and tort claims, state and local laws around PII, and other United States and foreign laws on individual data privacy. For example, an ongoing lawsuit filed by the city of Los Angeles, California alleges that the Weather Channel sold user location data to third parties, including hedge funds, in violation of California state law and The Weather Channel's own user privacy policy. Hollie Silverman & Joe Sterling, *Weather Channel App Sued Over Alleged Mining of Users' Data*, CNN (Jan. 5, 2019), https://www.cnn.com/2019/01/05/us/weather-channel-app-suit/index.html. *See also* Horton, *supra* note 5, at 5 ("Managers must understand not only the misappropriation framework under the Securities Exchange Act of 1934, but also how the New York State Attorney General and regulators in the E.U. pursue insider trading claims. Additionally, whether engaging internally in web scraping or purchasing scraped data from third parties, managers must be conscious of contractual, intellectual property and tort claims that a site owner may allege against a fund manager. Finally, many of the largest challenges posed by the use of big data are practical or ethical in nature.").

58. Horton, *supra* note 5, at 5.

59. *Id.*

60. *Id.*

managers to particularly unpleasant consequences, including large disgorgement and penalty judgments, officer/director and trading bars, loss of professional licensure, personal reputational damage, large legal bills, and in the most severe cases, criminal penalties including prison.[61]

A. Insider Trading: Rule 10b5-1

For investment firms and other end-users of alternative data, the most important regulatory concern is insider trading, or trading based on material, non-public information (MNPI).[62] Insider trading is governed by SEC Rule 10b5-1 (Rule 10b5-1), which prohibits the purchase or sale of a security of any issuer:

> On the basis of material, nonpublic information about that security or issuer; in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information.[63]

1. Materiality

For information to be material, "there must be a substantial likelihood that the fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of public information."[64] The "total mix" of public information available is a fact-specific inquiry based on contextual factors to determine if the inside information would have affected a reasonable investor's view of a particular investment decision.[65] In other words, information is material if there is a substantial likelihood that a reasonable investor would consider it important in deciding how to invest.[66]

There is no bright-line test for materiality; however, case law and SEC pronouncements have explained that information such as "earnings, mergers, acquisitions, tender offers, joint ventures, or changes in assets; significant new products or discoveries, or significant developments regarding customers or suppliers; changes in control or in management; change in auditors; significant events regarding the issuer's securities; and bankruptcies

---

61. *See, e.g.*, Bradley J. Bondi & Steven D. Lofchie, *The Law of Insider Trading: Legal Theories, Common Defenses, and Best Practices for Ensuring Compliance*, 8 N.Y.U. J. Law & Bus. 151, 201 (2012) ("The consequences for noncompliance with the laws pertaining to insider trading can be devastating. The DOJ may bring a criminal prosecution, resulting in a significant prison sentence and fine if an individual defendant is found guilty. The SEC may bring an enforcement action seeking disgorgement of ill-gotten gains (or losses avoided), a civil monetary penalty, and certain professional bars.").

62. *See supra* notes 58-61 and accompanying text.

63. 17 C.F.R. § 240.10b5-1 (2012).

64. SEC v. Huang, 684 F. App'x. 167, 172 (3d Cir. 2017).

65. *Id.*

66. SEC v. Mayhew, 121 F.3d 44, 51 (2d Cir. 1997).

or receiverships" are all material.[67] In *SEC v. Huang*, a case where a corporate insider stole a dataset of credit card transactions from his employer, the Third Circuit found that the dataset of credit card transactions collected by Huang was material when it represented just 2.4% of all credit card transaction revenues at a particular retailer, because it still allowed Huang to predict revenue more accurately than those with only publicly available data.[68]

Although materiality is traditionally determined from the standpoint of a reasonable investor, managers leveraging alternative datasets should understand that courts will generally view information in the context in which it was conveyed, taking into account whether the investor is sophisticated and whether they may also have the benefit of other additional information.[69] In addition, courts have found that individual investor behavior and willingness to pay for information can give rise to a sufficient inference that the information is material, and that information that is vague or uncertain can also be found to be material.[70]

2. Nonpublic Information

Nonpublic information becomes public for Rule 10b5-1 purposes in only one of two ways: (1) when it is "disclosed to achieve a broad dissemination to the investing public generally and without favoring any special person or group;"[71] or (2) when information known by only a few persons has been traded on by those particular persons to such an extent that the information is "fully impounded into the price of the particular stock."[72] To constitute nonpublic information, the information must be specific and more private than general rumor.[73] Further, information is nonpublic if it is more specific or more certain than publicly available information, or if it provides confirmation of public or press speculation.[74]

The SEC has argued in at least one case that MNPI which was disseminated via a subscription service did not qualify as public disclosure for Rule 10b5-1 purposes.[75] In *In re Certain Trading in the Common Stock of Faberge, Inc.*, the SEC charged a number of broker-dealers and investment

---

67. Harry S. Davis, *Overview of the Law of Insider Trading*, PRACTISING L. INST., 3 (2017), https://legacy. pli.edu/product_files/Titles/4553/%23172874_Insider%20Trading%20AB%202017_2016100509 5421.pdf.

68. *Huang*, 684 F. App'x. at 173.

69. Bondi & Lofchie, *supra* note 61, at 183 (citing SEC v. Happ, 392 F.3d 12, 21-23 (1st Cir. 2004)).

70. *Id.* at 182-83 (citing SEC v. Thrasher, 152 F. Supp. 2d 291, 301 (S.D.N.Y. 2001); United States. v. Cusimano, 123 F.3d 83, 88 (2d Cir. 1997)).

71. *Mayhew*, 121 F.3d at 51 (citing Dirks v. SEC, 463 U.S. 646, 653 n. 12, (1983) (citing In re Faberge, Inc., 45 S.E.C. 249, 256 (1973))).

72. *Id.* at 51 (citing United States v. Libera, 989 F.2d 596, 601 (2d Cir. 1993)).

73. *Id.* at 50.

74. United States v. Mylett 97 F.3d 663, 666 (2d Cir. 1996).

75. In re Certain Trading in the Common Stock of Faberge, Inc., 45 S.E.C. 249, 6 (1973).

advisers with insider trading in violation of Rule 10b5-1.[76] In that case, a broker-dealer and Faberge investor, after receiving news of poor Faberge earnings from Faberge's Vice President of Finance, disseminated the news via AutEx, a subscription-based service for institutional investors, and then used the same information to inform his own trading in Faberge securities.[77] The SEC argued that the AutEx transmission did not qualify as public dissemination of the earnings news because it was sent only to a limited number of institutional subscribers.[78]

In *SEC v. Mayhew*, the Second Circuit determined that confirmation by a corporate insider of a widely-rumored impending merger constituted nonpublic information because the insider's confirmation of the merger lessened the risk associated with uncertainty about the accuracy of the rumors.[79] The court further found that the rumored merger had not been fully impounded into the company's stock price because although the share price did increase on rumors of the merger in the financial press, it subsequently declined when the merger did not immediately come to fruition, and later increased by over 20% when the merger was later announced to the public by the company.[80]

In *United States v. Libera*, the Second Circuit held that information contained in pre-publication copies of Business Insider magazine, which the defendant purchased from a friend who worked at the magazine's printer, constituted nonpublic information.[81] The court found the defendant's friend had breached a fiduciary duty to his employer by taking the magazines outside of the plant in violation of the publisher's policy that all such information must remain confidential until the time of publication.[82] The court further found that the defendant knew that his friend had breached such a duty to his employer because the defendant was willing to compensate his friend by paying well above normal market price for copies of the magazine pre-publication.[83] The court also rejected the defendant's argument that Business Insiders' recommendations had been fully impounded into the price

---

76. *Id.*

77. *Id.*

78. *Id.*; *see also* In re Keyspan Corp. Sec. Litig., 383 F. Supp. 2d 358, 373 (E.D.N.Y. 2003) (finding that electronic filings with the SEC are public disclosure documents available to the investigation public by dissemination in a manner reasonably calculated to reach investors. . . through recognized channels of distribution); SEC v. Tex. Gulf Sulphur Co., 401 F. 2d 833, 853-54 (2d Cir. 1968) (holding that MNPI regarding discovery of a mineral deposit which was communicated to a reporter but not yet transmitted via a planned national financial news media release was not disseminated to the investing public generally); DuPont Glore Forgan, Inc. v. Arnold Bernhard & Co., No. 73 Civ. 3071, 1978 WL 1062, (S.D.N.Y. Feb. 27, 1978) (holding that a press release regarding poor airline earnings that was released via Reuter's wire service, which was less widely used than the Dow Jones broad tape, was nevertheless publicly disseminated).

79. SEC v. Mayhew, 121 F.3d 44, 51 (2d Cir. 1997).

80. *Id.*

81. United States v. Libera, 989 F.2d 596, 601 (2d Cir. 1993).

82. *Id.* at 601-02.

83. *Id.*

of the securities prior to the defendant's trades because although the price had been increasing prior to the defendant's trading, he was nevertheless able to profit by trading ahead of the magazine's publication.[84]

Thus, information which may be included in alternative datasets, which is released directly by an issuer via traditional channels (such as a Form 8-K or a press release) or is publicly observable (such as the number of cars in a parking lot), is unlikely to constitute nonpublic information, even if useful insights are gleaned from reviewing information of this type which is not yet reflected in the price of the issuer's stock.[85] However, not all information released by a company directly necessarily becomes public—for example, if a company sells its users' location data to a vendor, who processes the data and sells it to a hedge fund, that data could be considered non-public because it was not released to the investing public generally, but rather to one or more investors who paid for it.[86] Further, if a trader could profit by trading on insights obtained from the purchased data, it would be difficult for the trader to argue later that the information was so widely available that it had been fully impounded into the price of the security.[87]

3. Breach of a Duty

There is no general duty between market participants to forgo trading based on MNPI—including MNPI which may be included in alternative datasets—under Rule 10b5-1.[88] Rather, the duty to disclose such information or abstain from trading on it arises from some specific fiduciary relationship between two parties.[89] Such a fiduciary relationship can conventionally be violated in one of two ways: (1) under the "classical" or "traditional" theory of insider trading, whereby a corporate insider trades on the basis of MNPI in the securities of his or her own corporation in breach of his or her fiduciary

---

84. *Id.*

85. Bondi & Lofchie, *supra* note 61, at 175-76.

86. There is minimal case law that discusses when information has been disseminated to the investing public, and even fewer cases which have addressed the issue since the advent of modern technologies such as search engines and algorithms that monitor websites for breaking news. Regulation FD (see *infra* notes 120-124 and accompanying text) notes that information posted to a website which does not require a subscription or membership to view the content is considered public for purposes of Regulation FD; however, Regulation FD also clearly explains that a violation of its provisions, standing alone, is not sufficient to give rise to liability under Rule 10b5-1. *See* Bondi & Lofchie, *supra* note 61, at 172-76; *see also* SEC, Release 33-7881, 34-43154, IC-24599, *Final Rule: Selective Disclosure and Insider Trading* (Oct. 23, 2000) [hereinafter SEC Rel. No. 33-7881, Regulation FD] ("[T]o remove any doubt that private liability will not result from a Regulation FD violation, we have revised Regulation FD to make absolutely clear that it does not establish a duty for purposes of Rule 10b-5 under the Securities Exchange Act of 1934. The regulation now includes an express provision in the text stating that a failure to make a disclosure required solely by Regulation FD will not result in a violation of Rule 10b-5.") *see also* 17 C.F.R. §243 (codification of Regulation FD).

87. See discussion of *Mayhew* and *Libera*, *supra* notes 80-85 and accompanying text.

88. United States v. O'Hagan, 521 U.S. 642, 661 (1997).

89. *Id.*

duty to the shareholders of the same corporation; or (2) under the "misappropriation" theory whereby an individual misappropriates, and subsequently trades on, MNPI in breach of a duty owed to the source of that information.[90]

Courts have applied the misappropriation theory of insider trading where employees have stolen information from their employer. In *SEC v. Huang*, the defendant, an employee of Capital One, used Capital One transaction data to predict revenues of various retail companies accepting Capital One credit cards and subsequently used that information to inform his trading in the securities of those retailers.[91] In a jury trial, the U.S. District Court for the Eastern District of Pennsylvania found that the credit card data was both material and nonpublic, and that the defendant had breached his fiduciary duty to his employer by stealing it.[92]

Courts have also applied the misappropriation theory of insider trading where there is no apparent fiduciary duty owed but where the defendant fraudulently obtained insider information. In *SEC v. Dorozkho*, the defendant hacked into Thompson Financial's computer system in order to obtain confidential press releases before they were released to the public.[93] In remanding to the district court, the Second Circuit found that while the defendant owed no fiduciary duty to Thompson Financial or any other third-party, such a fiduciary relationship is not a necessary element for Rule 10b5-1 liability to exist when the defendant has made affirmative fraudulent misrepresentations.[94] The court further explained that while silence is only fraudulent if there is a duty to disclose—as under the traditional and misappropriation theories—affirmative misrepresentations are fraudulent absent any fiduciary duty within the context of Rule 10b5-1.[95]

Thus, if an investment manager purchases a dataset from a vendor, assuming that the dataset contains MNPI, the critical question with respect to whether trading on the basis of that dataset might give rise to Rule 10b5-1 liability is whether the dataset has been obtained in breach of a duty of trust or confidence.[96] Managers sourcing data from vendors must therefore understand how the vendor sourced the data, and managers sourcing data in-

---

90. *Id.* at 651-53.

91. SEC v. Huang, 684 F. App'x. 167, 168-69 (3d Cir. 2017).

92. *Id.* at 173.

93. SEC v. Dorozkho, 574 F.3d 42, 44 (2d Cir. 2009).

94. *Id.* at 49–50.

95. *Id.* at 50.

96. As the discussion above makes clear, determining whether an alternative dataset contains information which is both material and nonpublic requires legal inquiries independent of whether that dataset has been obtained in breach of a duty. However, the fact that fund managers are (1) willing to pay substantial sums for these datasets (or dedicate internal resources to sourcing them in-house), and (2) willing to use them to inform their trading strategies, would seem to inherently suggest that the datasets must contain some measure of MNPI. Indeed, if the information were in fact not material and was widely available to the public, one would reasonably ask why it would be valuable at all.

house must review contracts and other terms and conditions to ensure that data is not being obtained in breach of a duty.[97] For example, a fund purchasing data from a vendor who sourced that data through hacking, purchases from unauthorized employees, or other deceptive means, would likely be exposed to Rule 10b5-1 liability analogous to the stolen Business Insider magazines in *Libera* and the hacking in *Dorozkho*.[98]

B. SECTIONS 204A AND 15(G)

204A requires every investment adviser to establish, maintain, and enforce written policies and procedures reasonably designed to prevent the misuse of MNPI by investment advisers.[99] 15(g) is a parallel provision to 204A that requires the same of registered broker-dealers.[100] "There is no requirement under 15(g) that there be an underlying insider trading violation or other violation of the Exchange Act or the rules thereunder."[101]

The SEC has brought at least two enforcement actions for violations of 204A and 15(g) related to MNPI obtained from third parties. In *In re Marwood Group Research, LLC*, the SEC charged Marwood with failure to abide by its own policies and procedures requiring employees handling MNPI to report the information to the firm's compliance function. Marwood, a broker-dealer and political intelligence firm, gathered MNPI from the U.S. Food and Drug Administration and other government employees and sold research reports based in part on that information to hedge funds and other clients.[102] The SEC further argued that Marwood's policies and procedures were not reasonably designed to prevent the misuse of MNPI given: (1) the nature of Marwood's business preparing research notes which would be sold to clients who were expected to use the notes to inform their securities trading; (2) Marwood employees' regular interaction with government employees who possessed MNPI; and (3) the fact that the determination of whether information received from government employees constituted MNPI was made by Marwood's line employees rather than its Chief Compliance Officer (CCO).[103] Further, the SEC has maintained the position that if the nature of a broker-dealer or investment adviser's business exposes employees to individuals in possession of MNPI on a regular basis, a policy that those

---

97. See discussion on suggested compliance controls *infra* Part IV.

98. See discussion on United States v. Libera and SEC v. Dorozkho, *supra* notes 81–84 and 93–95.

99. 15 U.S.C.A. § 80b-4a (2012).

100. In re Gintel, Asset Mgmt. Inc., Advisers Act Rel. No. 2079 (Nov. 8, 2002); 15 U.S.C. § 78o(g) (formerly section 15(f) prior to 2010 renumbering).

101. In re Monness, Crespi, Hardt & Co., Inc., Exch. Act Rel. No. 72886 (Aug. 20, 2014).

102. In the Matter of Marwood Grp. Research, LLC, Exch. Act Rel. No. 76512 (Nov. 24, 2015).

103. *Id.*

employees self-evaluate whether information they receive from those individuals is in fact MNPI is insufficient to comply with 204A and 15(g).[104]

In *In re Deerfield Management Company, L.P.*, the SEC charged Deerfield with failure to establish, maintain, and enforce policies and procedures to address the risk of employees' misuse of MNPI obtained from political intelligence research firms retained by Deerfield.[105] Deerfield relied on its employees to self-evaluate and self-report potential receipt of MNPI, but failed to implement any procedures to ensure that the employees did so.[106] Further, Deerfield's policies and procedures regarding information obtained from third-party research firms was considerably less robust than its policies and procedures for expert networks.[107] Before engaging an expert network, Deerfield conducted a due diligence review of the network's compliance controls, and prior to beginning a consultation, required its analyst to provide an oral reminder to the expert not to disclose any MNPI.[108] After the consultation, the Deerfield analyst was required to enter a report on the consultation into the firm's internal database which was reviewed by Deerfield's head of research.[109] In contrast, Deerfield's policies and procedures specifically excluded research firms from this compliance process because research firms provided a "finished product based on the research firm's internal expertise and research."[110] Deerfield's compliance manual indicated that while Deerfield would conduct "diligence" on research firms, it would rely upon research firms to police their own conduct.[111] Further, Deerfield's compliance manual did not explain what these diligence reviews should entail or how Deerfield personnel should perform them; nor did Deerfield take any steps to enforce this requirement.[112] When Deerfield did review the policies and procedures of at least one research firm it retained, Deerfield continued to retain that firm and use information provided by it to inform trading decisions even after discovering red flags. One such red flag was that the firm's CCO was also a research analyst, and thus responsible for reviewing his own work. Deerfield had also received numerous emails from that same individual which contained MNPI regarding future government actions, and Deerfield took no actions to prevent the misuse of this MNPI[113]

---

104. *Id.* (citing In re Gintel, Asset Mgmt. Inc., Advisers Act Rel. No. 2079 (Nov. 8, 2002); In re Deprince, Race & Zollo, Inc., Advisers Act Rel. No. 2035 (June 12, 2002); In re Guy P. Wyserpratte, Advisers Act Rel. No. IA-1943 (May 2, 2001); In re Certain Market Making Activities on Nasdaq, Exch. Act Rel. No. 40910 (Jan. 11, 1999).

105. In the Matter of Deerfield Mgmt. Co., L.P., Advisers Act Rel. No. 4749 (Aug. 21, 2017).

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

III. ALTERNATIVE DATA PRESENTS THE SAME LEGAL RISKS AS EXPERT NETWORKS

The legal risks described in Part II are the same legal risks presented by the use of expert networks.[114] Expert networks are firms which connect industry experts, who may include academics, scientists, engineers, doctors, lawyers, suppliers, and former employees of a company, with clients in need of their particular expertise, who may include mutual and hedge funds, banks, private equity, and law firms.[115] For example, when a client needs an expert opinion about healthcare or consumer goods, the client accesses an online portal which connects them to an expert who—acting as an independent contractor—offers consultations, written reports, market studies, and/or other insights in exchange for fees that can exceed $1,000 per hour.[116] While the use of expert networks to inform securities trading is legal, there is a fine line between what experts can and cannot disclose if both the expert and the client are to remain in compliance with the securities laws.[117] Columbia Law School Professor John Coffee said of expert networks:

> I'm not saying there aren't legitimate expert networking firms, but they are a little like putting a group of teenagers together in one room with a lot of booze—something is going to happen. The expert network says there shall be no exchange of material non-public information, but why is the hedge fund paying $30,000 or $40,000 to meet those people?[118]

Expert networks are understood to have sprung up in response to the SEC's 2000 promulgation of Regulation Fair Disclosure (Regulation FD).[119] Regulation FD covers selective disclosure by issuers to securities market professionals and other holders of the issuer's securities who may be expected to trade or otherwise profit on the basis of the disclosure.[120] Specifically, Regulation FD requires that whenever an issuer, or any person acting on its behalf, discloses MNPI regarding that issuer or its securities to any of the covered parties, the issuer must also make public disclosure of the

---

114. *See e.g.,* Bondi & Lofchie, *supra* note 61, at 177; Daniel H. Jeng, *Expert Networks and Insider Trading: An Introduction and Recommendation*, 32 B.U. REV. BANKING & FIN. L. 245, 261-63 (2012-2013).

115. Bondi & Lofchie, *supra* note 61, at 177; Jeng, *supra* note 114, at 247-48.

116. Bondi & Lofchie, *supra* note 61, at 177; Jeng, *supra* note 114, at 248-49.

117. Jeng, *supra* note 114, at 254; *see also* SEC Rel. No. 2011-40, *SEC Charges Hedge Fund Managers and Traders in $30 Million Expert Network Insider Trading Scheme* (Feb. 8, 2011) ("It is illegal for company insiders who moonlight as consultants to sell confidential information about their companies to traders, and it is equally illegal to buy that corruptly obtained information and trade on it. . .While it is legal to obtain expert advice and analysis through expert networking arrangements, it is illegal to trade on material nonpublic information obtained in violation of a duty to keep that information confidential.").

118. Ronald D. Orol, *Expert Networks Key to SEC Insider-Trading Cases*, MARKETWATCH (Nov. 21, 2012), https://www.marketwatch.com/story/expert-networks-key-to-sec-insider-trading-cases-2012-11-21.

119. Bondi & Lofchie, *supra* note 61, at 177; Jeng, *supra* note 114, at 248-49.

120. SEC Rel. No. 33-7881, Regulation FD, *supra* note 87.

information.[121] Information is nonpublic for purposes of Regulation FD if it has not been disseminated in a manner making it available to investors generally.[122] However, "corporate management may reveal to securities analysts…non-public information that merely fills 'interstices in analysis,' or tests 'the meaning of public information.'"[123]

Because issuers could no longer release information to individual analysts without releasing it to the broader investing public generally after Regulation FD, analysts, seeking to fill an information void, turned to experts on particular issuers or industries for guidance.[124] By 2010, the expert network industry had grown to produce annual revenues of $400 million, according to a Harvard Business School case study.[125] However, this growth would be short lived—in 2011, Raj Rajaratnam of the Galleon Group was criminally convicted of insider trading and charged in a parallel SEC civil action which led to a $92.8 million judgment against him. Both cases involved Primary Global Research, an expert network firm.[126] Following Rajaratnam's conviction, the SEC brought a string of additional enforcement actions against several expert networks, including Primary Global Research, involving, in aggregate, 28 defendants and $400 million of alleged illicit profits.[127] Rajaratnam's conviction, and the subsequent expert network enforcement actions, unsettled the expert networks' Wall Street client base.[128] Industry revenue dropped by 20 to 30 percent during 2011.[129] Major industry players—including Och Ziff Capital Management, Millennium Partners, Morgan Stanley, and Credit Suisse—either adjusted their policies to limit the use of expert networks or suspended the use of them entirely.[130]

Since 2011, expert networks have rebounded and reached $1 billion in annual revenue industry wide as of 2018.[131] Gerson Lehrman Group (GLG), the largest expert network which captures 50% of the market, has 1,600 employees in 22 offices and over $500 million in annual revenue.[132] GLG engages with more than 600,000 experts and works with many of the world's

---

121. 17 C.F.R. §243 (2012).

122. SEC Rel. No. 33-7881, Regulation FD, *supra* note 87.

123. SEC v. Bausch & Lomb Inc., 565 F.2d 8, 14 (2d Cir. 1977).

124. Bondi & Lofchie, *supra* note 61, at 177; Jeng, *supra* note 114, at 249-50.

125. Jeng, *supra* note 114, at 253.

126. Evelyn Rusli, *Next Up, a Crackdown on Outside-Expert Firms*, N.Y. TIMES (May 11, 2011), https://dealbook.nytimes.com/2011/05/11/next-up-a-crackdown-on-outside-expert-firms; *see also* Orol, *supra* note 118.

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. Bruce Reed & Matthew Atwell, *The Rise of the Expert Economy: Could Sharing Wisdom be the Next Gig?*, CIVIC, 4 (2018), https://dfbaaa3e-0ce2-4de0-929d-4611a51646be.filesusr.com/ugd/03cac8_eb69a73ab4cc4141 af4b95880fe084b7.pdf (citing Sanford Bragg, *Expert Network Industry Nears $1 Billion*, INTEGRITY RESEARCH ASSOC., (April 12, 2018)).

132. *Id.*

largest banks, law firms, and industrial and pharmaceutical companies.[133] In the securities industry, a critical element of the resurgence of expert networks has been the development of robust compliance controls put in place by firms and internally at the expert networks themselves.[134] Robert Khuzami, former head of the SEC's Division of Enforcement, commented in a 2013 interview on whether expert networks might receive more regulatory scrutiny in the future:

> I think this is an example where the spotlight of law enforcement helped to clean up an industry. As a result of these prosecutions, those expert networks that crossed the line and used their companies to engage in insider trading are no longer in business. And also, hedge funds have imposed controls that make sure that their research analysts and traders do not, willingly or unwillingly, obtain inside information through these networks. These funds are conducting due diligence on the expert networks before they use them, making sure that the source of the information, and the information itself, is legitimate. They are asking for certifications to ensure that the expert network employee will not provide them with material nonpublic information. They are chaperoning the calls with expert networks, and taking other steps to make sure these networks are not being abused. So, it is a good example where law enforcement focuses on certain activity and it triggers steps by the industry to make sure abuses do not occur.[135]

Despite the progress that the expert network industry has made in compliance controls, the boundaries around expert networks and securities trading do remain fuzzy.[136] In March 2011, Preet Bharara, then the United States Attorney for the Southern District of New York, said there was "nothing inherently wrong or bad about hedge funds or expert networking firms or aggressive market research."[137] A few months later in October 2011, then SEC Chairwoman Mary Schapiro assured a hedge-fund industry trade group that "there is nothing wrong with doing tremendous due diligence"

---

133. *Id.* ("GLG works with nine of the world's 10 largest banks, more than 30 leading global industrials, nine of the 10 largest pharmaceuticals, and eight of the top 10 American law firms.").

134. *Id.* ("Somewhat ironically, heightened scrutiny of insider trading made the leading expert networks more sought after than ever. 'A lot of firms picked up share, rebounded quickly, and came out of the whole scandal in a stronger position,' says Integrity Research principal Sanford Bragg, who has tracked the sector for more than a decade. The leading firms beefed up their compliance policies and touted higher standards of professional ethics on their websites, requiring ethics training for experts. At some firms, clients can now 'chaperone' conversations between experts and employees, providing additional protections within a controlled environment. GLG alone now employs more than 50 compliance professionals, 'a key selling point for the company,' according to the *Financial Times*.").

135. Michael Mayhew, *Resurrection of Expert Networks*, INTEGRITY RESEARCH ASSOCS. (Nov. 11, 2013), http://www.integrity-research.com/resurrection-of-expert-networks/.

136. Jeng, *supra* note 114, at 262 ("The SEC thinks the rules are clear and that the line between illegal insider trading and permissive due diligence is a bright line. But it is not.").

137. Rusli, *supra* note 126.

with respect to stock research.[138] Statements like these provided somewhat minimal assurance to the expert network industry and clientele because the essence of the expert network—like the use of alternative datasets—is to provide information that is not readily available to the public.[139] If this information is also material and given in breach of a duty to its source, both of which are highly situationally-dependent, trading on the basis of the information could represent a violation of Rule 10b5-1.[140]

Rajaratnam's conviction also raised doubts about the continued viability of the "mosaic" theory of insider trading, whereby an analyst weaves together pieces of public facts and non-material disclosures to form a mosaic, which is only material after the pieces are assembled.[141] The mosaic theory is a perfectly legal investment strategy and can also operate as a defense in an insider-trading investigation.[142] However, Rajaratnam's case illustrates the difficulty of both leveraging the theory as a defense and determining whether information received—be it an alternative data set or information obtained through an expert network—constitutes a permissible piece of the mosaic or MNPI which violates insider-trading laws.[143]

Since 2011, the continuing viability of the mosaic theory as a defense has been a subject of debate. Some commentators have argued that the theory is no longer viable in light of Rajaratnam's conviction and aggressive prosecutorial definitions of insider trading by state and federal prosecutors and the SEC.[144] Others have argued that Rajaratnam's invocation of the mosaic theory as defense was unsuccessful not because of any issue with the mosaic theory itself; rather, it was the other more salient details of that case—such as the McKinsey consultant who admitted to receiving over $500,000 per year from Rajaratnam in exchange for McKinsey client secrets—which ultimately convinced the jury of Rajaratnam's guilt.[145]

---

138. Steve Eder, *SEC Chief Draws a 'Bright Line' on Insider Trading*, WALL ST. J. (Oct. 21, 2011), https://www.wsj.com/articles/SB10001424052970203752604576643474268068178 (Shapiro was responding to questions from hedge funds on whether regulators had set forth clear rules about expert networks and insider trading. Jamie Nash, a hedge fund lawyer who attended the conference, noted that Shapiro's comments "reinforced what the SEC's position has been all along . . . . There's nothing wrong with digging into the weeds and doing deep dives on your investments and potential investments. But you have to make sure you have robust compliance and controls.").

139. Bondi & Lofchie, *supra* note 61, at 177.

140. *Id.* at 177-78.

141. In the Matter of Dirks, SEC Rel. No. 34-17480, 1981 WL 36329 (Jan. 22, 1981).

142. Bondi & Lofchie, *supra* note 61, at 154-55.

143. *Id.* at 152.

144. See discussion *infra* note 154.

145. *See* Holman W. Jenkins, Jr. *Temporary Sanity in Insider-Trading Law*, WALL ST. J. (May 14, 2011), https://www.wsj.com/articles/SB10001424052748703864204576321013619678894 (arguing in a WSJ opinion piece that Rajaratnam was found guilty by the jury not because of prosecutor Preet Bharara's framing of the case as being about harm to ordinary investors, ("Unlawful insider trading should be offensive to everyone who believes in, and relies on, the market. It cheats the ordinary investor . . ."); rather, because of "concrete and smelly wrongs exposed in the courtroom" including "a McKinsey consultant [who] admitted to receiving $500,000 a year

Although case law directly involving the mosaic theory is limited,[146] at least one court has weighed in on the issue since 2011. In *SEC v. Steffes*, the SEC charged employees of a railroad company and several of their family members with insider trading.[147] There, the employees tipped off their family members after becoming aware that their employer appeared poised to be acquired based on rumors amongst fellow employees, their observation of people in suits touring the rail yards, and their having been asked to prepare inventories of company assets.[148] The SEC alleged that the fact that the company was for sale was MNPI and the employees had violated their fiduciary duty to their employer by informing family members and trading on the basis of that information,[149] and in doing so had violated Rule 10b5-1.[150] Although the employees and their family members were ultimately found not liable in a jury trial, in denying a motion for summary judgment filed by the employees, the court explained that it is "well established that a defendant can be held liable for insider trading when he or she obtains and acts on pieces of information, which, pieced together, constitute material nonpublic information."[151] The court further held that while the facts known by the defendants were not material standing alone, when taken together from the totality of information known to the defendants, the SEC could plausibly show that the information was material.[152] Although one commentator argued that *Steffes* stood for the proposition that "U.S. courts often do not recognize the mosaic theory as a defense at all,"[153] another countered that this "unjustifiably pessimistic assessment . . . fails to appreciate the nature of the case" because the defendants in *Steffes* were employees of the company who

---

under the table from Rajaratnam for betraying the secrets of McKinsey's clients [and] [a]n Intel executive [who] admitted accepting gifts and loans from Rajaratnam for blabbing inside information about Intel").

146. Allan Horwich, *The Mosaic Theory of Materiality – Does the illusion Have a Future?*, 43 SEC. REG. L. J. 129, 136 (2015) ("Very few cases have addressed the mosaic concept, fewer still by name.").

147. SEC v. Steffes, 805 F. Supp. 2d 601, 605 (N.D. Ill. 2011).

148. *Id.* at 616.

149. *Id.* at 607.

150. *Id.*

151. *Id.* at 610 (citing United States v. Mylett, 97 F.3d 663, 668 (2d Cir.1996)) (upholding criminal conviction for insider trading when the defendant "was never told about the acquisition and did no more than piece together evidence obtained while working for" the acquirer); SEC v. Binette, 679 F. Supp. 2d 153, 159 (D.Mass.2010) (citing SEC v. Materia, 745 F. 2d 197, 199 (2d Cir.1984) ("A defendant may be liable under the misappropriation theory when he pieces together incomplete fragments of confidential information provided through his employment to identify likely acquisition targets and then trades stock in those target companies.")); *see also* Horwich, *supra* note 147, at 136.

152. *Id.* at 613.

153. Horwich, *supra* note 146, at 139 quoting Greene and Schmid, *Duty-Free Insider Trading?*, 2013 COLUM. BUS. L. REV. 369, 415 (2013).

assembled their mosaic solely from internal corporate information, gained pursuant to their employment, that they knew was confidential.[154]

In any case, it seems clear that reliance on the mosaic theory as a defensive strategy exposes a defendant to considerable uncertainty regarding the robustness of the doctrine itself (what the current state of the law actually is) and how the court might apply the doctrine to the factual circumstances of the case (how that law applies to the defendant's particular circumstances). Investment managers using alternative data to inform their trading should understand this uncertainty and not rely heavily on the doctrine when developing policies and procedures to prevent insider trading.

IV. SOLUTION: COMPLIANCE CONTROLS TO GUARD AGAINST INSIDER TRADING

There is evidence that investment managers may not be sufficiently attuned to the risk that alternative data use could represent a securities law violation. According to a recent Lowenstein Sandler survey, just 33% of respondent hedge fund managers indicated that the risk that alternative datasets may contain MNPI was a major concern when gathering/purchasing and using alternative data, and just 21% indicated that increased compliance burden was a major concern.[155] In September 2018 remarks at Georgia State University College of Law, then SEC Commissioner Kara Stein described how alternative data market participants have prioritized returns over regulatory risk management: "This race to collect and control data is intensifying. Many firms and individuals are rushing onto the course but few are thinking about what the rules of the race should be. Most are focused on the potential benefits and not on the potential costs or unintended consequences."[156]

Thus, in order for alternative data to avoid becoming the next expert networks, investment managers should take seriously the risk that alternative datasets may contain MNPI.[157] As Part II discussed, an SEC or DOJ investigation arising from alternative data use presents an existential threat

---

154. Horwich, *supra* note 146, at 139 ("Steffes was not a case where some outsider, such as an analyst, pried one or two seemingly insignificant nuggets of information from an insider. On the contrary, the defendants were themselves corporate employees and their tippees and all of the information the employees allegedly used to form their mosaic—a term the court did not use—was gleaned either from their involvement in matters that were related to the proposed sale or activities they observed on company premises.").

155. Peter D. Greene, *Alternative Data = Better Investment Strategies, But Not Without Concerns*, LOWENSTEIN SANDLER, 10 (Sept. 2019) https://www.lowenstein.com/alternative datareport (follow the link and enter required information to access the report free of charge).

156. Stein, *supra* note 6.

157. See discussion *supra* Part III (reviewing the history of expert networks, which was marked by wide-spread adoption, followed by a landmark insider trading violation and an immediate steep decline in usage, and ultimately, measured re-adoption with compliance protections in place).

to investment managers.[158] In order to guard against this threat, managers should implement compliance programs that: (1) provide assurance that datasets have not been acquired in breach of a duty for purposes of Rule 10b5-1;[159] and (2) satisfy their obligations to establish, maintain, and enforce written policies and procedures designed to prevent misuse of MNPI under 204A and 15(g).[160] Establishing robust compliance procedures around alternative data will both protect firms from legal and regulatory risk and provide assurance to the SEC and DOJ that the firm takes its compliance obligations seriously.[161]

As in all areas of compliance and risk management, firms seeking to implement alternative data compliance procedures should observe general best practices, including creating a culture which encourages employees to report receipt of any MNPI—especially MNPI which may be sourced in an unusual way—to legal and compliance professionals,[162] documenting policies and procedures,[163] recording situations where employees have received MNPI and reported it to the legal and compliance function, and training employees on securities laws, identification of MNPI, and other potential red flags.[164] Firms should also ensure that responsibilities and

---

158. *See supra* notes 58-61 and accompanying text (explaining that violations of federal securities laws represent an existential threat to investment managers).

159. With respect to Rule 10b5-1, the most significant legal question will perhaps be whether alternative datasets have been purchased or made available for sale in breach of a duty. Regulation FD makes clear that a violation of its provisions is not sufficient alone to give rise to a breach of duty for 10b5-1 purposes. Thus, to prove a violation of Rule 10b5-1, the SEC must show that there was a breach of duty (outside of a potential Regulation FD violation) where a data seller has made a dataset available without having the contractual right to do so (e.g., a credit card company selling customer transaction data), or a firm has collected data in breach of some other contractual obligation (e.g., website scraping in violation of a site's terms and conditions).

160. See discussion on enforcement actions arising from violations of 204A and 15(g) *supra* Part II.

161. Bondi & Lofchie, *supra* note 61, at 200 ("It is important to be able to demonstrate to government investigators the extent to which a firm strives to comply with the law. For this reason, a firm should maintain consistent and thorough documentation of its compliance program. Firms should be able to show investigators that they have taken steps to inform employees of appropriate policies and procedures, actively followed through in implementing and enforcing the policies and procedures, and consistently investigated red flags and other unusual matters.").

162. *Id.* at 199 ("Compliance programs should encourage employees to voice concerns and question conduct where doubt exists as to the propriety of trading on certain information. Even firms with the most well-designed and well-operated compliance programs will find it difficult to completely safeguard themselves from all regulatory problems. Creating an atmosphere in which employees feel comfortable raising legal and compliance questions helps firms ensure that they are taking a broad view on regulatory concerns.").

163. *Id.* at 200.

164. *Id.* at 199 ("Training programs should be robust, regular, and well-documented, including topics covered and attendance. Such programs should focus on: the substance of the law; the substance of the firm's procedures; and the need to self-report or flag problematic issues for further discussion and review. To the extent possible, training should avoid abstract analysis and instead reflect and speak to real life activities and behaviors faced by firm personnel. . .Training should emphasize the need to immediately reach out to compliance and legal personnel when there is any doubt as to whether certain information can be used.").

reporting lines are appropriately delineated such that the compliance function enjoys sufficient independence from business pressures and support from upper management.[165]

While management should make clear to front-office employees that their obligations include protecting the firm from potential securities law violations, front-office employees, especially those involved in securities trading, should never be the firm's first and last line of defense.[166] Legal and compliance professionals should instead have a strong understanding of the firm's business practices and be monitoring those practices as well as individual employees for compliance with policies and procedures on an ongoing basis, and where proposed transactions may be especially fraught with legal or regulatory risk, providing ad-hoc approvals and advice.[167] Legal and compliance professionals should leverage legal publications and CLEs to stay abreast of the latest developments in the securities laws and understand that the laws around insider trading are highly nuanced and factually-dependent and will continue to evolve as business practices change and the SEC and DOJ develop new theories of insider trading liability.[168]

Effective compliance programs specific to alternative data will necessarily focus on due diligence on data vendors and data originators (companies actually generating alternative datasets as a byproduct of their business).[169] Due diligence on data obtained from vendors should be two-pronged: research on the data vendor, and research on the alternative datasets being considered.

First, buyers should perform due diligence on the vendor itself.[170] Data vendors may be small, private, opaque operations, with widely varying levels of legal sophistication and risk appetite, and alternative data purchasers should be mindful when assessing vendors that business practices have outpaced legal developments, few best practices exist, and some data vendors

---

165. See discussion on enforcement actions arising from violations of 204A and 15(g), *supra* Part II.

166. See generally discussion on compliance shortcomings in *Marwood* and *Deerfield*, *supra* notes 102-113.

167. Bondi & Lofchie, *supra* note 61, at 198 ("Supervisory programs should be ongoing and tailored to the particularities of a firm's business. Supervisors should meet regularly with persons supervised and should be fully informed of the person's conduct and of the business being conducted. Firms' supervisory procedures should include appropriate documentation of applicable processes, including (1) monitoring of employees' compliance with procedures; (2) supervisory approval; and (3) trade monitoring and review.").

168. *Id.* at 200-01.

169. As Part I discussed, most fund managers are sourcing data through vendors; however, to the extent that funds may be sourcing data themselves by contracting directly with data originators or collecting data through some other means, it will be necessary to perform due diligence on those data originators and relevant collection procedures in addition to due diligence on data vendors.

170. ROBERT LEONARD, JEFFREY NEUBURGER, JOSHUA NEWVILLE, & JONATHAN RICHMAN, Presentation, *Big Data and Hedge Funds: Current Legal and Compliance Issues*, PROSKAUER, 30 (June 7, 2017) (available at: https://s3.amazonaws.com/assets.production.proskauer/uploads/5c2ca cdac56dac24afdfaf2b73625e09.pdf).

may be particularly susceptible to market pressures to deliver valuable datasets.[171] Purchasers should therefore exercise skepticism when assessing vendors by asking questions in writing, getting contractual representations, warranties, and indemnifications,[172] and seeking to understand the vendor, its founders and employees, its methods and business practices, its other clients, and whether it has been involved in any litigation or government investigations.[173]

Second, buyers should perform due diligence on the alternative datasets they are considering purchasing.[174] Buyers should understand the nuts and bolts of how the vendor is sourcing the data, and should especially focus on ensuring that the vendor has the explicit right to sell the data, as a breach of duty for purposes of Rule 10b5-1 may arise from data obtained by deceptive means (which could potentially include, for example with web-scraping, a violation of a website's terms and conditions) or data sold in violation of a contract with the data originator.[175] As part of this diligence, buyers should request and review contracts and other relevant agreements, avoid relying on the vendor's legal analysis, spot check the dataset, and carefully document the diligence procedures performed.[176] Vendors and recurring alternative datasets should be recertified on an ongoing basis, and buyers should be clear with vendors about their aversion to MNPI and trust in their instincts about the vendor and its data offerings.[177]

To the extent that firms may be sourcing alternative data in-house by contracting directly with data originators or collecting it via other means such as web scraping, it will be necessary to perform due diligence focused on whether such contract or other sourcing method could represent a breach of duty.[178] With respect to contracts with data originators, buyers should focus on whether the originator has the right to sell the data, as a breach of a contractual obligation to a customer to keep information confidential, for example, could represent a potential breach of duty for Rule 10b5-1

---

171. *Id.*

172. Buyers of alternative datasets should be aware, however, that contractual representations, warranties, or indemnities may not shield them from government investigations, litigation, or other adverse publicity if they either know or are reckless in not knowing that the dataset they are purchasing has been sold to them in breach of a duty for purposes of Rule 10b5-1. In the civil context, an insider-trading claim requires the government to show that the defendant was at least reckless in not knowing whether he or she was trading on the basis of MNPI obtained in breach of a duty, and in the criminal context, the government must show that the defendant acted "willfully," a standard which has been interpreted inconsistently by the lower courts, but case law seems to approximate a standard which is roughly recklessness. *See* Davis, *supra* note 67, at 4; *see also* Miriam H. Baer, *Insider Trading's Legality Problem*, 127 YALE L. J. F. 129 (2017).

173. LEONARD, ET AL., supra note 170, at 33-36.

174. *Id.* at 33.

175. *Id.* at 23-24.

176. *Id.* at 33, 38.

177. *Id.* at 33-36.

178. *Id.* at 23-28.

purposes.[179] Buyers should also ensure that their contract with the data originator gives them the right to use the data to inform securities trading, as a breach of the contract's terms could also represent a potential breach of duty under Rule 10b5-1's misappropriation theory.[180] Firms sourcing data in-house via other means, such as web-scraping, should ensure that their methods do not involve deception, misrepresentations of their identity, violation of site's terms and conditions, or any other means of gaining unauthorized access or otherwise circumventing controls such as "captchas," as any of these would likely represent a breach of duty under the misappropriation theory of Rule 10b5-1.[181] As with due diligence on vendors, firms contracting with data originators or sourcing data via other means in-house should request and review relevant documentation, ask questions in writing, get contractual assurances that the originator has the right to sell the data, and document all procedures performed.[182]

In addition to establishing Rule 10b5-1 compliance procedures for alternative data use, firms should also be mindful of their obligations under 204A and 15(g).[183] It is critical for firms to not only implement policies and procedures designed to protect MNPI and avoid insider-trading, but to also monitor compliance with those policies and procedures on an ongoing basis.[184] Firms should avoid the compliance failures of *Marwood* and *Deerfield* by: (1) ensuring that line employees, especially those involved in securities trading, are not permitted to self-evaluate whether alternative datasets contain MNPI; (2) documenting detailed procedures on how diligence reviews of alternative data vendors, contracts, and other sourcing methods are to be performed; (3) avoiding relying on alternative data vendors to police their own conduct with respect to distribution of MNPI; and (4) monitoring employees for compliance with policies and procedures on an ongoing basis.[185]

---

179. *Id.* at 25.
180. *Id.*
181. *Id.* at 23-24, 37.
182. *Id.*
183. *See supra* notes 99-113 and accompanying text.
184. *Id.*
185. *Id.*

CONCLUSION

Every day, companies collect millions of data points from every American with a smartphone.[186] The data is nearly simultaneously packaged up and sold in huge datasets to a wide variety purchasers for a wide variety of reasons, including personally-targeted advertising, political activism, and understanding consumer movements and behaviors.. [187] This massive proliferation of alternative data throughout every facet of modern life means that use of these datasets to inform securities trading is not going away. However, investment managers leveraging these alternative datasets should understand that modern practices are far ahead of the nuanced and factually-dependent securities laws, and that doing so without the appropriate guardrails may expose them to substantial and devastating legal and reputational risks.

The history of expert networks offers a cautionary tale that wide-spread adoption and common industry practices will not protect investment managers from insider-trading investigations and prosecutions if their conduct is violative of the law, nor is the mosaic theory likely to provide a substantial defensive shield. The best defensive strategy is therefore a good offensive strategy—a robust compliance program around alternative data use will help prevent insider trading and inadvertent receipt of MNPI, satisfy the firm's obligations under 204A and 15(g), and in the event of a
government investigation, prosecution, or enforcement action, provide defenses and evidence that the firm acts in good faith to comply with the laws.

<div align="right">

William Montemarano[*]

</div>

---

186. Thompson & Warzel, *supra* note 1.

187. See e.g., Sam Schechner, Emily Glazer, & Patience Haggin, *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, WALL. ST. J. (Oct. 10, 2019), https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889 (explaining that a Republican PAC had hired an outside company to "collect unique identification numbers from attendees' smartphones that evening [at a campaign event], based on location data those phones were sending to third parties. The goal was to target ads at people it could drive to the polls the next day.").