THOMSON REUTERS
Westlaw®

Big data, hedge funds, securities regulation, and privacy: mitigating liability in a changing legal landscape

By Charles D. Riely, Esq. Keisha N. Stanford, Esq., and Logan J. Gowdey, Esq., *Jenner & Block*

NOVEMBER 21, 2019

By now, it is no secret that the use of big data to analyze market activity is on the rise. Hedge funds and other investment firms buy "bespoke data sets" that can make otherwise nonpublic information available for sale.

While the use of this information creates opportunities, it also requires firms to navigate a complex regulatory landscape. To avoid risks when using big data to guide securities transactions, firms must consider a series of issues arising both under the federal securities laws and under federal and state privacy laws.

This commentary is an introduction to these issues and offers a starting point for general counsels and chief compliance officers to consider strategies to mitigate the legal — and related headline — risks of using big data to guide securities transactions.

ADDRESSING RISKS CREATED UNDER THE FEDERAL SECURITIES LAWS

In analyzing risks under securities laws, investment firms should first ensure that their policies and procedures are designed to fit their business. Both the Securities Exchange Act of 1934 and the Investment Advisers Act of 1940 require registered firms to establish, maintain, and enforce written policies and procedures reasonably designed to prevent the misuse of material, nonpublic information by the firm or by an associated person.

In its enforcement of these provisions, the SEC has emphasized that if a firm's business creates unique risks, the policies and procedures must anticipate and specifically address those risks. For example, in a case involving the hedge fund manager Deerfield Management Co. LP, the SEC faulted Deerfield for not adequately addressing the firm's use of political intelligence.[1]

As alleged by the SEC, Deerfield conducted "extensive research in the healthcare sector" and this research included engaging consultants that provided political intelligence about impending regulatory or legislative decisions. The SEC alleged that Deerfield did not employ sufficient safeguards to ensure that the use of such political intelligence consultants did not result in the passing of inside information. The SEC found that Deerfield violated securities laws by failing to have policies tailored to controlling information obtained from political intelligence firms.

Similarly, in a case against Artis Capital Management LP, the SEC faulted Artis for not having policies that addressed the particular risk of having an analyst who relied primarily on industry sources for trading information. The SEC also alleged that Artis missed certain red flags indicating that the information supplied by analysts was based on material, nonpublic information.[2]

> When the SEC inevitably turns its attention to the use of big data for trades, it will likely take a careful look at firms' policies.

When the SEC inevitably turns its attention to the use of big data for trades, it will likely take a careful look at firms' policies. The SEC will likely examine whether firms sought to address the risks of using big data to conduct research and had effective policies to detect possible misuse of material, nonpublic information. Accordingly, firms must address current data usage, and continue to update their policies as types and sources of data change.

AVOIDING INSIDER TRADING LIABILITY

When hedge funds use data sets to plan securities transactions, they also obviously need to avoid insider trading liability. To prove insider trading, the government generally must show the use of material, nonpublic information and that the trades were based on information obtained in breach of a duty owed. Although there has not yet been an insider trading case involving big data, precedent provides a guide to how the government would attempt to build such a case.

Nonpublic information

As an initial matter, at least some big data sought out by hedge funds and other investment firms may be deemed to be nonpublic. After all, the search for an investment edge drives the development of more sophisticated proprietary tools to generate investment

insights that might not be fully appreciated by all market participants.

In determining whether information is nonpublic, courts are likely to consider the degree of penetration of the data into the market, whether the "sell-side" industry reports on the data, whether the data is the fungible equivalent of other data that is widely distributed, whether anyone can buy the data and if so, at how accessible of a price point.

Material information

The question of whether information will be material will be a separate and perhaps more difficult hurdle for the government. A recent case in the 3rd U.S. Circuit Court of Appeals provides some clues on how the government and courts will analyze whether data sets are material.

> In considering whether a data set contains material information, it is important to consider how strongly predictive a particular set likely is.

In *Securities and Exchange Commission v. Huang*, 684 F. App'x 167 (3d Cir. 2017), the SEC alleged that a former bank employee improperly used his employer's database to access confidential sales data concerning 100 consumer retail companies and used that information to trade in those companies' securities. The SEC's expert at trial conceded that the information gleaned through the bank's systems constituted, on average, less than 3% of the companies' total revenue.

To demonstrate materiality, the SEC's expert explained that the defendant used this data to create a revenue projection and then compared that projection to stock analysts' expectations. As the expert showed, the defendant, using the confidential data, was able to consistently predict whether the company would beat expectations. In fact, the SEC expert emphasized that the trader was able to earn over $1.48 million and an astronomical rate of return — over 12,929% on his initial investment.

In affirming the district court's finding of materiality, the 3rd Circuit emphasized that the "data altered the 'total' mix of information an investor would have had to make a decision." The *Huang* case illustrates how the SEC may be able to craft materiality arguments when big data proves effective at driving returns.

The *Huang* case also has three other important reminders that will likely inform a court's analysis of the materiality of a data set:

- It is no defense that the information did not come from the issuer of the traded securities. The Huang case involved a misuse of a bank's information and not the misuse of the public company's information.
- The fact that the information at issue is just a small slice of the total available information on a company will not preclude a finding of materiality. The Huang case involved an average of less than 3% of the consumer companies' total sales and was found to be material.
- The materiality analysis will not be done in a vacuum. When the court weighs materiality, it will look at how the information was used in practice and whether it created out-sized returns consistent with inside information.

In the context of big data, the question of whether data constitute material, nonpublic information involves potentially complex legal and context-dependent factual judgments. Data collection has made it possible to purchase large data sets containing information underlying one or more of a company's financial metrics, including revenue.

In considering whether a data set contains material information, it is important to consider how strongly predictive a particular set likely is. To the extent possible, it is also important to analyze the materiality of the information itself as distinguished from the deductions or inferences drawn from it by investment professionals. Firms should rely on counsel when making these judgments.

Breach of duty

To satisfy the breach element, the government generally must show that the trader knew or should have known the information was obtained in breach of a duty of confidentiality. To mitigate risk, firms can take several steps to protect themselves from liability.

> If a firm is in possession of data that is too good to be true, a firm could be at risk of liability.

First, they should ensure that their practices show that they were reasonable in vetting purchased data. Steps to take include obtaining representations from data brokers that the information was not obtained in violation of a breach of duty. The firm must also understand the origin of the information, including all the inputs.

Second, firms need to avoid situations in which the nature of the information itself suggests that it was obtained in breach of a duty due. For instance, in cases dealing with a corrupt investment banker, courts have observed that specific information about an impending acquisition usually cannot be obtained without a breach of duty. Receipt of such

information itself can be evidence that a defendant should have known of a breach.

If a firm is in possession of data that is too good to be true, or suggests by its nature that it is derived from insider sources, a firm could be at risk of liability.

The risk that hedge funds will be accused of knowing that information was obtained in breach of a duty can be mitigated by a due diligence process that thoroughly examines the provenance of data and the legal propriety of the vendors obtaining the information.

Firms should also take steps to ensure that they understand the sources of the information. Relevant questions include:

- Where was it obtained from?
- How was it obtained?
- Was there compensation paid?
- What is the vendor's compliance program in obtaining and dealing in the information?
- What do the vendor's acquisition contracts, if any, say?

And perhaps most importantly, firms should instruct their professionals that, when in doubt, they should always consult their legal and compliance departments.

PRIVACY

The second significant risk faced by hedge funds that use big data is privacy. Firms using consumer data may have obligations to the individuals whose data is being analyzed and may also face lawsuits from states or individuals for misuses of data.

The key concept for privacy regulation is personally identifiable information (PII). Generally, PII is defined as any data that can be used, alone or together with other data, to distinguish or trace an individual's identity. Depending on the source of the data, a jurisdiction's definition of PII may be more or less expansive, with differing implications for how data are to be protected.

Firms should pay close attention to the types of information they are collecting to make sure that they are aware of any PII that is part of a data set, which can trigger a wide range of obligations under federal and state law. And because the privacy space is likely to change significantly in the coming years as more states regulate consumer data, firms should pay close attention to legislative and regulatory action and adjust their practices and policies accordingly.

This commentary examines the most restrictive federal and state privacy laws: the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH Act); and the California Consumer Privacy Act of 2018 (CCPA).[3]

Federal regulation — HIPAA

HIPAA is the federal government's principal privacy regulation and governs the use of protected health information (PHI). PHI is defined as "individually identifiable health information" transmitted or maintained in electronic media or "any other form or medium."[4] With limited exceptions, PHI may only be sold to a third party if the seller of the information has received an authorization that states that the seller can sell the information.[5]

A recipient of PHI may only redisclose PHI to a third party in exchange for remuneration if "an additional authorization" is obtained, unless "it is sufficiently clear to the individual in the original authorization that the recipient [of PHI] will further disclose the individual's protected health information in exchange for remuneration."[6]

Thus, investment firms should first confirm whether data include PHI. If so, they should carefully review authorizations obtained by data brokers to ensure that the initial authorizations clearly encompass the resale of PHI or that the data broker has obtained additional authorizations in conformance with HIPAA's requirements.

If a review of authorizations seems unduly burdensome, hedge funds can avoid HIPAA regulations entirely by "de-identifying data." The regulations provide two methods of de-identification.

First, the firm can provide an expert review of health information, supported by documentation, determining that "the risk is very small that the information could be used, alone or in combination with other reasonably available information . . . to identify an individual who is a subject of the information."[7]

Second, firms can remove from the data names, contact information, and certain other identifiers listed in the regulation. De-identified information is not subject to HIPAA, so investment firms should consider requiring data brokers to de-identify information before transmitting it.

State regulation — the CCPA

The California Consumer Privacy Act, which is set to go into effect on Jan. 1, 2020, broadly defines PII to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[8] This definition is significantly broader than other state law privacy statutes.

If a hedge fund obtains PII subject to the CCPA, the fund is required to delete the PII at the request of the consumer.[9] The CCPA, as proposed, is principally enforceable by the

state attorney general, with a private right of action currently available only in cases of data breaches.[10]

Thus, failure to delete PII after a consumer has made such a request could expose firms to state enforcement actions or, in the event of a data breach, private consumer class actions.

However, a hedge fund is likely to acquire data from brokers and may not be aware that a consumer has requested deletion of his or her PII. To avoid this risk, hedge funds should include in data broker contracts a provision that requires them to pass on consumer requests to delete data so that the hedge funds can comply with this requirement.

The CCPA also requires the California Attorney General to adopt regulations further defining PII and setting rules and procedures for complying with the statute.[11] After those regulations are promulgated, investment firms will need to pay close attention to their policies and contracts with data brokers to ensure that they are complying with the new requirements. Draft regulations were published on Oct. 10, 2019.

NOTES

[1] *See* Order, Investment Advisers Act Release No. 4749 (Aug. 21, 2017) (available at https://www.sec.gov/litigation/admin/2017/ia-4749.pdf).

[2] *See* Order, Investment Advisers Act Release No. 4550 (Oct. 13, 2016) (available at https://www.sec.gov/litigation/admin/2016/ia-4550.pdf).

[3] This article addresses only the requirements under US law. It does not address the regulations of other jurisdictions or the European Union General Data Protection Regulation.

[4] *See* 45 C.F.R. § 160.103.

[5] *See* 45 C.F.R. §§ 164.502(a)(1), 164.508(a)(4).

[6] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, Dep't of Health & Hum. Servs., 78 Fed. Reg. 5,566, 5,608 (Jan. 25, 2013).

[7] 45 C.F.R. § 164.514(b).

[8] Cal. Civ. Code § 1798.140(o)(1).

[9] *See* Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, Harvard Business Review, July 11, 2018, https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

[10] *See* Cal. Civ. Code § 1798.150(a)(1).

[11] *See* Cal. Civ. Code § 1798.185.

This article first appeared in the November 21, 2019, edition of Westlaw Journal Securities Litigation & Regulation.

ABOUT THE AUTHORS



(L-R) **Charles D. Riely** is a partner in **Jenner & Block**'s Investigations, Compliance and Defense Practice in New York, and is a former assistant regional director for the Division of Enforcement for the Securities and Exchange Commission. He has worked extensively with criminal authorities in parallel investigations and has developed deep expertise in all aspects of the federal securities laws. He can be reached at criely@jenner.com. **Keisha N. Stanford**, a partner in Jenner & Block's Investigations, Compliance and Defense Practice and Government Controversies and Public Policy Litigation Practice in Washington, D.C., represents public and private multinational corporations and individuals in the areas of compliance, white collar criminal defense matters, government enforcement matters and internal investigations. She can be reached at kstanford@jenner.com. **Logan J. Gowdey** is a New York-based associate in Jenner & Block's Litigation Department and can be reached at lgowdey@jenner.com.