LATHAM & WATKINS LLP

Alternative Data

Regulatory and Ethical Issues for Financial Services Firms to Consider

March 2020

Contents

Introduction

Not too long ago, an investment manager looking to invest in a company might conduct due diligence, attend investor relation calls, peruse quarterly or annual filings, and consider standard ratios such as price to earnings and debt to equity. Today, such an investment manager might supplement this fundamental analysis with data analytics on a range of topics; for example, the company's supply chains, shipping routes, consumer credit card transactions, social media mentions, and employment trends, to forecast earnings, growth prospects, and long/short opportunities (such information typically referred to as "alternative data").

Today's computerized and mobile world generates countless gigabytes of data every second, and those seeking an informational advantage in the markets have taken notice. Data sources can be mined for insights not apparent to other market participants. Regulators have taken notice as well, because the use and possible informational advantage of such alternative data sources and "dark analytics" raises some very thorny questions regarding propriety, privacy, fairness, and ethics.

Traditional data used by investment managers and other investors (such as regulatory filings, press releases, and management commentary) are produced directly by the company itself. While traditional sources of data may contain inside information and must be treated appropriately before they are made public, the nature of alternative data is less clear-cut. Alternative data does not come from the company itself, and may be derived (or be extrapolated) from a number of non-traditional sources. Alternative data sets can be compiled from sources as wide-ranging as credit and debit transactions, public records, web traffic, web searches, social media posts, online discussion board postings, product reviews, sentiment analysis, crowdsourcing platforms, news feeds, email metadata, biometric data, mobile device tracking, satellite imagery, geo-spatial information, supply chain and logistics data, sensors, job listings, flight trajectories and statistics, and weather data.

Such data is readily available from hundreds of vendors both in its raw and/or aggregated and processed forms. Firms looking to capitalize on — and information providers looking to supply — alternative data for tradable insights should be aware of the regulatory environment within which they are operating, as well as the attendant risks.

Financial Services Regulation Implications — EU

In the EU, the key financial services measures likely to be relevant to the use of alternative data are the Market Abuse Regulation (MAR) and the Markets in Financial Instruments Directive (MiFID).

MAR

MAR is potentially relevant to investment research produced anywhere in the world because its geographical reach is determined by where an instrument can trade, rather than the issuer's country of incorporation or an analyst's location. MAR applies (in summary) to financial instruments admitted to trading on a European Regulated Market, Multilateral Trading Facility, or

Organised Trading Facility, and to instruments whose price or value depends on or has an effect on the price or value of an instrument listed above. Issuers have no control over whether or not their instruments might be traded on (for example) a Multilateral Trading Facility. Indeed, searches of the EU's Financial Instrument Reference Database System (FIRDS) frequently produce numerous hits for companies with little connection to the EU. As part of its Brexit withdrawal process, the UK has also announced plans to keep a separate UK FIRDS register.

MAR prohibits insider dealing. A person is "inside" when they have inside information. This is information relating to a MAR instrument that is precise, likely to have a significant impact on price, and has not been made public. MAR does clarify that information is "public" if it is obtained by observation. (The UK Financial Conduct Authority (FCA) has previously given the example of a person who realizes a factory is on fire; this is public information even if it has not yet been reported because it has been obtained by observation.) Information is also public even if it can only be observed, or interpreted, by those with above average financial resources, expertise, competence, or luck.

Therefore, it is possible that alternative data sources could be public even if they could not readily be found out by members of the public. An investment bank which, for example, was prepared to buy expensive data from a number of vendors and then uses a clever proprietary method of combining the data into a valuable new source, which only the bank knew, would nonetheless be handling public information for the purposes of MAR. Information, therefore, is not inside information under MAR even if sophisticated analytical skills are required to reach a meaningful interpretation.

The extent to which this example can be taken must have limits. MAR itself contains one: if the announcement of information is (or becomes) routinely expected by the market, and contributes to price formation, then knowledge about this information prior to its publication will be inside. This provision is likely to affect a small number of closely followed data sources, which are also likely to be in scope of measures such as the EU Benchmarks Regulation.

Another way in which this example could result in the production of non-public data would be if the bank involved prevented the third-party vendors from selling the data to any other party that was willing to pay the same rates for it. If all of the information sources were exclusive, and could not be replicated by anyone else, then arguably the contractual restriction could produce the exclusivity that would result in the production of non-public information.

The FCA published an article in January 2020 called "Turning Data Inside Out" that addressed whether it was fair that an information asymmetry might exist in the market. The article suggested that market participants and regulators may have differences of opinion over what is, and is not, an unfair advantage, with the FCA suggesting a debate should follow. (For an in-depth look at this piece, see Latham's prior coverage: "Regulator Raises Concerns Over Alternative Data.")

MiFID

MiFID sets out a number of rules that apply to the production of investment research, and the management of conflicts of interest, generally. Notably, MiFID's geographical scope significantly differs from that of MAR's. MiFID applies only to EU-regulated investment vehicles (with a number of limited exceptions, which are not relevant to the production of investment research). Therefore, MiFID will only impinge on the use of sources of alternative data by EU-regulated investment firms.

First, MiFID contains a definition of research in which it clarifies that research must:

- Concern a financial instrument
- Explicitly or implicitly recommend or suggest an investment strategy
- Be intended for distribution channels or for the public
- Most importantly, provide a substantiated opinion as to the present or future value or price of an instrument, or contain analysis and original insights and reach conclusions based on new or existing information that could be used to inform an investment strategy

This last requirement suggests that, to be investment research, the analysis must have sufficient depth (the "substantiation" of the opinion), covering the financial instrument in a rounded rather than narrow way.

Therefore, alternative data that is not relevant to one or several financial instruments (because, for example, it only enables broader macroeconomic trends to be understood) would not be investment research for the purposes of MiFID. Further, even information that did relate to particular financial instruments, but provided merely limited statistics rather than substantiated opinions, would not amount to research.

If the use of alternative data does amount to the production of research, a number of consequences apply. MiFID contains detailed presentation and disclosure requirements. Distribution tends to be limited (i.e., not to retail). Conflicts of interest management requirements apply that are specific to the research industry. Finally, inducements rules apply. These rules could require consumers to be obliged to pay for the research, or (in some circumstances) to have concluded that the information does not amount to investment research, and is a minor non-monetary benefit within the meaning of MiFID.

Confusingly, MAR also contains a similar (but broader) provision relating to investment recommendations. An investment recommendation is information explicitly or implicitly suggesting an investment strategy, relating to a financial instrument, which is intended for distribution channels or the public. An investment recommendation does not require the same degree of substantiation (other than being capable of substantiation) as investment research. Therefore, an off-the-cuff comment, or a more limited piece of analysis, which might not amount to research, would nonetheless be an investment recommendation if it suggested an investment strategy.

Investment recommendations also have presentation and disclosure requirements, and firms that disseminate investment recommendations have additional obligations requiring them to, for instance, track the changes and recommendations given over periods of time. These requirements are generally well-known in the context of sales notes issued by EU investment firms.

MiFID also contains two other potentially relevant points:

- MiFID contains rules relating to marketing communications, and publications containing alternative data sources would need to be considered in light of these rules. In the UK, additional requirements apply to a UK-only concept, the financial promotion.
- MiFID contains rules relating to personal recommendations. Whilst it is unlikely that broadly distributed content would amount to a personal recommendation, client-specific use of alternative data sources could possibly amount to a personal recommendation in the context of MiFID.

Financial Services Regulation Implications — US

In the US, some of the key federal laws affecting the use of alternative data include the Investment Advisers Act of 1940 (Advisers Act) and the Securities Exchange Act of 1934 (Exchange Act). Although these laws, and their associated rules and regulations, do not address the use of alternative data on their face, they do contain provisions that have important implications for providers of alternative data.

Advisers Act

Providers of alternative data or data sources need to be aware of the possibility that their activities may cross over the line into the provision of investment advice, which could subject them to the regulatory requirements of the Advisers Act.

Under Section 202(a)(11) of the Advisers Act, an "investment adviser" is "any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities."[1] Accordingly, a person's status as an investment adviser for purposes of regulation under the Advisers Act depends on a three-prong analysis as to whether that person:

- Provides advice or issues reports or analyses to others regarding securities
- Is in the business of providing such services
- Provides such services for compensation

The first prong of the analysis is often pivotal, as the second two prongs will typically collapse into a determination of whether the provider of investment research or data sources receives regular compensation for such services from its customers.

Furthermore, the staff of the US Securities and Exchange Commission (SEC) takes an expansive view of what constitutes advice, analyses, or reports concerning securities.[2] For example, advice concerning the relative advantages and disadvantages of investing in securities as compared to other investments, advice with respect to securities either generally or specifically, or advice with respect to how to allocate assets to different categories of investments (including securities) would each constitute investment advice.[3] In addition, a person providing advice regarding whether or not to retain an investment adviser in the first instance would also be considered to be in the business of giving investment advice, as would a person providing a market timing service or otherwise offering market timing advice.[4]

The SEC staff generally takes the position that presenting securities data or information does not constitute furnishing investment advice or an analysis or report if:

- The information is readily available to the public in its raw state.
- The categories of information presented are not highly selective.
- The information is not organized or presented in a manner that suggests the purchase, holding, or sale of any security or securities.[5]

Providers of investment research or data sources need to consider all these conditions when they present alternative data sources for compensation. While they have the ability to control how the information is presented to their customers in order to satisfy the second two conditions, the first condition may often pose a problem. Indeed, one of the perceived benefits of certain alternative data sources for investors is that the information is not already known widely by the public. Nonetheless, so long as the information is available to the public in its raw state, and the provider is merely gathering or aggregating such information for its customers, and not presenting the data in such a way as to preference a particular security or investment opportunity over another, the provider may be able to satisfy this condition as well.

Exchange Act

Section 15(a)(1) of the Exchange Act generally makes it unlawful for a "broker" to make use of U.S. jurisdictional means to effect transactions in, or to induce or attempt to induce the purchase or sale of, any security unless such broker is registered with the SEC. SEC-registered brokers are also generally required to become members of the Financial Industry Regulatory Authority, Inc. (FINRA). Section 3(a)(4) of the Exchange Act, in general, defines a "broker" as "any person engaged in the business of effecting transactions in securities for the account of others." Based on no-action guidance from the SEC staff, activities that may be deemed (alone or in combination) to confer "broker" status include:

- soliciting clients to enter into securities transactions[6]
- assisting issuers in structuring prospective securities transactions or helping issuers to identify potential purchasers of securities
- participating in the order-taking or order-routing process or otherwise bringing buyers and sellers of securities together
- receipt of compensation that is contingent on the success of a securities transaction or that is based on the amount, size or value of a securities transaction (typically referred to as "transaction-based compensation")

Accordingly, a person providing certain types of information or analysis with respect to securities transactions and/or receiving transaction-based compensation for securities-related services could be deemed to be acting as a "broker" and thereby subject to registration and regulation under the Exchange Act.

FINRA members are additionally subject to specific content, approval, disclosure and other requirements with respect to general written communications with external parties, as well as in connection with the provision of information that falls within FINRA's definition of "research report".[7] Note in particular, with respect to equity securities, FINRA Rule 2241(a)(11) defines a "research report" to include (subject to a number of important exceptions) "any written (including electronic) communication that includes an analysis of equity securities of individual companies or industries . . . and that provides information reasonably sufficient upon which to base an investment decision."

Thus, a provider of alternative data services that wishes to avoid characterization and regulation as a broker under the Exchange Act (with attendant obligations as a FINRA member) should – in addition to not engaging in the other activities noted above – take particular care not to base its fees for such services on the amount, value, size or successful consummation of a securities transaction.

Data Privacy

Alternative data may allow those with access to know information about a company or consumers that others in the market do not know. This may be the case, even if the pool of structured/unstructured data used by the investor or analytics engine was harvested on the open web and ostensibly in the public domain. A key concern, however, is that personal data is often the source, or essential component of, alternative data. Use and abuse of personal data (also known as personal information or personally identifiable information), or data that in aggregate can be used to piece together an individual's identity, has become a lightning rod for regulators and in the wider public discourse. To the extent that alternative data sources contain personal data, data protection and privacy laws will likely be applicable.

Data Privacy Implications — EU

GDPR

Data privacy legislation, on an almost globally consistent scale, demands fair, accurate, and non-discriminatory use of personal data. Nowhere is this more evident than in the EU, where the General Data Protection Regulation (GDPR) puts individuals at the heart of its rules, requiring — in respect of all data processing — enforceable data subject rights and effective remedies for data subjects.

The EU's GDPR came into force in May 2018, and made a host of enhancements to the EU data protection regime. GDPR gives individuals far more control over their personal data, requires data controllers to be more transparent about how they use data, and has substantially increased the level of fines that may be imposed for non-compliance.

GDPR notably has extraterritorial scope, and, in addition to applying to data collected in the context of an EU establishment of a controller or processor, may also apply to non-EU entities processing personal data of EU data subjects collected pursuant to specific criteria. The territorial application of GDPR does not turn on citizenship or nationality of the data subjects (a common misconception).

In the EU, data is "personal data" if it is "reasonably likely" that the data can be used to identify a living individual. The collation of multiple data points (in the form of "big data") can often increase the risk of individual identification. Mechanisms for anonymizing data are subject to considerable debate — historic (pre-GDPR) guidance exists in this field, but there is nothing current from the regulators on this topic. There are general concerns that technology is moving so quickly in this space that data that is effectively anonymized today could be re-identified tomorrow. Machine learning and artificial intelligence (AI) give rise to considerable concerns.

GDPR assumes that data flows will be relatively straight-forward — the legislation was not drafted with new technologies such as AI, blockchain, or big data in mind. It assumes that there will be:

- A "data controller" determining the means and basis for processing of the data
- "Data processors" who act on behalf of, and subject to the instructions of, the data controller
- A "data subject" who will have a relationship (either contractual or otherwise) with the data controller and, accordingly, is aware of, or can be made aware of, the processing of their data

Transparency and data minimization are critical principles of GDPR. The transparency principle requires that any information addressed to the public or to the data subject be concise, easily accessible, and easy to understand, and in clear and plain language. The data minimization principle says that when personal data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose. It is therefore key that data subjects are informed of the use of their data and data is only used as anticipated by data subjects and for the purposes collected. This means that if organizations are using personal data in the context of big data, then as part of assessing fairness they need to be aware of and factor in the effects of their processing on the data subjects concerned. Given the sometimes novel and unexpected ways in which alternative data is used in analytics, this may be less straightforward than in more conventional data-processing scenarios.

In many cases, the users of alternative data sources will not have any relationship with the data subject and will not be in a position to ensure that the transparency, fairness, or minimization principles as set forth in the GDPR are met. However, this scenario does not mitigate the risk for that investment manager. Depending on the use of the relevant data points, the investment manager may be deemed to be a data controller of such data even though they have not collected it directly. Detailed diligence is required, up-front, to assess the categories of data collected, the purpose for which it was collected, how it will be used, and how it will be aggregated. Notably, personal data subject to pseudonymisation techniques (i.e., processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information) must still be treated as personal data for the purposes of GDPR; while pseudonymisation can help reduce the risks associated with the processing of personal data, it is only a security measure and does not change the status of the data. GDPR does not, however, apply to anonymized data and, therefore (subject to the considerations above) anonymization is encouraged if possible. If personal data is being anonymized by the vendor, appropriate contractual protections must be sought.

Infringements of GDPR carry significant financial consequences. Regulators can impose fines up to €20 million or 4% of an undertaking's global revenue. Data hygiene (such as pseudonymisation and ideally anonymization) and good governance (such as robust policies and procedures for data operations) are therefore critical to the use of alternative data, not only for the purpose of mitigating regulatory risk, but also for alleviating potential reputational risk.

Data Privacy Implications — US

There are various US federal laws that address privacy issues relevant to the financial services sector, most notably the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). The Federal Trade Commission (FTC) has enforcement authority in relation to both the GLBA and the FCRA and also uses its general power to enforce the prohibition against unfair or deceptive commercial practices in Section 5 of the FTC Act to enforce consumer privacy and security, such as promises made in privacy policies.

Regulation S-P

Regulation S-P ("Privacy of Consumer Financial Information and Safeguarding Personal Information") is the rule adopted by the SEC to implement the privacy rules promulgated under Section 504 of the GLBA. Regulation S-P mandates customer data safeguards and privacy notices for investment advisers, broker-dealers, and investment companies. Under Regulation S-P, firms are required to protect customers' nonpublic personal information and financial records from unauthorized access or use. Firms must have written policies describing the data safeguards they have in place, and procedures appropriate to their size, complexity, business activities,

and risk profile. The rule also requires firms to provide customers with "clear and conspicuous" privacy notices and disclosures (upon customer relationship initiation and annually thereafter during the continuation of the customer relationship) describing the firm's privacy protection and information-sharing policies. Customers must also be informed of their rights concerning their personal information, such as the right to opt out of having their personal information disclosed to nonaffiliated third parties.

California Consumer Privacy Act (CCPA)

US state laws also exist (and are being developed), but at present, are not as comprehensive as the GDPR. The most notable state legislation concerning privacy is the CCPA. The CCPA, which was enacted in 2018 and effective on January 1, 2020, "creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses."[8] The CCPA applies to any business that meets the below thresholds and handles the personal information of California residents, regardless of location. Therefore, the CCPA promises to have a major impact on the privacy landscape not only in California but also in the rest of the US and around the world.

The CCPA applies to a business (meaning a legal entity organised or operated for the profit or financial benefit of its owners) that:

- Is doing business in California
- Is collecting personal information about consumers
- Is determining the means of processing
- Either:
    - Has annual gross revenues of more than US$25 million
    - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of US$50,000 or more consumers, households, or devices
    - Derives 50% or more of its annual revenues from selling consumer's personal information

Under the CCPA:

- Personal information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
- Consumer means a natural person who is a California resident
- Sell, selling, sale, or sold means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration

The CCPA requires businesses subject to the CCPA to meet a range of individual rights including:

- The right to know what personal information has been collected, used, shared or sold about them
- The right to request that their personal information be deleted
- The right to opt out of the sale of their personal information by the business to third parties

In addition, businesses are prohibited from discriminating against California residents based on their exercise of these rights.

Like the GDPR, the CCPA also requires transparent policies and processes. Therefore, many of the GDPR challenges outlined above also apply when trying to reconcile big data with the CCPA. For example, businesses subject to the CCPA are required to provide notice to California residents at or before data collection and must respond within specific timeframes to requests from individuals in relation to the above rights.

In addition, the CCPA includes a number of exceptions, some generic and some specific to existing US privacy laws, including certain laws applicable in the financial services sector. The relevant generic exceptions (both of which are currently set to expire on January 1, 2021) are as follows:

- Personal information collected about personnel (including employees, job applicants, and contractors) in the course of employment is excluded from the CCPA, except for the obligation to provide notice.
- Personal information collected in the course of certain business-to-business (B2B) communications or transactions is excluded from the CCPA, except for the obligations relating to the sale of personal information.

The primary exceptions most specific to the financial services sector are:

- Personal information that is collected, processed, sold, or disclosed pursuant to the GLBA (see above) or the California Financial Information Privacy Act (FIPA)
- Personal information that is reported in or used to generate a consumer credit reports to the extent that the information is subject to the FCRA (see above)

The private right of action (see below) applies in all cases (notwithstanding the above exceptions).

Both categories of exceptions are potentially helpful to firms. However, because firms typically handle some personal information caught by the existing US laws; some caught by the generic exceptions; and the remainder not caught by either (and therefore subject to the CCPA), the exceptions also create a layer of complexity.

Fines under the CCPA may amount to US$2,500 for each violation or US$7,500 for an intentional violation, enforced by the California Attorney General. In relation to certain security breaches there is a private right of action for individuals which, significantly, opens the doors to potential class actions.

Other Important Considerations

Terms of Use Risk. Alternative data that is obtained from web-scraping services or proprietary algorithms may run afoul of the terms and conditions of the websites from which the data originates, as well as governing copyright and intellectual property laws. The originating site owner may strictly prohibit either the use of the data itself, or the sale of the data to third parties. Therefore, users of alternative data should understand the provenance of the data and the underlying terms and conditions that govern its use and sale.

MNPI Risk. It goes without saying that the use of material non-public information (MNPI) for trading purposes, whether defined narrowly or broadly, is restricted in nearly every jurisdiction. Users of alternative data must ensure that the vendors they subscribe to have strong governance policies and procedures in place for data access and hygiene, so that algorithms or web-scraping bots do not inappropriately obtain data that may in fact not be public. Effective due diligence on third party data providers and data sets is essential to avoid insider-trading violations and enforcement actions by market regulators.

Ethical Risk. As market participants search for new sources of return on investment, innovative use of data will proliferate. But innovation not guided by a moral compass may unintentionally stray into misuse. The financial and reputational risks are too high, in what is to some degree a politicised area, to simply wait for clear regulatory guidance on alternative data use. Proactive behavioural frameworks — underpinned by policies, procedures, due diligence, and customer disclosures, and coupled with unambiguous accountability — are critical to investment management operations in a world where consumers are increasingly focused not simply on the what, but just as importantly, on the *how* and the *why*.

Regulatory Focus on Alternative Data, Big Data and Data Ethics

Global regulators are recognizing the increasing availability of alternative data and big data usage and are beginning to focus more intently on the attendant risks. The FCA, in its 2018/2019 Business Plan, highlighted the opportunities and risks inherent in big data, and announced that it would look to review the use and analysis of big data by financial services firms. The FCA launched a Call for Input on the use of data in wholesale markets in March 2020, seeking to explore how innovations in data are generated and used, the value offered to market participants, and whether data are being competitively sold and priced. This will help the FCA to assess any implications for competition and market integrity in wholesale financial markets. Due to the "pace,

scale and potentially wide-ranging impacts of data-related innovation," the FCA will monitor and address emerging data risks such as barriers to access, informational asymmetry, biased data and analysis, concentration, and exploitation of market power, collusion, and other forms of market abuse. The FCA has also stated that, in order to promote transparency and accountability, and mitigate potential harms, it will explore the need for official policy frameworks for how firms collect and use data.

The SEC has also shown increasing interest in privacy matters in the past few years. The SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert on April 16, 2019, covering examination findings related to Regulation S-P. OCIE found that many broker-dealers and investment advisers lacked sufficient policies and procedures to ensure the security and confidentiality of nonpublic customer records and information, failed to provide customers with required privacy or opt-out notices, or failed to enforce their policies and procedures on personal data security with nonaffiliated third parties. While Regulation S-P defines a "customer" as a consumer who has a "customer relationship" with a financial institution,[9] financial institution users of alternative data and big data should understand the source and breadth of data they are accessing, compiling and storing. If the data includes customers' personal data — either intentionally or unintentionally — then the safeguard and notice rules apply.

In OCIE's 2020 Examination Priorities discussion of key market risks, the agency for the first time highlighted alternative data usage by registered financial service firms as an emergent area for ongoing scrutiny. OCIE noted that "examinations will focus on firms' use of these data sets and technologies to interact with and provide services to investors, firms, and other service providers and assess the effectiveness of related compliance and control functions." OCIE will likely be assessing alternative data use by broker-dealers, investment advisers, and investment management firms for personal data compromise, misuse of material non-public information, conflicts of interest, and data vendor management.

The data privacy regulators also recognize the need for ethics to play an integral part in the balancing of individuals' rights regarding their data and the advancement in technology and innovative use of data. In November 2019, the UK's Information Commissioner's Office (ICO) appointed its first Data Ethics Adviser, who is tasked with ensuring that the ICO contributes to the data ethics discussion in a way that upholds data subjects' rights in the UK. Other regulators are expected to follow this approach. Notably, the data regulators do not consider it their role to "enforce" data ethics (which is, by its nature, a subjective concept), but, rather, to ensure that the use of data and the application of data protection laws are continually challenged by ethical debate.

Federal lawmakers in the US are also actively pursuing more comprehensive data privacy legislation, with recent overlapping proposals such as the Data Protection Act of 2020, that would establish a "Data Protection Agency" responsible for enforcing US data privacy laws; the Consumer Online Privacy Rights Act, that would allow consumers to view and control the distribution of their personal data; and the Online Privacy Act of 2019, that would establish a "Digital Privacy Agency," create user rights and company obligations, and strengthen enforcement for non-compliance. The collection, dissemination, and use of alternative data and big data, especially when inclusive of nonpublic personal data, is likely to be impacted if any one of these bills is enacted.

Conclusion

At this stage, global regulators do not have a unified or settled view on how to approach the various issues surrounding the collection and use of alternative data or big data. While a standardized approach is unlikely, burgeoning focus by regulators worldwide on personal data use and abuse indicates heightened concern for the potential market risks and ethical concerns. The industry for alternative data and big data will only continue to grow in tandem with demand for tradable insights that complex and expanding data sets can provide. Financial services firms that use or source such data for provision to others should implement strong governance frameworks and best practices if they wish to safely navigate the regulatory (and ethical) minefield.

Endnotes

1. 15 U.S.C. § 80b-2(a)(11).

2. As a threshold matter, the SEC staff take the position that the term "security" should be read broadly for the purposes of both the Advisers Act and the Investment Company Act of 1940 (the 1940 Act) — even more broadly than the definition of the term "security" in the Securities Act of 1933 (the Securities Act) and the Exchange Act. *See, e.g.*, Harrell Int'l Inc., SEC No-Action Letter (avail. May 24, 1989) (a commercial note was a security for purposes of the 1940 Act even if it was not a security for purposes of either the Securities Act or the Exchange Act).

3. *See, e.g.*, Financial Strategies, Inc., SEC No-Action Letter (avail. Feb. 14, 1994); Thomas Beard, SEC No-Action Letter (avail. May 8, 1975).

4. *See, e.g., SEC v. Washington Investment Network*, 475 F. 3d 392 (D.C. Cir. 2007) (person advising clients on selection of managers in a wrap fee program is within the statutory definition of "investment adviser"); David Parkinson, PhD, SEC No-Action Letter (avail. Oct. 19, 1995) (provider of bond market timing device is within the statutory definition of "investment adviser"); Charles L. Simpson, SEC No-Action Letter (avail. July 7, 1992) (operator of a stock-market timing service disseminating information consisting of short-term buy and sell signals via telephone twice daily is within the statutory definition of "investment adviser").

5. *See, e.g., Datastream Int'l., Inc.,* SEC No-Action Letter (avail. Mar. 15, 1993); *EJV Partners, L.P.*, SEC No-Action Letter (available Dec. 7, 1992).

6. The SEC generally views "solicitation" very broadly for this purpose *See, e.g.*, Rule 15a-6 Adopting Release at 54 FR 30021.

7. *See* FINRA Rules 2210, 2241 and 2242.

8. *See* https://oag.ca.gov/privacy/ccpa.

9. A "customer relationship" is further defined as "a continuing relationship between a consumer and a broker-dealer, fund, or registered adviser under which the institution provides a financial product or service that is to be used by the consumer primarily for personal, family, or household purposes." *See*, https://www.sec.gov/rules/final/34-42974.htm.

Contacts

Financial Regulatory

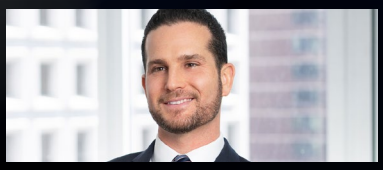
Dana Fleischman
Partner
T +1.212.906.1220
E dana.fleischman@lw.com

Fiona M. Maclean
Partner
T +44.20.7710.1822
E fiona.maclean@lw.com

Rob Moulton
Partner
T +44.20.7710.4523
E rob.moulton@lw.com

Robert Blamires
Counsel
T +1.415.395.8142
E robert.blamires@lw.com

Laura N. Ferrell
Counsel
T +1.312.876.7616
E laura.ferrell@lw.com



Deric Behar
Knowledge Management Lawyer
T +1.212.906.4534
E deric.behar@lw.com

Charlotte Collins
Knowledge Management Lawyer
T +44.20.7710.1804
E charlotte.collins@lw.com