Proskauer

# WSJ Article on Geolocation Data Highlights Risks for Fund Managers

**The Capital Commitment Blog** on **November 6, 2018**

On Friday, the WSJ published an article detailing how companies are monetizing smartphone location data by selling it to hedge fund clients. The data vendor featured in the WSJ article obtains geolocation data from about 1,000 apps that fund managers use to predict trends involving public companies. However, as we've noted, the use of alternative data collection for investment research purposes may give rise to a host of potential issues under relevant laws.

Alternative data sets may conceivably contain material nonpublic information (MNPI), or information that, when aggregated, could be considered MNPI. Trading while in possession of such information might lead to liability under the securities laws if confidential information has been "misappropriated" in breach of a duty owed to the source of the information. If data has been collected in a manner considered "deceptive," then there is a risk that trading on that information may be considered part of a fraudulent scheme in violation of the anti-fraud provisions under the securities laws.

Fund managers who use such data need to be careful. One concern is whether vendors have obtained appropriate consents to both the usage and sharing of the information. Many smartphone users may not be aware that their phone is sharing location data. Another concern is heightened risk of the data containing personally identifiable information (PII) or information which can readily be linked to PII. The vendor highlighted in the WSJ article apparently scrubs location data of personally identifiable information, and most data collectors de-identify or anonymize data that comes from sources that contain PII. Fund managers who purchase scrubbed data from third parties should check to ensure the information they receive is appropriately de-identified or anonymized and, if not, take steps to remove all identifying information.

Fund managers should also be aware of a host of other potential concerns involving collection and use of alternative data. For example, the Computer Fraud and Abuse Act (CFAA) prohibits access to information from a computer, website, server or database that is without authorization or in a way that exceeds authorized access. The Electronic Communications Privacy Act prohibits the collection or use of communications collected in violation of the Act. Other potential concerns involve claims as varied as copyright to breach of contract.

When using alternative data sets, due diligence and appropriate representations are required in order to minimize risk.

View Original

**Related Professionals**

- **Jeffrey D. Neuburger**
  Partner
- **Joshua M. Newville**
  Partner