Entities that collect data from websites through an automated device, including but not limited to “scraping,” “harvesting,” and “crawling” (such entities, “**Data Collectors**”), should be mindful of enhanced scrutiny where the Data Collector may be using the data with the purpose to compete with the website that is the object of such data collection (entities operating the underlying websites being scraped, harvested or crawled, “**Operating Companies**”). In particular, situations that could warrant enhanced scrutiny include if the data collection is done in a manner that interferes with the Operating Company's ability to offer its products or services or is harmful to the site, or if the Data Collector obtains information in breach of a copyright or other IP rights of the Operating Company.

As a general matter, investment industry firms collecting or using alternative data are not using data collected through automated means to compete with Operating Companies. Rather, they are typically using the data to derive insights to better inform investment decision-making.

Data Collectors using data collected through automated means to compete with Operating Companies should consider that there may be an enhanced risk that such collection and use is objectionable to the Operating Company and may additionally be deemed:

* Copyright infringement (*See* Web Data Collection Copyright Considerations v1.0),
* Misappropriation of trade secrets, and/or
* More generally unjust enrichment or misappropriation.

While the legal theories put forward by Operating Companies in web data collection cases may not require establishment of competitive uses, the majority of U.S. cases relating to web scraping involve firms scraping or harvesting data from websites of competitors or potential competitors. Claims such as copyright infringement or misappropriation of trade secrets or similar claims are often fact-specific and not readily dismissed. These risks are heightened where the Data Collector is collecting substantial amounts of website content to compete against the Operating Company (as oppose to limiting scraping activity to gathering public facts, such as pricing information) and where the collected data is republished or otherwise made public.

To avoid the enhanced scrutiny and litigation risks, some Data Collectors adopt a policy of not scraping sites for purposes of competing with the Operating Company or seek to obtain the consent of the Operating Company in advance of scraping.

In circumstances where a Data Collector scrapes sites that compete with it or its affiliates or sells data products incorporating data scraped from a competing Operating Company’s website, the following can help to mitigate the risks associated with such collection of web data:

* Have a full understanding of the use case for the scraping activity, and carefully evaluate any potentially competitive uses;
* Limit the scraping activity to the collection of facts and information on the public portions of websites;
* Avoid scraping activity that would interfere with the activity of other visitors or consumers on the site, e.g. removing merchandise from available inventory for consumers or purchasers if there is no intent to complete the purchase of such merchandise;
* Avoid use or republication of the data that could breach copyright or other IP rights; and
* Secure the scraped data.

The considerations identified here are in addition to, and should be read together with, those identified in other Web Data Considerations guides published by the FISD Web Data Collection Group (e.g., Web Data Collection Volume Considerations, Web Data Collection Proxy Considerations, Web Data Collection Terms of Service Considerations, etc.).