While some website operators may utilize CAPTCHAs to prevent the automated collection of information, the FISD Alternative Data Council is unaware of any case law that classifies CAPTCHAs as a denial of authorization under the Computer Fraud and Abuse Act (CFAA)[[1]](#footnote-1). To the contrary, CAPTCHAs are designed to be easy to comprehend and solve and may be utilized for a variety of other purposes, e.g., impose hit rate “speed bumps”, train image or text recognition software, create competition amongst data collectors. While there have not historically been any generally accepted principles concerning CAPTCHAs, the FISD Alternative Data Council recommends that Data Collectors seek to follow the guidelines discussed below, unless circumstances merit otherwise.

**Given that CAPTCHAs do not normally render information inaccessible to the general public, it may be permissible to solve CAPTCHAs in some cases.** If a Data Collector has reason to know that the CAPTCHA is intended to restrict the automated collection of information, the Data Collector should consider not bypassing or solving the CAPTCHA.

In cases in which a Data Collector decides to solve a CAPTCHA, it is important that the Data Collector does so in conjunction with the other FISD Web Data Collection Considerations below:

* Seek to ensure that the amount and rate of requests to websites do not cause an adverse impact on those websites. *See* Web Data Collection Volume Considerations v1.0.
* If using proxy servers, seek to ensure that website operators are provided with sufficient information that would allow them to contact Data Collectors, either directly or through third parties operating at the direction of the Data Collectors. *See* Web Data Collection Proxy Considerations v1.0.
* If the CAPTCHA presents Data Collectors with any Terms of Service Agreements (“*TOS*”) that include restrictive language regarding the automated collection of information, consider whether the TOS requires Data Collectors to take any affirmative action that may evidence constructive notice and contractual acceptance. *See* Web Data Collection Terms of Service Considerations v 1.0.
* Seek to ensure that only factual information is collected. *See* Web Data Collection Copyright Considerations v1.0.
* Seek to avoid the collection of personally identifiable information to the extent possible and otherwise seek to comply with applicable privacy regulations. *See* Web Data Collection Privacy Considerations v1.0.
* Do not collect information from a website with the intent to directly compete with the core business of the website operator.
* *See* Web Data Collection Competition Considerations v1.0.

After the Data Collector has taken the foregoing actions, it may avoid being presented with the CAPTCHA, in which case, the Data Collector may proceed with its normal activities. If the foregoing actions are taken and the Data Collector continues to encounter the CAPTCHA, provided that the Data Collector has no reasonable basis to know that the purpose of a particular CAPTCHA is to prevent automated collection of information or render the information inaccessible to the general public, the Data Collector may choose to solve the CAPTCHA. If a Data Collector has reason to know that the CAPTCHA is intended to restrict the automated collection of information, the Data Collector should consider not solving the CAPTCHA. It should be noted that the decision to bypass or solve a CAPTCHA is a fact-specific inquiry that should not be taken lightly and is not risk-free. Data Collectors should consider memorializing their review of any such activity.

1. 18 U.S. Code § 1030 [↑](#footnote-ref-1)