12 Tips for Web Scraping Compliance

There is no federal law of web scraping. To understand the law, we must see how courts have interpreted other laws to learn what is and what is not permitted.

Here are some tips on how to comply with the current law of web scraping

1 It Is Usually Ok to Access Data That is Not Protected by an Access/Authentication Barrier

In 2019, a federal court said that the main law applied to web scraping does not prohibit the scraping of publicly available data, unless the data is blocked from the public by an access-restriction barrier.

[W]hen a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA." hiQ Labs, Inc. v. LinkedInCorp.

2 Copyrighted data should not be scraped except for limited circumstances that are deemed by courts to be "fair use."

Words, phrases, logos, and other intellectual property is often protected by laws that provide exclusivity to the owner in using them

3 Trademarks

Web scrapers should not misuse or misappropriate the trademarks or other intellectual property of the scraped website.

4 Don't Breach a Contract

Many websites have binding terms of use that prohibit web scraping or use of their data.

Not all terms of use agreements are enforceable in all jurisdictions

Acquiring data under false pretenses (such as through a fake email or through a third party) increases your risk

5 Trade Secrets

Depending on how the data is acquired and the extent of material re-used and repurposed by a web scraper, some scraping may be considered theft or misappropriation of trade secrets.

6 Don't Burden, Bog Down, or Damage a Website

Some web scraping activities involve so many queries or requests that they slow down the servers or damage the scraped web site. This could lead to multiple state-law legal claims

7 Don't "Free Ride" or Usurp Someone Else's Business Model

If someone spends time and money to develop a business model and you, through scraping, take away or profit from that effort in a way that courts deem unfair, this may be "unjust enrichment."

8 Don't Collect or Take Personal Data Without Permission

Web scrapers rarely have any relationship with users of web sites, which means they must take extreme caution not to collect and use personal information without authorization or permission.

The clear trend in privacy law is toward greater restrictions and more severe punishments for privacy violations

9 Don't Interfere with Someone Else's Business Relationships or Contracts

If your web scraping activities interfere with a business's contracts or business prospects, you could be liable for the damages caused by the interference.

There are any number of novel illegal activities that, when coupled with web scraping, could create legal liability. This isn't meant to be a perfect or airtight checklist.

Written by **Kieran McCarthy**, Partner at McCarthy Garber Law, LLC

10 Don't Collect Data and Use It to Spam People

Web scrapers almost never have permission to use data from scraping activity to send emails for sales purposes. This is almost always a bad idea that can create significant liability.

11 Don't Scrape Biometric Data

This issue is still working its way through the courts, but based on what we have seen to date, collecting biometric data is a recipe for becoming the subject of a class-action lawsuit.

12 Use Common Sense

There are at least seventeen different laws that have been litigated in web scraping cases. No simple checklist can shield you from liability. Use your intuitions--if something seems borderline or sketchy to you, it might seem that way to a judge or jury as well.

* ask If in Doubt, Seek Professional Guidance

Web scraping jurisprudence is a complex and evolving area of law. Working with a professional to assess the wellness and propriety of your business practices will always be cheaper than defending a lawsuit or responding to a cease and desist letter.