DATA PRIVACY AND CYBERSECURITY

DID DATA SCRAPING JUST GET A TINY BIT SAFER?

by Justin Root and Sara Jodka

Is it okay to scrape data from another website? This is a frequently asked question that almost always leads to an ambiguous and equivocal answer. Legal practitioners are quick to point out the risks of civil and criminal liability that could be incurred by scraping data from someone else's website, and several lawsuits have been spurred by the practice. This week, the United States District Court for the Northern District of California (the "Court") issued an order in hiQ Labs, Inc. v. LinkedIn Corporation that may foretell of a somewhat safer landscape for some data scrapers.

What is data "scraping"? Basically, it is the process by which a company uses a software algorithm to automatically collect or harvest data. The case at issue concerned a company, hiQ Labs, Inc. ("hiQ"), that developed software to analyze data from public LinkedIn profiles to help employers determine which workers are likely to leave or stay. hiQ's software automatically collects, i.e., "scrapes," publicly available workforce data from LinkedIn profiles. By analyzing this data over time, hiQ can identify changes that may indicate an employee is looking for other employment opportunities. In the case, hiQ moved the court for a preliminary injunction in response to LinkedIn sending a cease and desist letter to hiQ that threatened litigation, and implementing blocking techniques designed to prevent hiQ's automated data collection methods from scraping user data. LinkedIn had allowed hiQ to engage in this activity for years before sending the cease and desist letter, terminating hiQ's LinkedIn subscription, and (citing LinkedIn's User Agreement) alleging that any continued access by hiQ would be unauthorized and, therefore, a violation of several laws, including the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. In addition to moving for a temporary restraining order, hiQ also asked the Court for a declaration that its scraping activity did not violate the CFAA.

On August 14, 2017, the Court granted HiQ's request and issued a preliminary injunction preventing LinkedIn from interfering with hiQ's scraping of data from public LinkedIn profiles. In a quite thorough decision, Judge Edward M. Chen questioned whether the automated scraping of publicly available data from public-facing websites would violate the CFAA, regardless of the website's user agreement. Equating LinkedIn's position to that of a store owner who hangs a sign in a window and then seeks to ban certain people outside from looking at it, the Court opined:

> *A user does not "access" a computer "without authorization" by using bots, even in the face of technical countermeasures, when the data it accessed is otherwise open to the public.*

The Court went further and, in addressing LinkedIn's privacy argument, noted:

> *LinkedIn's professed privacy concerns are somewhat undermined by the fact that LinkedIn allows other third parties to access user data without its members' knowledge or consent.*

It is important to note that this Order is limited in scope to only the issue of whether injunctive relief is appropriate based on the particular facts of the matter; it is not a true finding that the CFAA does not apply. The Court, however, appeared highly critical of the argument that it does. Further, the Court's leanings are based on a number of factors that weight in hiQ's favor, such as:

- hiQ does not have to log into a LinkedIn account to see the data (and, therefore, may not be bound by the User Agreement);
- LinkedIn does not claim a proprietary interest in its users' profiles;
- The user accounts from which data is scraped are set to be publicly viewable by anyone, regardless of whether the viewer has a LinkedIn account; and
- hiQ had engaged in the activity for years with LinkedIn's knowledge prior to LinkedIn terminating its access and sending a cease and desist letter.

This is not to say that all data scraping is safe from CFAA (or other) challenges. Judge Chen noted that other cases have gone the other way, with courts finding CFAA violations for automated data scraping, but usually only when the data being scraped is protected behind access control measures (such as logon credentials). Agreeing to a website's terms of service and utilizing (or bypassing) access control measures to scrape a website's data would lean toward a finding that the access was unauthorized (especially where a site's terms of service ban such activities by its authorized users). In addition, it is important to note that data scraping may run afoul of state laws, intellectual property protections, or contractual obligations with or running to the benefit of the party whose data is being scraped.

If you have questions about your company's automated collection, storage, and use of information; concerns about protecting your information from unauthorized scraping; or otherwise need assistance with data privacy or cybersecurity matters, Dickinson Wright's Data Privacy and Cybersecurity attorneys can help you analyze and navigate your particular situation.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of data privacy and cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Justin L. Root is Of Counsel in Dickinson Wright's Columbus office. He can be reached at 614.591.5465 or jroot@dickinsonwright.com.

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.