Again, Computer Fraud and Abuse Act Likely Does Not Protected "Ungated" Date, 9th Circuit

HiQ Labs, Inc. v. LinkedIn Corp., Case No. 17-16783 (9th Cir. Apr. 18, 2022)

By: Jason Keener & Victoria Hanson | May 2, 2022

While a website owner may not want competitors scraping information from their system, it may not be a violation of the Computer Fraud and Abuse Act ("CFAA") unless the website owner has "gates-up." The Ninth Circuit recently upheld a preliminary injunction preventing LinkedIn Corp ("LinkedIn") from denying hiQ Labs, Inc. ("hiQ") access to publicly available information on LinkedIn member profiles.

LinkedIn, a professional networking site, permits users to create profiles with their personal professional information. Using automated bots, hiQ, a data analytics company, scraped information from public LinkedIn profiles which it then used to create "people analytics" to sell to business clients. In May 2017, LinkedIn sent hiQ a cease-and-desist letter. In return, hiQ asserted its right to access LinkedIn's public pages and filed an action seeking injunctive relief and a declaratory judgment that LinkedIn, among other things, could not invoke the CFAA, which prohibits a person from accessing a "protected computer" without authorization.

The district court found in favor of hiQ, granting a preliminary injunction and ordering LinkedIn to remove technical barriers to hiQ's access of public profiles. LinkedIn asserted that hiQ had violated the CFAA once it received a cease-and-desist letter from LinkedIn because it continued scraping LinkedIn's data. LinkedIn appealed and the Ninth Circuit affirmed the preliminary injunction. The Supreme Court granted certiorari, vacated the judgment, and remanded for further consideration in light of *Van Buren v. United States*, 141 S. Ct. 1648 (2021), which held that the CFAA "covers those who obtain information from particular areas in the computer . . . to which their computer access does not extend" and does not cover "information that is otherwise available to them."

On remand, finding that *Van Buren* reinforced its interpretation of the CFAA, the Ninth Circuit reaffirmed the district court's granting of the preliminary injunction. LinkedIn could not prevent hiQ from collecting and using information that LinkedIn users had shared on their public profiles because LinkedIn did not have its "gates-up" such that an authorization was required to access that information. Instead, LinkedIn profiles contained information that was available for viewing by anyone with a web browser. Further, the Ninth Circuit found that hiQ's actions were not "without authorization" because that statutory language was limited to "when a person circumvents a computer's generally applicable rules regarding access permissions" rather than a contract-based interpretation.

This case demonstrates that, if a company does not have its "gates-up" such that there are no restrictions to accessing information, then that company likely cannot bring a CFAA claim against another if it is using publicly available data on that company's website. Therefore, in order to ensure that a CFAA claim is available, that company's information must be password protected or restricted in a way that information is not otherwise publicly available.