LinkedIn v. HiQ and the trans-Atlantic privacy divide

Apr 22, 2022 Save This

Omer Tene
IAPP Member Contributor (/about/person/0011a00000DlJ5bAAF)

In a resounding victory for companies whose business model depends on web scraping, the U.S. Ninth Circuit Court of Appeals held this week (https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf) that such activity does not violate the U.S. Computer Fraud and Abuse Act. The decision, which allows hiQ, a "people analytics" company, to continue scraping publicly available profile information from LinkedIn for its own business purposes, crystalizes the deep divide around the notion of privacy and data protection between Europe and the U.S. It also brings into sharp relief the fault lines between privacy and competition policy, particularly in the context of major tech platforms and the data ecosystems they nurture.

The case, hiQ Labs vs. LinkedIn Corporation (https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf), was put in motion when in May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ was violating LinkedIn's terms of use and demanding that it stop accessing and copying data from LinkedIn's servers.

The decision primarily turned around the court's interpretation of the CFAA, an anti-hacking law with criminal sanctions that companies have repeatedly invoked to enforce their terms of use.

In a nutshell, LinkedIn argued that scraping data violated its terms of use and therefore constituted "unauthorized access" to its servers under CFAA. HiQ countered, and the court agreed, that there can be no "unauthorized access" where authorization for access isn't required in the first place. According to the court, the CFAA concept of access "without authorization" is akin to "breaking and entering," yet one cannot break and enter into a space that is open to the public. The court viewed the Supreme Court's ruling in Van Buren v. United States (https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf), which held a policeman didn't violate CFAA by running an unauthorized license plate search in a police database, as supportive of its decision.

Think about it this way: If a garden is surrounded by a fence with a gate and the gate is closed, anyone climbing over the fence is breaking and entering. But a garden owner cannot accuse someone of breaking and entering if there is no fence. A possible counterargument is that while there's no fence, there's a "sign" — LinkedIn's terms of use — which says that access to the garden is permitted only for personal recreation but not for running a business.

In this case, in addition to that "sign" LinkedIn handed the "visitor" a personal note — the cease-and-desist — warning they're not welcome on the property. But the court rejected such an argument, at least insofar as the encroachment is regarded as a violation of the criminally enforced CFAA.

with their username and password. Circumventing such password restrictions to scrape data could be a violation of CFAA (Facebook v. Power Ventures (https://cdn.ca9.uscourts.gov/datastore/opinions/2016/07/12/13-17102.pdf)).

Moreover, scrapers aren't entirely out of the woods yet. As the court stated, "even if the CFAA does not apply: state law trespass to chattels claims may still be available. And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie."

Be that as it may, the threat of a criminal penalty that hovered over scrapers for violating terms of use now seems remote.

To a European bystander, the result of the decision may seem odd. How could hiQ possibly be allowed to scrape individuals' personal data and use it for "people analytics"? What is the legal basis for this? Of course, even if the information is publicly available, individuals have not consented to such a use; and they do not have a contract with hiQ.

Cross GDPR Articles 6(1)(a) and (b) from the list.

Could hiQ rely on its "legitimate interest" under Article 6(1)(f)? To scrape individuals' data without their knowledge or consent and in violation of the platform's terms of use? Surely not. And while hiQ may argue that users "manifestly made public" the information by posting it on LinkedIn, therefore satisfying a condition to processing even sensitive data under the stricter Article 9(2)(e), the conventional interpretation is that a controller needs an Article 6 hook for data processing in addition to one under Article 9.

Herein lies the trans-Atlantic divide on privacy and data protection.

In Europe, a company needs a legal basis, that is, positive permission, to process data. You are allowed to do only what the law explicitly sanctions. Whereas in the U.S., the opposite is true. A company — anyone really — is allowed to do anything with data, as long as the law doesn't prohibit it. And indeed, the hiQ court held that the law, or at least CFAA, doesn't prohibit access to an area that is open to the public. The differences in views around privacy are particularly stark in connection with publicly available information, since in the U.S. any limitation of collection and use of such data also triggers First Amendment concerns.

The privacy implications of the decision were not lost on the Ninth Circuit. To LinkedIn's argument that hiQ should be enjoined from accessing data to protect users' privacy, the court replied that such privacy interests are outweighed by hiQ's right to conduct business. The court stated that "there is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and it is doubtful that they do."

More saliently, the court questioned the bona fides of LinkedIn's argument, given that LinkedIn itself offered to recruiters similar analytics services to those of hiQ. To that effect, the court quoted a CBS interview with LinkedIn CEO Jeff Weiner, who expressed the platform's intent to "leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site."

The court's reasoning resonates at a time when companies position privacy as an argument in competitive maneuvers against market rivals. Critics have claimed that EU regulators' single-minded mission and focus on data protection misses the forest for the trees. For example, by decimating the online adtech ecosystem, privacy policymakers may be dealing large platforms a lucrative prize.

It's worth quoting the court on this issue:

> “HiQ points out that data scraping is a common method of gathering information, used by search engines, academic researchers, and many others. According to hiQ, letting established entities that already have accumulated large user data sets decide who can scrape that data from otherwise public websites gives those entities outsized control over how such data may be put to use.”

And later:

> “We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.”

These strong words demonstrate how, in the U.S., courts adjudicate cases across a plurality of arguments, fields of law and policy considerations. While privacy policy may point one way, competition points another, and criminal law in yet another direction. Regardless of whether one agrees with the outcome of this specific case, it seems that a synthesis of all of these factors, privacy, publicly available information, competition, speech and freedom to run a business — yields results that are more grounded than decisions based on just one line of reasoning.

Photo by Veronica Reverse on Unsplash

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200