Data Privacy and Cybersecurity

Data Scraping: In *hiQ v. LinkedIn*, the Ninth Circuit Reaffirms Narrow Interpretation of CFAA

By: Sara M. Crook, Aaron R. Cooper and Madeleine V. Findley

On April 18, 2022, the Ninth Circuit reaffirmed its narrow interpretation of the Computer Fraud and Abuse Act's (CFAA) "without authorization" prong in a data scraping dispute between hiQ and LinkedIn. The opinion upheld a preliminary injunction that barred LinkedIn from stopping hiQ from scraping public data from the LinkedIn website and held that scraping such public information likely does not constitute accessing a computer "without authorization" under the CFAA.[1] The opinion is good news for companies employing data scraping practices for publicly available information. More broadly, the decision's narrow interpretation of the CFAA follows the Supreme Court's narrow approach to the statute in its *Van Buren* decision and clarifies (at least in the Ninth Circuit) several questions that the Supreme Court's ruling in *Van Buren* left open.[2]

The CFAA and the *Van Buren* Decision

The CFAA prohibits, in relevant part, accessing computers "without authorization" or "exceed[ing] authorized access" and thereby obtaining information, and permits civil recovery for victims suffering "damage or loss" as a result of a violation.[3] As a prior Jenner & Block alert discussed, in *Van Buren v. United States*, the Supreme Court resolved a Circuit split over the CFAA's "exceeds authorized access" prong, holding that the CFAA does not apply to an individual who is authorized to access information on a computer, even if they do so for an improper purpose. Instead, the Court held, the CFAA creates a "gates-up-or-down" inquiry: either an individual is authorized to access a computer system or parts of that system, or they are not; a person "exceeds authorized access" by accessing a part of the computer system to which the authorization does not extend.[4]

The Supreme Court's decision suggested—but did not expressly hold—that violating purpose-based limits on access to a computer system, such as the terms of service of a public website, would also not on its own violate the CFAA's "without authorization" prong.[5] Instead, the Court limited its holding to the scope of "exceeds authorized access."[6] Enter the *hiQ v. LinkedIn* dispute.

hiQ v. LinkedIn

Before the *Van Buren* decision, LinkedIn Corporation (LinkedIn) and data science company hiQ Labs, Inc. (hiQ) were litigating in the Ninth Circuit about whether hiQ's data scraping practices violate the CFAA. Data scraping, for purposes of the litigation, was defined as an information gathering and analysis tactic whereby a robot or individual "extract[s] data from a website and cop[ies] it into a structured format, allowing for data manipulation or analysis."[7] At issue in this litigation, hiQ scraped information from public profiles on LinkedIn and then sold the resulting "people analytics"—such as whether a person was likely to leave a job—to its clients.[8] LinkedIn sent a cease-and-desist letter demanding hiQ stop scraping data from its website and implemented technical barriers specifically to "prevent hiQ from accessing, and assisting others to access, LinkedIn's site, through systems that detect, monitor, and block scraping activity."[9] In the cease-and-desist letter, LinkedIn asserted that hiQ's conduct violated LinkedIn's terms of service, and if hiQ continued to scrape data in the future, it would violate the CFAA and similar statutes.[10]

hiQ sought, and the district court granted, a preliminary injunction to enjoin LinkedIn from halting its business practices.[11] At issue was the "without authorization" prong of the CFAA: did LinkedIn have a viable claim that hiQ's data scraping constituted access without authorization after LinkedIn sent its cease-and-desist letter and implemented technical barriers to access, or was hiQ correct that there was no CFAA violation because it was only scraping publicly available LinkedIn data?

Agreeing with hiQ that the CFAA likely does not prohibit access to publicly available information, the district court noted it had "serious doubt" that LinkedIn's cease-and-desist letter revoking hiQ's access to "public portions of its site" meant that hiQ was acting without authorization under the CFAA, and the district court ordered LinkedIn to remove all barriers blocking hiQ from accessing public profiles.[12] In September 2019, the Ninth Circuit affirmed the district court, holding that hiQ had established the elements for a preliminary injunction in part because hiQ raised a "serious question" as to whether "without authorization" is applicable to information publicly available.[13] LinkedIn petitioned the Supreme Court for review. But, on June 3, 2021, the Supreme Court decided *Van Buren*, and shortly thereafter remanded and instructed the Ninth Circuit to reevaluate the case in light of that opinion.[14]

On remand, the Ninth Circuit again narrowly interpreted "without authorization,"[15] and reaffirmed the district court's preliminary injunction.[16] The Ninth Circuit held that "the concept of 'without authorization' does not apply to public websites."[17] It defined "without authorization" as "when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer."[18] The Ninth Circuit read *Van Buren* to side with this narrow approach to "without authorization," looking to whether the unauthorized conduct was akin to breaking and entering, in contrast to the First and Eleventh Circuits' broader "contract-based" approach.[19]

The Ninth Circuit also interpreted the CFAA to contemplate three types of accessible computer systems: "(1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed)."[20] In the Ninth Circuit's view, scraping public information from publicly accessible websites falls into the first category—and it is not an issue of authorization at all. Rather, "access is open to the general public and permission is not required."[21] Thus, LinkedIn's putative CFAA claim was unlikely to prevail on the merits. As the Ninth Circuit explained it, the Supreme Court's "gates-up-or-down" approach in *Van Buren* governed the second and third categories—where authorization is required and has been given, and where authorization has not been given at all or has not been given for the specific part of the system the user accessed.[22]

***hiQ v. LinkedIn's* Impact**

The Ninth Circuit's interpretation is a positive development for those employing data scraping, but bad news for companies that seek to assert control over data posted on otherwise public websites. For any data analytics business that relies on access to or scraping of publicly accessible data, this opinion offers a roadmap to avoid CFAA threats or liability within the Ninth Circuit. That is because, in the Ninth Circuit's view, the effect of blocking hiQ from LinkedIn was enough to constitute irreparable harm.[23] In particular, the Ninth Circuit rejected LinkedIn's argument that hiQ could change its practices to avoid data scraping, because doing so would be resource-heavy and expensive.[24] And, the Ninth Circuit weighed hiQ's business interest more heavily than LinkedIn's stated interest in the privacy of its users, because the data at issue was comprised of profiles that these users chose to make public, and which LinkedIn itself disclaimed any responsibility for or ownership of.[25]

For that reason, though the opinion was limited to the preliminary injunction context, its effects may

expand beyond the CFAA and have implications for data privacy law. LinkedIn voiced concern that users' privacy interests were implicated, in part because many of these users likely wanted to hide their job searches from their employers.[26] The Ninth Circuit rejected LinkedIn's argument because it found it "doubtful" that "users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly."[27] In addition, LinkedIn's privacy policy alerted users that information they posted would be publicly accessible.[28]

The Ninth Circuit also expressed a concern over "information monopolies."[29] The opinion noted that, while the public has an interest in preventing bad-actor use of data, like identity theft or cyber-abuse, there was not a public benefit in LinkedIn having "free rein to decide, on any basis, who can collect and use data—data that the companies do not own."[30] This policy interest may guide further legal decisions in this area.

From the perspective of companies that host information on public websites, the Ninth Circuit's opinion obviously makes it harder to prevent third parties from collecting and monetizing that information. Such companies may have to consider whether to require the equivalent of "gates down" approaches going forward if they seek to invoke the protections of the CFAA.

What Comes Next

How other courts of appeals interpret *Van Buren* in new contexts, and whether they adopt the Ninth Circuit's view of the CFAA's structure, remains to be seen. There is no guarantee that other courts will follow the same approach as the Ninth Circuit, which means that risk remains for this kind of data scraping in other jurisdictions, including jurisdictions outside the United States where foreign law applies. Moreover, it may not always be clear what Circuit's law applies if a computer outside of the Ninth Circuit accesses a website hosted inside the Ninth Circuit. The effect of this decision—like *Van Buren*—on interpretation of similar state laws prohibiting computer misuse also may vary.

In addition, the facts in this case stress both the public accessibility of the data *and* LinkedIn's own position with respect to its user's information. As a result, the Ninth Circuit's view of whether information is truly "public" may vary if the user intent to make information publicly available is not clear, if a website owner asserts some claim with respect to its user's data, or if the data has been "demarcated … as private" in some way, including through utilization of an "authentication system" like usernames and passwords.[31] Thus, application of this case will be a context-dependent inquiry.

In the context of cybersecurity, website owners will want to keep an eye on how other Circuits interpret *Van Buren*. For now, at least in the Ninth Circuit, website owners who want to keep public information private would not succeed in implementing technical barriers and issuing cease-and-desist letters to offending parties who have an established business use.

The Ninth Circuit's decision is also more positive news for those in favor of a narrow CFAA application—like computer security researchers who feared CFAA prosecution would interfere with their work.[32] But they will need to monitor how other Circuits rule on this issue, keeping in mind that *Van Buren* did not adopt as narrow of a view of "without authorization" as the Ninth Circuit just did.

Finally, the *hiQ* opinion also does not preclude—and expressly leaves open—risk of liability based on other legal regimes. In particular, the Ninth Circuit left open the possibility for "victims of data scraping" to recover through state law causes of action like trespass to chattels, misappropriation, or breach of contract.[33] While *Van Buren* and *hiQ* suggest that courts will be hostile to attaching CFAA liability to violations of websites' Terms of Service alone, an open question remains about whether civil penalties based on state torts may attach to such violations. In addition, the CFAA prohibits other forms of computer use that do not require access, including causing unauthorized "damage," defined as "any impairment to the integrity or availability of data, a program, a system, or information."[34]

Contact Us

Sara M. Crook
scrook@jenner.com | Download V-Card

Aaron R. Cooper
acooper@jenner.com | Download V-Card

Madeleine V. Findley
mfindley@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card

Shoba Pillay
Co-Chair
spillay@jenner.com
Download V-Card

[1] *hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-16783, 2022 WL 1132814, at *16 (9th Cir. Apr. 18, 2022).
[2] *See* Jenner & Block's June 9, 2021 client alert on the *Van Buren* decision.
[3] 18 U.S.C. § 1030(a)(2), (c), (g).
[4] 141 S. Ct. 1648, 1662 (2021).
[5] *Id*. at 1661.
[6] *Id*. at 1662.
[7] *hiQ Labs, Inc.*, 2022 WL 1132814, at *3 n.4
[8] *Id*. at *4. These analytics would indicate, for example, if someone appeared likely to leave their job.
[9] *Id*.
[10] *Id*. at *5.
[11] *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1103 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019), *cert. granted, judgment vacated*, 141 S. Ct. 2752, 210 L. Ed. 2d 902 (2021), and *aff'd*, No. 17-16783, 2022 WL 1132814 (9th Cir. Apr. 18, 2022).
[12] *hiQ Labs, Inc.*, 2022 WL 1132814, at *5; *see also hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019), *cert. granted, judgment vacated*, 141 S. Ct. 2752, 210 L. Ed. 2d 902 (2021), *and aff'd*, No. 17-16783, 2022 WL 1132814 (9th Cir. Apr. 18, 2022).
[13] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 990 (9th Cir. 2019), *cert. granted, judgment vacated*, 141 S. Ct. 2752, 210 L. Ed. 2d 902 (2021).
[14] *LinkedIn Corp. v. hiQ Labs, Inc.*, 141 S. Ct. 2752 (2021); *see* Jenner & Block's *Van Buren* client alert.

[15] *hiQ Labs, Inc.*, 2022 WL 1132814, at *16.
[16] *Id.* at *17.
[17] *Id.* at *14.
[18] *Id.* at *16.
[19] *Id.* at *13.
[20] *Id.* at *14.
[21] *Id.*
[22] *Id.*
[23] *Id.* at *5.
[24] *Id.*
[25] *Id.* at *2, 7.
[26] *Id.* at *6.
[27] *Id.* at *7.
[28] *Id.*
[29] *Id.* at *17.
[30] *Id.*
[31] *Id.* at *14, 16.
[32] Jenner & Block formerly discussed this in its June 9, 2021 client alert on the *Van Buren* decision.
[33] *hiQ Labs, Inc.*, 2022 WL 1132814, at *16.
[34] 18 U.S.C. § 1030(a)(5), (e)(8).