Marquette Intellectual Property & Innovation Law Review

Volume 25 | Issue 2 Article 8

Summer 2021

Access Denied? Unauthorized Access After hiQ Labs v. LinkedIn

Dalton Sjong

ACCESS DENIED? UNAUTHORIZED ACCESS AFTER *HIQ LABS V. LINKEDIN*

DALTON SJONG

I. INTRODUCTION

Technological progression has increased the rate and efficiency at which information is disseminated and has connected global marketplaces in a way that was previously inconceivable. However, as technological innovation has made information more widely available, protecting that information and who has access to it has proven to be a challenging task. Computers are now able to store massive amounts of information and the invention of the internet and its progression has connected computers across the globe. On the one hand, we can communicate and share information across the world in an instant, creating a worldwide marketplace for idea sharing and more efficient business transactions. On the other hand, keeping track of where this information is accessed and used is nearly impossible given the rapid speed at which it is shared.

Naturally, individuals, as well as corporations, have data stored on computers that they want to share selectively or not at all. Restricting access and granting selective authorization is an obvious solution. Just as naturally, however, those without access or authorization still wish to obtain this

information as it is presumably protected for a reason. Hackers have become more sophisticated and monitoring selective authorization can be cumbersome. Cybersecurity measures such as password encryption and contractual use agreements are not unfailing safeguards to protection.

Recognizing this difficult issue, legislators took steps to provide further legal recourse to protect information. Thus, the Computer Fraud and Abuse Act (CFAA) was introduced. Since its inception, the CFAA has been the subject of much criticism and litigation. Recently, courts' interpretation of "without authorization" has been the subject of several high-profile cases. The recent Ninth Circuit holding in *hiQ Labs v. LinkedIn* conflicts with previous Ninth Circuit precedent regarding the Computer Fraud and Abuse Act.[1] There appears to be a shift to a narrower interpretation of the CFAA in order to "de-weaponize" the statute and reel it in to more closely align with its original purpose.

Prior to the *hiQ Labs* ruling, the CFAA had an extremely broad sweeping effect beyond that of simply computer hacking.[2] For example, in *United States v. Drew*, the defendant, Lori Drew, used a fraudulent account on MySpace to bully a girl her daughter went to school with, ultimately pushing the girl to commit suicide.[3] The Central District Court of California convicted Lori Drew of a misdemeanor violation of CFAA Section 1030(a)(2)(C) for violating the MySpace terms of use.[4] In another example, Andrew Auernheimer was convicted under the CFAA for finding a hole in AT&T's website security and harvesting over 100,000 email addresses of users that had used AT&T's network.[5] This was done without circumventing any password requirements or access restrictions.[6] Although his conviction was overturned on a technicality as to venue, it highlights the wide-ranging array of activities that courts have determined fall under the CFAA.[7] The *hiQ Labs* result is a landmark case that conflicts with this historically broad enforcement and sparks a trend toward narrowing the scope of CFAA applicability.

The *hiQ Labs* decision stands for the proposition that those making information publicly available should not be able to use the CFAA to criminalize access by some but not others.[8] This seems to limit the amount of

1. *See* United States v. Nosal (*Nosal I*), 676 F.3d 854 (9th Cir. 2012).

2. Andrew Couts, *You're Probably Unknowingly Breaking Laws Online Thanks to the CFAA*, DIGITAL TRENDS (Jan. 18, 2013) https://www.digitaltrends.com/web/understanding-the-cfaa/.

3. United States v. Drew, 259 F.R.D. 449, 452–53 (C.D. Cal. 2009).

4. *Id.* at 467.

5. United States v. Auernheimer, 748 F.3d 525, 532 (3d Cir. 2014).

6. *Id.* at 534 n.5.

7. *Id.* at 530 n.2, 541.

8. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1003 (9th Cir. 2019).

protection that platforms can provide to users that choose to opt out of platform privacy protections that limit the amount of publicly available information.[9] The effect of this ruling places an affirmative duty on the information provider to protect their information themselves and rely less on the CFAA.[10] The CFAA has strayed from its original purpose and become a weapon for private entities to selectively criminalize users that access information they make publicly available. This comment will focus on how the Ninth Circuit's interpretation of the "without authorization" language of the CFAA in the *hiQ Labs* case appropriately narrows the scope of the CFAA.

The ruling in this case turned on the Ninth Circuit's interpretation of the term "without authorization" which is left undefined in the CFAA.[11] The court's interpretation seems to limit the scope of "without authorization" to more narrowly tailor its application strictly to situations that involve access to information through hacking and password circumvention.[12] If this Ninth Circuit interpretation is indicative of a change in ideology, those that hold information must take greater care in how they present that information publicly.

II. COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act was enacted in 1986 primarily as a response to combat computer hacking.[13] Although it has been amended several times, it has historically had a broad sweeping effect covering conduct not originally contemplated when enacted.[14] In some regards, the breadth of the CFAA is concerning and, according to some, has become an abusive tool to reach all aspects of computer use activities.[15] The clause at issue is 18 U.S.C. Section 1030(a)(2); this provision reads "[w]hoever . . . intentionally accesses a computer *without authorization* or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished . . ." by fine or imprisonment.[16] The elements the government must prove to find a violation are that the defendant: (1) intentionally, (2) exceeded authorized access, (3) to a protected computer, and (4) thereby obtained information.[17]

---

9. *Id.* at 920.

10. *Id.* at 1000.

11. *See* 18 U.S.C. § 1030.

12. *Computer Fraud and Abuse Act (CFAA)*, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct (last visited Mar. 21, 2020).

13. *Id.*

14. *Id.*

15. *Id.*

16. 18 U.S.C. § 1030(a)(2).

17. United States v. Auernheimer, 748 F.3d 525, 533 (3d Cir. 2014).

The most relevant provision of the CFAA contains the vital terms "without authorization" and "exceeds authorized access" which was the crux of the *hiQ Labs* decision which sparked this conflict.[18] To begin, the term "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication."[19] As computer systems have become more readily accessible, this definition of "protected computer" has essentially come to include any computer connected to the internet that can access servers and "computers that manage network resources and provide data to other computers."[20]

III. RELEVANT CASELAW

The *hiQ Labs* decision is important because it appears to conflict with how the CFAA and, more specifically, the "without authorization" provision, has been previously interpreted. The *Nosal* decisions lay the foundation for how the Ninth Circuit arrived at *hiQ Labs* and provide some insight into the *hiQ Labs* analysis.

A. The Build-Up to hiQ: The Nosal Cases

David Nosal was the subject of two Ninth Circuit cases that arose when he decided to leave his executive search firm Korn/Ferry International and form a competitor with his colleagues.[21] Before they split from the firm, the group downloaded confidential information from the firm's database for use in their competing endeavor.[22] The information was obtained by the employees through use of their own passwords which gave them access as part of their employment.[23] In *Nosal I*, the court distinguished between access restrictions and use restrictions and concluded that the "exceeds authorized access" prong of Section 1030(a)(4) of the CFAA does not extend to a company's own use policies and restrictions.[24] The court dismissed the CFAA violations against Nosal for aiding and abetting misuse of data accessed by his co-workers because a violation of a company's use restrictions does not necessarily violate the CFAA.[25] The court held that the phrase "exceeds authorized access" in the

18. *Id.*
19. 18 U.S.C. § 1030(e)(2)(B).
20. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019).
21. *Nosal I*, 676 F.3d 854, 856 (9th Cir. 2012).
22. *Id.*
23. *Id.*
24. *Id.* at 863.
25. *Id.* at 864.

CFAA is limited to violations of restrictions on access to information and not restrictions on its *use*, as that is dealt with elsewhere in legislation.[26]

In *Nosal II*, the Ninth Circuit Court of Appeals made a ruling on the same set of facts as applied in *Nosal I* to accessing a computer "without authorization."[27] The court held that once authorization to access a computer has been affirmatively revoked, access cannot be obtained by that user through a third party.[28] In its analysis, the court interpreted "without authorization" to mean a situation in which an employer has revoked permission to access a computer and an employee accesses it regardless.[29]

The Ninth Circuit Court of Appeals used the *Nosal* cases to limit the relevant CFAA provisions to their applicability in access, but not use. Revocation of access and obtaining access through a proxy are clear violations of the CFAA following the *Nosal* decisions.

B. Diminishing the Scope of the CFAA: hiQ Labs v. LinkedIn

Upon the decisions of *Nosal I* and *Nosal II*, it appeared as if the Ninth Circuit Court of Appeals had established a straightforward and deliberate interpretation of the CFAA provision. It seemed the court had narrowed the legislation to contemplate situations in which permission to access had not been granted, but access was obtained regardless.[30] The court also closed the "back door" to this issue by determining that access could not be obtained by a third-party proxy by way of circumventing access requirements.[31]

The decision in *hiQ Labs* convolutes the straightforward interpretation achieved by the *Nosal* cases. In *hiQ Labs v. LinkedIn*, hiQ Labs was using an automated computer program (bot) to obtain information from LinkedIn's public member profiles and providing that information to third parties for use in recruiting and employment decisions.[32]

The *hiQ Labs* court noted the CFAA "contemplates the existence" of three categories of computer information: (1) information for which access is open to the general public and permission is not required; (2) information for which authorization is required and has been given; and (3) information for which authorization is required but has not been given.[33] The *hiQ Labs* case is

26. *Id.* at 863–64.
27. *See* United States v. Nosal (*Nosal II*), 844 F.3d 1024, 1030–31 (9th Cir. 2016).
28. *Id.* at 1028.
29. *Id.* at 1029.
30. *See id.*
31. *Id.*
32. *See* hiQ Labs Inc. v. LinkedIn, 938 F.3d 985, 991 (9th Cir. 2019).
33. *See id.* at 1001.

concerned with the first category, whereas the *Nosal* and *Powerventures* cases revolve around the second and third categories.[34]

As a business practice, hiQ was using bots to scrape information that LinkedIn users made public on their profiles along with an algorithm to provide analytics services to clients.[35] These analytics services came in two forms: "Keeper" and "Skill Mapper."[36] Furthermore, LinkedIn was fully aware of hiQ offering these services with their public information, and even contributed to the development of these programs.[37]

With the "Keeper" service, clients were able to identify the employees that were most at risk of being poached by other companies and enabled clients to offer opportunities to retain these employees.[38] The "Skill Mapper" service identified skill gaps and allowed employers the opportunity to provide training to close those gaps.[39]

LinkedIn subsequently announced they were launching a service called "Talent Insights" which, essentially, accomplished internally the same thing hiQ was doing externally.[40] Upon the launch of this program, LinkedIn sent cease and desist letters to hiQ demanding that they stop scraping LinkedIn's information and any such further use would be in violation of LinkedIn's user agreement.[41] hiQ retaliated by demanding LinkedIn recognize their right to access public information and, when LinkedIn refused, filed suit for a preliminary injunction.[42]

C. Ninth Circuit Rationale in hiQ Labs v. LinkedIn

The Ninth Circuit was asked to determine whether once hiQ received the cease-and-desist letter, any further scraping by hiQ was "without authorization" and thus a violation under the CFAA. In its interpretation, the court noted that when a statute is ambiguous, as is the term "without authorization," it should be interpreted by giving the words their plain and ordinary meaning.[43] "Without authorization" would then mean simply accessing a protected computer without permission.[44]

---

34. *See id.* at 1002.
35. *Id.* at 991.
36. *Id.* at 991.
37. *See id.*
38. *Id.*
39. *Id.*
40. *Id.* at 992.
41. *Id.*
42. *Id.*
43. *Id.* at 999.
44. *Id.*

The court clarified that "authorization" carries an "affirmative notion" indicating that access is prohibited except to those which it is explicitly granted.[45] Following this logic, the court concluded that, where the default is free access without authorization, selective denial of access would be a ban, not a lack of authorization.[46] To bolster this logic, the court looked at the legislative history and Congress's intent in order to defer to the statute's overall purpose.[47] Specifically, they looked at the Senate Judiciary Committee's comment on Section 1030(a)(2)(c) added in the 1996 amendment.[48] The Committee articulated that the Section was designed to "increase protection for the privacy and confidentiality of computer information."[49] The court therefore determined that the statute was enacted to prevent intentional intrusion onto someone else's computer in order to combat computer hacking.[50] The court used this legislative history to reach the conclusion that the prohibition on unauthorized access only applies to private information, and it follows that private information is classified as such through some sort of permission requirement.[51]

In conclusion, the court affirmed the district court's determination that hiQ established the elemental requirements to receive a judgment in favor of their motion for a preliminary injunction.

III. ANALYSIS OF THE HIQ DECISION'S EFFECT ON AN ENTITY'S ABILITY TO INVOKE THE CFAA

Essentially, the recent *hiQ Labs* ruling effectively narrows the scope of the CFAA by determining conduct that does *not* violate the "without authorization" provision. The Ninth Circuit seems to want to reduce the CFAA breadth to encompass only its original intent to combat hacking.[52] This would appear to be a victory for industries of research and data collection, but a battle won in the *hiQ Labs* decision for narrowing the CFAA scope could mean a long-term loss for information sharing. As the arm of legislative reach in information protection is shortened, the wall that entities build around that information will grow taller.

Entities that hold information they choose to make public will most likely view this decision as a negative outcome creating an obligation to implement affirmative restrictions as it pertains to accessing information they currently

45. *Id.* at 1000.
46. *Id.*
47. *Id.* at 1000–01.
48. *Id.* at 1001.
49. *Id.*
50. *Id.* at 1000.
51. *See id.* at 1001.
52. *See id.* at 1000–01.

make public. Companies that previously believed the CFAA could be used to protect the information they provided publicly will now be left without the statute as a means of legal protection. However, companies that would like to provide useful data and information to the public may choose not to do so at all without statutory protection.

Without legislative protection by way of the CFAA, entities have no assurance as to the protection of their public information unless they take affirmative precautions to restrict access to it. Following the *hiQ Labs* case, the CFAA does not protect information unless an entity takes affirmative steps to restrict access to information and explicitly authorize access to select parties. As a result, entities may simply choose to restrict all information they could provide on every platform rather than endure the administrative burden and expense that comes without the CFAA protection. Although *hiQ Labs* turned on access, if companies choose to authorize access, they will then likely feel the need to further restrict use. However, if the *Nosal* cases decided that a violation of a user agreement is not a CFAA violation, then a company is stuck between the choice of providing unfiltered, unprotected access to information they would like to make public or create restrictions which require access to be granted. But once access is granted, a company cannot restrict use. In the position of a business owner, it can be conceived that entities would instead just choose to restrict any and all access rather than take on the burdens that come with the narrowing applicability of the CFAA.

Although the *hiQ Labs* decision seems to align with the purported intention of the CFAA provisions at issue, it presents a huge barrier for entities that obtain and provide public information.

A. hiQ Labs Decision effect on the CFAA and Publicly Provided Information

Although the Ninth Circuit seems to stand for the proposition that it supports the free flow of information by creating a means of access that does not fall under the purview of the statute, the *hiQ Labs* decision seems to stand more for the adoption of the ideology that entities should take a proactive approach to protecting their online information. As a result of this Ninth Circuit decision, entities are now on clear notice that the CFAA will not be a crutch for entities to lean on when they provide public information on their platforms. Although this is only a case granting preliminary injunction, the court's approach sparks a trend towards affirmative precautions for entities providing information publicly. This could mark the end of publicly shared information on social media platforms (such as LinkedIn) and beyond.

The district court observed that LinkedIn implicitly recognizes that the information provided on their platform is public and that users do not have an

expectation of privacy.[53] The privacy policy itself tells LinkedIn users that they should not provide any information on their profile that they do not want to be public.[54] This alone makes it seem as if LinkedIn concedes that the information users choose to make public is public, and the default is that no authorization is required to access that information.[55] The court appears to create a presumption that, absent some sort of authorization requirement or barrier that selectively limits access, the information is public and the "without authorization" provision is inapplicable.

It could be argued that, at some point, the cost of protection will outweigh the benefit of providing public information. For example, social media platforms such as LinkedIn and Facebook could restrict their information to even Google searches to avoid use of the information they collect on their platform. From LinkedIn's perspective, it would seem to make more sense for them to incur the expense to make their user's information secure rather than use their funds to develop services to compete with third parties to use information that LinkedIn provides for the same purpose. Even if LinkedIn allowed Google and other search engines to access this information, a search engine user would find this information useless as they would have to provide their information to LinkedIn to gain access. It could be said this undermines the superficial intention that the *hiQ Labs* decision promotes information sharing as it just encourages entities to further limit access.

Although LinkedIn took precautions to prevent data scrubbing by way of using a text file to prohibit bots from gaining access to its servers, it generally provided the information it collected to the public.[56] Since it therefore falls under the CFAA first category of information, in order to be protected, LinkedIn must explicitly authorize access to specific parties in order to effectively prohibit access to others. LinkedIn left it up to their users to make the decision of whether or not to provide their information to the public, and, therefore, LinkedIn cannot be said to have restricted access when it deferred to its users to choose what information was public. LinkedIn would have to move this information from the first category to the second or third category as recognized by the courts.

Therefore, in the long run, it could be said that the Ninth Circuit *hiQ Labs* decision would ultimately restrict any and all information that entities would provide publicly. For example, currently, if one receives an invitation for a job interview, one can Google search the interviewer's name, come across the

53. *Id.* at 994.
54. *Id.*
55. *See id.* at 995.
56. *See id.* at 990–91.

individual's LinkedIn profile, and educate themselves on the interviewer's background. This provides the interviewee with information and talking points going into the interview. On the opposite end of the spectrum, an interviewer can come across a resume and easily search a candidate in order to further vet resumes based on information they receive from platforms such as LinkedIn that provide public information. Without such available information, entities may incur unnecessary administrative expenses vetting resumes, and candidates, although well-intentioned and motivated, may lack the resources to conduct proper interview research. This lack of information presents a strain to not only the potential employer but the candidate as well.

While that all may be well and true, it is not appropriate to continue broadening the scope of the CFAA. If an entity would like to make information available publicly without an access restriction, then it shall accept that it will relinquish control over where that information is disseminated and how it is used. Should that create an inconvenience to users and sharers, that inconvenience seems minor compared to the potential consequences of interpreting "without authorization" so broadly as to allow that provision to criminally regulate information use.

B. Applying the hiQ Labs Decision Retroactively

The Ninth Circuit's shift in interpretation of "without authorization" narrows the CFAA's breadth and would potentially change the outcome of cases in the not-so-distant past. For example, applying the new Ninth Circuit interpretation of CFAA Section 1030(a)(2)(c) to *United States v. Auernheimer* would potentially yield a different result.

As stated previously, in *Auernheimer*, the defendant used a gap in AT&T's security system to obtain over 100,000 e-mail addresses via their 3G network.[57] This was done without any password circumvention or "back-door" techniques such as using a third-party proxy to gain access with its authorization.[58] Although the case was overruled on grounds of improper venue, Auernheimer was convicted under Section 1030(a)(2)(c) provision of "without authorization" in New Jersey.[59] These factual circumstances present an interesting analysis in which a different outcome is probable under the recent Ninth Circuit interpretation.

Although it can be inferred that AT&T customers had a reasonable expectation of privacy when they provided their information for 3G access on their devices, the defendant's conduct may not be considered a violation of

57. *See* United States v. Auernheimer, 748 F.3d 525, 532 (3d Cir. 2014).

58. *Id.* at 530–31.

59. *Id.*

"without authorization" under the new Ninth Circuit interpretation. The reasonable expectation of privacy was but one small factor the Ninth Circuit had to consider when determining whether the information on LinkedIn was public in *hiQ Labs*. The court seemed to give more weight to the extent that access to the information was restricted. In *hiQ Labs*, LinkedIn left it up to individual users to choose what information they wanted to provide publicly. Once the user decided to provide information to the public, LinkedIn failed to enforce any measures, such as password protection or selective authorization, to access that information. Thus, when hiQ's bots scraped the information, there was no access restriction, which made it public and free to scraping as it fell in the first category of information contemplated by the CFAA.

Applying this rationale to *Auernheimer*, it can be reasonably foreseen that the defendant may escape liability under the CFAA. Although AT&T took steps to generally protect their user's information, the hole in its security system allowed unfettered access to user information. On its face, this would tend to fall into the first category of information just like *hiQ Labs*. For information to fall into one of the other two categories, there must be authorization required which is either granted or prohibited. In *Auernheimer*, there was no authorization requirement as the defendant obtained the information without circumventing a password restriction or using a third-party proxy's authorization to gain access. Therefore, this would appear to be public information in the first category which would be fair game for use if accessed. This seems to be a far more appropriate interpretation of the CFAA.

Although it may appear that narrowing the scope of the CFAA would harm public information sharers and information sharing in general, that concern is merely an illusion. In a general sense, those with information that warrant protection should bear the burden of protecting it. The *hiQ Labs* decision really prevents those that provide public information from using the "without authorization" provision to regulate use by choosing what access is authorized based on how the accessor uses said information. LinkedIn attempted to argue that hiQ did not have authorization to access user information because they were using a bot to scrape it, although any computer connected to the internet could have access to that information at any time. LinkedIn argued under the guise of "without authorization" to limit scraping because hiQ labs was using LinkedIn's public information in a way that LinkedIn did not like. If the court were to accept LinkedIn's position, private entities could make information available publicly without any authorization requirement and then selectively determine certain behaviors constituted as "unauthorized access" based on how the information is used. This is not an ideal outcome.

In addition, the court would have created an intimate connection between information use and the "without authorization" provision to access. This

would open the door for private entities like LinkedIn to enact user agreements that, if violated, would automatically revoke previous authorizations, thus rendering access unauthorized and subject it to prosecution under the CFAA. Although it may seem harmless or even a good idea to prevent scraping via a user agreement, this would have a far-reaching impact and even further broaden the scope of the CFAA.

To illustrate, an employer could grant an employee access to a work laptop supplied by the company and force the employee to sign a user agreement that the employee will not use the laptop for personal reasons. If that employee then goes home and uses the laptop to search for a dinner recipe online, that employee is then in violation of the user agreement, immediately triggering revocation of authorization and subjecting them to criminal prosecution under the CFAA provision of "unauthorized access." Although those user agreements are common and necessary, it seems reasonable to agree that inappropriate web surfing on a work computer should not be a criminal violation, but rather an issue that should be handled between employer and employee. Even further, a private entity or employer should not have the authority to pick and choose what behavior is deemed criminal.

However, a recent Eleventh Circuit decision that is now before the U.S. Supreme Court, *Van Buren v. United States*, potentially creates some tension between user agreements, use, and authorized access. In *Van Buren*, a police officer was using a police database to run license plate searches for personal reasons (also in exchange for money) in violation of a user agreement that stated the database was to be used for police activities only.[60] Ultimately, Van Buren was convicted of honest-services wire fraud, but he was also convicted under the CFAA.[61] The court used *United States v. Rodriguez* as support for Van Buren's conviction.[62] In *Rodriguez*, an employee at the Social Security Administration (SSA) used the SSA database to obtain address and birth date information of people in violation of an SSA policy, which prohibited employees from obtaining information from SSA databases without a legitimate business reason.[63] On appeal, Van Buren argued that he was innocent because "he accessed only databases that he was authorized to use."[64] However, the court was not willing to rule against *Rodriguez* and upheld Van Buren's conviction on the grounds that he did not have authorized access because access was only granted for "law enforcement purposes only."[65]

60. United States v. Van Buren, 940 F.3d 1192, 1197–98 (11th Cir. 2019).
61. *Id.* at 1198.
62. *Id.* at 1208.
63. United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).
64. *Id.* at 1263.
65. Van Buren, 940 F.3d at 1208.

In its ruling, the court acknowledges that other courts have been critical of the *Rodriguez* interpretation of "exceeds authorized access" because "it purportedly allows employers or other parties to legislate what counts as criminal behavior through their internal policies or their terms of use."[66] Notably, the court in *Nosal* rejected the *Rodriguez* interpretation ("noting that activities like '[Google]-chatting with friends, playing games, shopping or watching sports highlights' on a work computer are routinely prohibited by computer-use policies, and worrying that 'under the broad interpretation . . . such minor dalliances would become federal crimes'").[67]

The criticisms of *Rodriguez* are the product of well-founded concerns. For the purposes of this analysis, it should be noted there is an important distinction to be made between *Van Buren*, *Rodriguez*, and *hiQ Labs*. Where *hiQ Labs* concerns publicly available information on the internet, *Van Buren* and *Rodriguez* concern information that is stored on a *private* database that only grants authorization through employment. Therefore, the criticisms of the *Rodriguez* case hold value in an analysis of *hiQ Labs*. Violation of a user agreement where authorization is required and granted makes sense as that information has been protected and use controlled. However, violating a user agreement where authorization is not required would fulfill the prophecy of the concerns noted in the criticisms of *Rodriguez* as all kinds of seemingly harmless behavior could be subject to criminality ("[w]hile the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters").[68]

V. NINTH CIRCUIT INTERPRETATION: THE MORE APPROPRIATE APPROACH

Allowing entities to regulate the use of publicly available information by criminalizing certain behaviors and not others would further weaponize the CFAA and allow it to reach far beyond its originally intended scope. If an entity wants to regulate the use of information it holds, it should take affirmative steps to require authorization. Providing information on a public platform without any authorization requirements and then subsequently revoking authorization (that was never required in the first place) is essentially a trap to criminalize competitors and those using information in a way the provider does not like.

As it pertains to web scraping by bots, this analysis should not change. The mechanism by which information is collected should not influence

66. *Id.*

67. *Id.* (citing Nosal I, 676 F.3d 854, 860 (9th Cir. 2012)).

68. *Van Buren*, 940 F.3d at 1208 (citing United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015)).

authorization. This analysis has established that when information is made publicly available without an authorization requirement, the information provider cannot use the CFAA to regulate the use of that information by retroactively revoking an authorization that was never required in the first place. The fact that a bot is the one accessing the information does not change the fact that there was no authorization requirement and, thus, there can be no violation of the "without authorization" provision. This, however, does not mean that entities are left without any protections for information they choose to make publicly available, it just means that the CFAA should not be the protection.

Recently, the Eleventh Circuit had to address the issue of whether scraping publicly available information can constitute theft of trade secrets in *Compulife Software, Inc. v. Newman*.[69] The court held that bots that scrape publicly available information on a website may constitute trade secret misappropriation.[70] Compulife Software is a company that obtains publicly available rate tables from insurance companies, compiles them into a database, and then licenses access to the database for a fee to certain entities.[71] The defendants hired a "hacker" to use a bot to scrape the publicly available data from their website and generate their own insurance quotes.[72] Without diving too deeply into the court's analysis, the Eleventh Circuit found that, under Florida's trade secret laws, if publicly available information can amount to a trade secret (i.e. a unique compilation), then scraping that information could constitute trade secret theft.[73] The Supreme Court is currently contemplating granting cert for this case. Although the author is critical of expanding trade secret protection, this would seem to be the far more appropriate way to protect publicly available information than the CFAA. Expanding trade secret protection to scraping by bots would allow courts to comfortably narrow the scope of the CFAA while still providing public information sharers a way to monitor how that information is used and accessed. Trade secret protection as a means to regulate publicly available information would allow information providers peace of mind as to providing free access while eliminating the potentially catastrophic consequences of allowing entities to use the CFAA to regulate use of public information.

---

69. Peter J. Toren, *A Dubious Decision: Eleventh Circuit Finds Scraping of Data from a Public Website Can Constitute Theft of Trade Secrets (Part I)*, IP WATCHDOG (July 2, 2020) https://www.ipwatchdog.com/2020/07/02/dubious-decision-eleventh-circuit-finds-scraping-data-public-website-can-constitute-theft-trade-secrets-part/id=123029/.

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.*

VI. CONCLUSION

The Ninth Circuit interpretation of the "without authorization" provision of the CFAA in the case of *hiQ Labs* has the potential to mark a substantial reduction in the breadth of the statute. The *hiQ Labs* ruling indicates a shift in ideology to cut the CFAA down in order to bring the statute in line with its original intent of combating computer hacking. Although this interpretation is only binding under the Ninth Circuit's jurisdiction, this is hardly the only litigation pending concerning the breadth of the CFAA. As of writing, LinkedIn has appealed the decision. It appears as if the *hiQ Labs* court's interpretation of "without authorization" is just the beginning in what will be a constant back and forth between information owners and information seekers as each side tries to manipulate the CFAA in their favor.

It would not be surprising to see other circuits follow the Ninth Circuit rationale and limit CFAA interpretation on a national scale. As the scope of the CFAA is diminished, however, it will not be rendered obsolete. The CFAA was enacted as a broad piece of legislation and, as cyber technology advanced, the CFAA developed into an abusive tool covering a wide range of computer activities that were not originally contemplated by the CFAA. Shrinking applicability of the CFAA puts an affirmative obligation on entities to take steps to protect their information in ways that will bring any unauthorized intrusion by third parties within the scope of CFAA Section 1030(a)(2)(c).

As this could be argued as unfair to those that are now required to implement additional mechanisms to protect their information, this requirement brings the CFAA closer to its original intention of being an anti-hacking statute. Furthermore, it is hard to find inequity in requiring an entity to take precautions to protect something that it purports to own rather than relying on a statute. This is not to say that entities are left without remedy when their information is taken or used without their permission, only that this act will only fall under the scope of the CFAA under certain circumstances. In essence, entities will be forced to use extra care when deciding what information to make public. If the provider is concerned about how the information will be used, providers must implement proper safeguards to ensure that any taking or using of the information without permission would fall under the "without authorization" provision of CFAA Section 1030(a)(2)(c) and use the statute as a remedy. The legislators that introduced the CFAA surely did not intend for it to be used by entities providing public information as a weapon to regulate information use by criminalizing selective behaviors. The CFAA, although still useful, must be reeled in to more closely align with its intended purpose as a tool to prevent computer hacking.