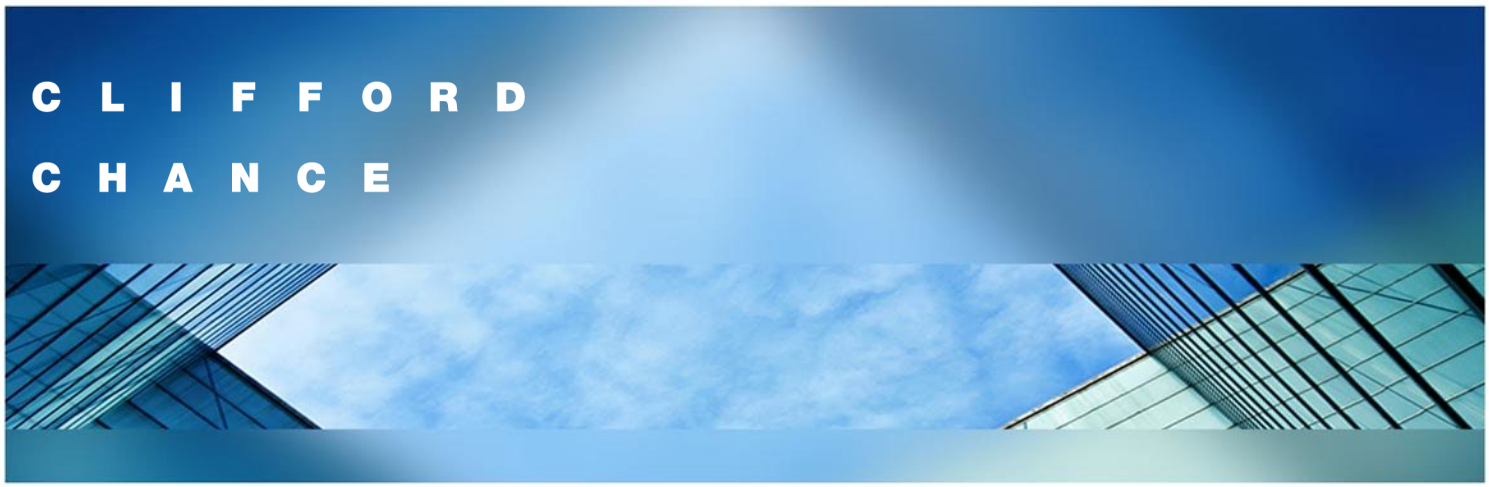

SCRAPING AWAY AT THE CFAA – THE SUPREME COURT'S INTERPRETATION OF "EXCEEDS AUTHORIZED ACCESS" LIMITS THE SCOPE OF THE STATUTE'S APPLICATION TO DATA SCRAPERS

In a long awaited decision that has a significant application for data scraping, the Supreme Court issued on June 3, 2021 its decision in *Van Buren v. United States*, significantly limiting the scope of the Computer Fraud and Abuse Act ("CFAA") by holding that users who access information that they are entitled to obtain but use that information for improper purposes do not violate the statute. The majority opinion adopted a narrow interpretation of the statute that will make it more difficult to pursue both civil and criminal actions based on alleged misappropriation of data.

This decision will likely limit the liability of companies that engage in data scraping. Data scraping is the use of software to harvest automatically, or "scrape", publicly available data from online sources. Scraped data can then be stored, copied or analyzed for various purposes, such as cataloging email addresses or photographs, or comparing pricing information. Prior to *Van Buren*, there was a circuit split regarding the application of the CFAA to data scrapers. Some circuits found no violation of the CFAA when the scraped information was publicly available, while others held that a violation could be established if data scraping was prohibited by a website's terms of use. At the time of the Supreme Court's decision in *Van Buren*, there was a petition for cert pending before the Court in *hiQ Labs, Inc. v. LinkedIn Corp*. asking the Court to resolve the split as it related to data scraping. In that case, the Ninth Circuit held that hiQ had not violated the CFAA when it scraped data from LinkedIn because LinkedIn's site is public. Soon after the *Van Buren* decision, the Supreme Court remanded the *LinkedIn* case back to the Ninth Circuit with instructions to reconsider in light of *Van Buren*. This remand suggests that the Supreme Court agrees with the Ninth Circuit that data scrapers are immune from liability under the CFAA when they gather publicly accessible data from websites, even if that activity is prohibited by the website's terms of use.

Background of *Van Buren*

Congress passed the CFAA in 1984, providing for criminal and civil liability for users who access computers either without authorization or in a manner that exceeds their authorization. Over the years, many have criticized the law as poorly drafted,[1] and there has been extensive litigation regarding its scope.

In *Van Buren*,[2] the government brought a CFAA prosecution against a Georgia police officer who took a bribe to run a license plate check. While the officer was entitled to use the relevant database to run license plate checks, he clearly violated departmental policy, which authorized him only to run checks for valid law enforcement purposes. The government advocated a broad reading of the phrase "exceeds authorized access" and argued that the CFAA prohibits impermissible use of information even when access to that information is lawful.[3] Justice Barrett, writing for the majority, rejected this view because it "incorporate[d] purpose-based limits" into this phrase without any textual basis.[4]

Significantly, the statute defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"[5] (emphasis added). Justice Barrett focused on the word "so" in the statute and framed the dispute as whether Van Buren was "entitled so to obtain" the license plate information. Justice Barrett reasoned that the government's interpretation would make the phrase cover "information one was not allowed to obtain in the particular manner or circumstances in which he obtained it."[6] Justice Barrett examined the structure of the statute, and endorsed Van Buren's position that "the phrase 'is not entitled so to obtain' …refers to information that one is not allowed to obtain *by using a computer that he is authorized to access*"[7] (emphasis in original).

In addition to focusing on the text, the Court also discussed policy concerns and the practical implications of the government's broader reading of the statute. The Supreme Court cited a mundane example of employees using a work computer for a personal purpose, such as sending a personal email, to illustrate how a broad interpretation "would attach criminal penalties to a breathtaking amount of commonplace computer activity."[8] The Court concluded that this would criminalize every violation of a computer-use policy.[9]

Justice Thomas dissented, with the Chief Justice and Justice Alito joining, arguing that the statute applied when persons used computers for improper reasons.[10] The examples cited in the majority opinion did not persuade Justice Thomas, who

---

1 Grant Burningham, *The Most Hated Law on the Internet and Its Many Problems*, NEWSWEEK, Apr. 16. 2016; Justin Peters, *Congress Has a Chance to Fix Its Bad "Internet Crime" Law*, SLATE, Apr. 24, 2015, available at https://slate.com/technology/2015/04/aarons-law-why-its-needed-to-fix-the-horrendously-bad-cfaa.html.; Ron Wyden United States Senator for Oregon, Wyden Statement on SCOTUS Van Buren v. United States Decision, Jun. 3, 2021, available at: https://www.wyden.senate.gov/news/press-releases/wyden-statement-on-scotus-van-buren-v-united-states-decision.

2 *Van Buren v. United States*, No. 19-783, 2021 U.S. LEXIS 2843 (June 3, 2021).

3 Brief for the United States, *Van Buren*, 2021 U.S. LEXIS 2843, at 18-21 (Aug. 27, 2020).

4 *Van Buren*, 2021 U.S. LEXIS 2843, at *16, 24.

5 18 U.S.C § 1030 (e)(6).

6 *Van Buren*, 2021 U.S. LEXIS 2843, at *15.

7 *Id*. at *17.

8 *Id*. at *28.

9 *Id*.

10 *Id*. at *33-48.

dismissed the majority's concern that the statute would criminalize an overbroad swath of conduct since "[m]uch of the Federal Code criminalizes common activity."[11] He opined that "[i]t is understandable to be uncomfortable with so much conduct being criminalized, but that discomfort does not give us authority to alter statutes."[12]

CFAA and Data Scraping

In the context of data scraping, some circuits have taken a narrow view of the scope of the CFAA to find data scraping unlawful only when the activity circumvented technical measures to access restricted data. Most notably, the Ninth Circuit held in *LinkedIn* that hiQ did not violate the CFAA because scraping publicly available information did not exceed authorized access.[13] The Second and Fourth Circuits also agreed with this approach. Other circuits, however, have taken a broad view of the statute and focused on whether the use of data is against the host website's terms of use. For example, the First Circuit squarely held that a "lack of authorization could be established by an explicit statement [by the website] restricting access."[14]

LinkedIn filed a petition for cert before the Supreme Court ahead of the *Van Buren* decision. The Ninth Circuit, when it first considered the case, held in favor of hiQ, which argued LinkedIn cannot rely on the CFAA to prevent a competitor from accessing information that is publicly available for anyone with a web browser.[15] The *Van Buren* and *LinkedIn* cases address different prongs of the CFAA, with *Van Buren* focusing on the "exceeds authorized access" prong and *LinkedIn* focusing on the "without authorization" prong. Nonetheless, the *Van Buren* opinion likely means the Ninth Circuit will again find for hiQ, because the Supreme Court's remand indicates that it's interpretation of "exceeds authorized access" directly bears on the meaning of the "without authorization" prong.

LinkedIn, apparently recognizing the challenging terrain set out for CFAA claims in the *Van Buren* opinion, argued in a supplemental brief filed shortly after the *Van Buren* opinion that the Supreme Court did not conclusively resolve the question of what constitutes accessing a site without authorization.[16] Indeed, the *Van Buren* majority noted that: "we need not address whether this inquiry turns only on technical (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[17] Nonetheless, the Supreme Court's remand suggests that it believes it has given the circuits sufficient guidance on the CFAA to resolve the pending split.

While the *Van Buren* decision did not directly address data scraping, it signals that the Supreme Court would likely be unsympathetic to arguments that the CFAA reaches the alleged misuse of data by scrapers who compile publicly available information from websites. Justice Barrett criticized the government's expansive reading of the statute, noting that the government's approach could result in the

11 *Id*. at *50.
12 *Id*.
13 938 F.3d 985 (9th Cir.2019).
14 *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62-63 (1st Cir. 2003).
15 *LinkedIn*, 938 F.3d 985.
16 *LinkedIn Corporation v. HiQ Labs, Inc.*, No. 19-1116 (Supplemental Brief for Petitioner filed Jun. 7, 2021).
17 *Van Buren*, 2021 U.S. LEXIS 2843, at *24 n.8

criminalization of "everything from embellishing an online-dating profile to using a pseudonym on Facebook."[18] Justice Barrett's reasoning will bolster the arguments of hiQ and others that data scraping does not constitute a violation of the CFAA.

Looking Ahead

Under *Van Buren*, as long as a data scraper relies on publicly accessible information, it is unlikely that a violation of a website's terms of service will constitute a civil or criminal violation of the CFAA. However, websites on the receiving end of scraping can still set up technical barriers to prevent scraping and contravention of those barriers could potentially constitute a CFAA violation if the activity results in unauthorized access to the site. Further, even without the CFAA, websites that are targeted for scraping may still pursue actions against data scrapers based on contract, tort and intellectual property law claims.

[18] *Id.*, at *29.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Chris Morvillo
Partner

T +1 212 878 3437
E christopher.morvillo
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

E. Carlisle Overbey
Associate

T +1 212 878 8504
E carlisle.overbey
@cliffordchance.com

Alex Sisto
Associate

T +1 212 878 4990
E alex.sisto
@cliffordchance.com

Gege Wang
Associate

T +1 212 878 8106
E gege.wang
@cliffordchance.com