BCLP. Client Intelligent

Insights

SUPREME COURT CLARIFIES THAT VIOLATION OF COMPUTER USE POLICY DOES NOT VIOLATE COMPUTER FRAUD AND ABUSE ACT

Jun 10, 2021

SUMMARY

Resolving a circuit split in the interpretation of the federal Computer Fraud and Abuse Act of 1986 (CFAA) – an anti-hacking statute – the Supreme Court recently held that the CFAA does not impose liability on individuals who access information they are otherwise authorized to access even though they have improper motives.

In *Van Buren v. United States*, Nathan Van Buren, a former Georgia police sergeant, was caught in an FBI sting operation running license-plate searches in exchange for cash payments via his patrol-car computer. Although Van Buren was authorized to run license-plate searches, it was a clear violation of department policy to conduct searches for other than law enforcement purposes. Federal prosecutors charged Van Buren with a felony under the CFAA, which subjects to criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access," and thereby obtains computer information. 18 U.S.C. § 1030(a)(2). Prosecutors claimed that by accessing the license plate database for purposes that violated department policy, Van Buren had "exceeded authorized access" and violated the CFAA. Van Buren was convicted and sentenced to 18 months in prison by the district court.

On appeal, the Eleventh Circuit affirmed. Although several Circuits have read the "exceeds authorized access" language of § 1030(a)(2) to apply only in situations in which individuals access "information to which their computer access does not extend," the broader view embraced by the Eleventh Circuit also encompasses "those who misuse access that they otherwise have." Thus, courts have held that an employee who violates an employer's computer use policy to access user account information, *United States v. John*, 597 F.3d 263 (5th Cir. 2010), a former employee who used a web "scraping" tool to extract publicly accessible information from his former employer's website contrary to a broad confidentiality agreement, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), and a former employee who used secure deletion software to wipe a laptop

before returning it to his employer, *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), violated the "exceeds authorized access" provision of the CFAA.

In a 6-3 decision, the Supreme Court reversed, holding that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him."

Justice Barrett, writing for the majority, began, as expected, with a textualist analysis supported by various dictionary definitions, but perhaps most compellingly, concludes by noting:

> To top it all off, the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity…. If the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA. Or consider the Internet. Many websites, services, and databases—which provide "information" from "protected computer[s]," § 1030(a)(2)(C)—authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers.

In so holding, the Supreme Court provides some welcome clarity into an area that was fraught with ambiguity. At the same time, the decision also removes a powerful arrow from the quiver of companies seeking to deal with rogue employees or aggressive competitors who seek to use the company's data or website to glean information helpful to their cause.

For more detailed advice regarding the implications of the decision, please contact Daniel Rockey at daniel.rockey@bclplaw.com or Sam Garner at sam.garner@bclplaw.com.

RELATED CAPABILITIES

- Appellate
- Data Privacy & Security

MEET THE TEAM

Daniel T. Rockey

San Francisco

daniel.rockey@bclplaw.com
+1 415 268 1986
