Exceeding Authorized Access Under the Computer Fraud and Abuse Act
An appeal pending at the U.S. Supreme Court should resolve the issue of whether employee action exceeding access authorization will implicate the CFAA. Regardless of the ruling, employers can and should take certain steps.

By Michelle A. Schaap and Gregory D. Green – Chiesa Shahinian & Giantomasi PC
November 24th, 2020

The United States Supreme Court has granted certiorari in Van Buren v. United States, a case which deepened the federal circuit court split regarding the extent to which the Computer Fraud and Abuse Act ("CFAA") covers an employee's alleged misappropriation of information from the employer's systems where the employee otherwise had authorized access. This pending appeal should resolve the issue of whether employee action exceeding access authorization will implicate the CFAA. Regardless of the ruling, employers can and should adopt written policies, impose contractual restrictions, and implement technology to protect valued systems and information.

The Circuit Split – "Exceeding Authorized Access"

A Broad Interpretation

The First, Fifth, Seventh and Eleventh Circuits have embraced a broad approach when finding a violation of CFAA where an employee misuses information they otherwise have permission to access and that misuse violates the employer's policies and/or confidentiality agreement.

The Eleventh Circuit in Van Buren ruled that the CFAA "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 accessor is not entitled [so] to obtain or alter." 940 F.3d 1192, 1207 (11th Cir. 2019), cert. granted, 206 L. Ed. 2d 822 (Apr. 20, 2020). In Van Buren, the Court held that defendant "exceeded his authorized access and violated the [computer-fraud statute]" when he used the Police Department systems to obtain what he thought was an exotic dancer's personal information for a nonbusiness reason. Id. The Court expressly rejected defendant's argument that he was innocent of computer fraud and did not exceed his authorized access because he accessed only databases that he was authorized to use, even though he did so for reasons wholly outside the scope of his duties. Id.

Similarly, in EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001), the First Circuit held that the use of a scraper software program to systematically and rapidly glean prices from a company's website in order to allow systematic undercutting of those prices "exceeded authorized access" within the meaning of the CFAA. In reaching its decision, the Court pointed to an all-encompassing confidentiality agreement, signed by the former EF employee, which prohibited the defendant from disclosing information considered contrary to his former employer's interests. Id. at 582-84.

Under a broad interpretation of the CFAA, a cause of action arises when an employee acts without authorization or exceeds his authority whenever the employee permissibly acquires computer information and then uses the information in a manner adverse to his employer's interest or breaches an obligation owed to the employer.

A Narrower Analysis

In determining whether a violation of the CFAA has occurred, the Second, Fourth, Sixth, and Ninth Circuits, however, have adopted a narrower view, which focuses on the measures implemented by an entity to prevent a defendant from accessing information -- not the defendant's misuse of the information.

The Ninth Circuit, in hiQ Labs, Inc. v. LinkedIn Corp., recently held that the rule of lenity dictates a narrow interpretation of "without authorization" in the CFAA. 938 F.3d 985, 1003 (9th Cir. 2019). The Court observed that the "CFAA's prohibition on accessing a computer 'without authorization' is violated 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." Id. The Ninth Circuit's decision in hiQ Labs, Inc. v. LinkedIn Corp. rested on the analysis of prior cases, including United States v. Nosal, where it held that the term "exceeds authorized access" is limited to violations of restrictions on access to information, and not restrictions on the information's use – or misuse. 676 F.3d 854, 863–64 (9th Cir. 2012). For this reason, a former employee's accomplices, who accessed information using valid credentials for an improper use, did not exceed authorized access, even though the company's policies prohibited the disclosure of confidential information. Id.; see also WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205-06 (4th Cir. 2012) (a departing employee did not exceed authorized access by downloading confidential information to a personal computer in violation of company policy because the employee was authorized to review the material in question.).

Similarly, the Second Circuit reversed the conviction of a police officer who accessed a restricted database without a legitimate purpose because he was otherwise authorized to access the database. United States v. Valle, 807 F.3d 508, 523 (2d Cir. 2015). The Second Circuit expressly acknowledged that, as with Van Buren, defendant accessed a database with no law enforcement (or business) purpose. The court found, however, that the *purpose was irrelevant* where the employee had access even though written policies proscribed the usage at issue. Consistent with the rule of lenity, prior legislation considered by the court included the following language, which was excluded from the current law: "accessed a computer with authorization…for purposes to which such authorization does not intend." Id. at 521 – 522.

New Jersey State Law

The New Jersey Trade Secrets Act ("NJTSA"), adopted in 2012, is similar to the Uniform Trade Secrets Act ("USTA") and codifies the existing common law protections for employers' trade secrets. However, for the purposes of "exceed authorized access," the

NJTSA expands on the UTSA's definition of "improper means" by adding that it is improper to obtain a trade secret by using: (1) unauthorized access; (2) access that exceeds the scope of authorization; and (3) other means violating a person's rights under New Jersey law. N.J.S.A. 56:15-2. Similarly, the New Jersey Computer Related Offenses Act ("CROA") also prohibits a person from purposefully or knowingly without authorization "altering, damaging, taking, or destroying any data, database, computer program, computer software, internal or external computer equipment, computer system, or computer network. N.J.S.A. 2A:38A-3.

Although New Jersey courts have not yet interpreted the phrase "exceed authorized access" in the NJTSA, the courts have considered the issue in the context of a criminal statute. In 2014, a New Jersey court held that computer crime laws may apply to employees who exceed the scope of their authority in the use of their password-protected access to their employer's computer systems. State v. Thompson, 444 N.J. Super. 619, 633, 135 A.3d 166, 174 (Law. Div. 2014). In that case, the Court noted that, while there has been divergence among the federal circuits regarding the interpretation of the term "exceeds authorized access," an allegation that defendants acted outside the scope of their employment when they accessed other employees' e-mails supports an indictable offense under New Jersey Computer Criminal Activity Law. Id.; N.J.S.A. 2C:20-25.

Employers Can Proactively Defend Themselves in the Face of Uncertain CFAA Enforcement

Given the uncertainty of the Supreme Court's interpretation of "access" with regard to employees' misuse of their access credentials, employers should take measures to protect and secure their proprietary information and systems, particularly if the employer is in a Circuit that has taken the more narrow reading of the CFAA. The following are examples of measures to protect a businesses' data and information:

1. Implement "least rights" access controls by limiting the systems particular employees have access to.
2. Require confidentiality and non-disclosure agreements where employees agree to protect and secure company systems and assets. "Confidential information" should include an entity's systems and access credentials in addition to the other traditional information protected by such agreements (trade secrets, customer lists, etc.). These agreements should also address ownership of the employer's social media accounts. A carefully crafted agreement should mandate the return of confidential information as well as the delivery of all personal devices used to access any confidential information to ensure the permanent removal of that information from such devices.
3. Promulgate "acceptable use" policies to clearly state that employer systems and the data housed on those systems are for company use only, and should never be accessed, copied or removed for an employee's own benefit or the benefit of any third party.

4. Distribute policies proscribing (a) the exfiltration, duplication and/or removal of any confidential information with any removable media (such as a USB drive); and (b) the transfer of any company information to a personal cloud account or personal hard drive.

5. All policies should clearly state that employees have no expectation of privacy in connection with the use of any company systems, whether use and access is on a company or personal device.

6. Where employees are permitted to access company resources through personal devices, the company should deploy mobile device management (MDM) technology to ensure the company can remotely wipe company data from those devices if they are lost, stolen or the employee leaves the company for any reason.

7. If an employee is on a leave of absence, employers should suspend access credentials during the leave. If an employer plans to terminate an employee, access credentials should be terminated concurrently with the termination of employment.

8. Deploy technology and monitoring systems to detect large downloads of company data or other unusual online or system behavior.

With these written policies, contractual undertakings and technology solutions, an employer can protect the proverbial keys to the kingdom from unauthorized access and misuse of access authorization regardless of the fate of the CFAA.

Michelle A. Schaap is a member with Chiesa Shahinian & Giantomasi PC and is the founder of the firm's Privacy & Data Security Group. Gregory Green is an Associate with the firm's Employment Group.