

Whistleblowers Accessing Company Documents Likely Will Not Be Prosecuted Under the Computer Fraud and Abuse Act

By [Nicolas Enrique O'Connor](#)

August 16, 2021

Until recently, logging onto Facebook a few too many times on a work computer could not only get workers fired but also theoretically land them in prison for up to 10 years if they were prosecuted under the Computer Fraud and Abuse Act ("CFAA"). Workers who push the envelope on conducting personal business on company property will be relieved to hear that, although their employers may still penalize their misconduct, they will not be prosecuted under the CFAA. On June 3, 2021, the Supreme Court in a 6-3 decision overturned the CFAA conviction of Nathan Van Buren, a former Georgia police officer who accepted \$5,000 in exchange for searching the Georgia Crime Information Center database to see if an exotic dancer was actually an undercover police officer. [Van Buren v. United States](#), 141 S.Ct. 1648 (2021). Van Buren's accepting a bribe to abuse his authorized computer access was a serious violation of the public trust and was separately prosecuted as honest-services wire fraud, but his conviction under the criminal statute prohibiting the acceptance of bribes was overturned on separate grounds. In this case the Court recognized that prosecuting that same reprehensible conduct under the CFAA would pose a serious risk to average Americans engaging in commonplace personal business on their employer's computer, such as "embellishing an online-dating profile," "using a pseudonym on Facebook," or "checking sports scores or paying bills." *Id.* at 1661-62.

Although the Court did not mention it, the threat of litigation – and even prosecution – under the CFAA has been used as a tool to deter whistleblowers and other potential claimants from collecting the documents and information necessary to prove that their employer had engaged in fraud or violated their rights. The Court's rejection of the broad application of the CFAA urged by the government should reassure whistleblowers that their employers will have a much more difficult time using the CFAA to chill whistleblowing activity.

Circuit Split on Computer Fraud and Abuse Act

The CFAA, which was enacted in 1986, is generally used by the government to prosecute hacking attempts, the most obvious form of unauthorized access, and in this regard the law has been both successful and useful. However, part of the CFAA covers individuals who "access a computer without authorization and use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Determining the bounds of when an individual "exceeds authorized access" in a way that triggers the CFAA gave rise to a circuit split: The First, Fifth, Seventh, and Eleventh Circuit Courts held that accessing a computer with authorization but for an improper purpose

(e.g. a police officer running a background check on her daughter's boyfriend) is a violation of the CFAA. The Second, Fourth, and Ninth Circuit Courts opted for a narrower interpretation, holding that an individual exceeds authorization only when she accesses information which she was prohibited from accessing (e.g. a police officer borrowing a coworker's credentials to access an evidence log).

Supreme Court Sides with Broader Interpretation of Computer Fraud and Abuse Act

In a majority opinion written by Justice Amy Coney Barrett, the Supreme Court sided with the Second, Fourth, and Ninth Circuits and advocates opposing the broader interpretation. The Court held that inclusion of the word "so" in the statutory definition of "exceeds authorized access" means that "the phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." *Van Buren*, 141 S.Ct. at 1654-55 (analyzing the word "so").

After dispensing with the government's arguments about the definitions of "entitled" and "so," the Court concluded that the criminalization of a wide range of commonplace computer activity illegal under the government's interpretation "underscores the implausibility" of that interpretation. *Van Buren*, 141 S.Ct. at 1661-62. The CFAA was not intended to criminalize actions such as checking personal emails on a company computer, and allowing prosecutions for an improper use of one's authorized access would potentially criminalize these normal, even if improper, uses of a company computer. In a dissent, Justice Clarence Thomas, joined by Chief Justice John Roberts and Justice Samuel Alito, homed in on the definition of "entitled" and concluded that the plain language of the CFAA was broad enough to encompass these commonplace computer activities. *Van Buren*, 141 S.Ct. at 1664 (Thomas, J. dissenting). Justice Thomas further commented that shock at the amount of conduct criminalized does not entitle the Court to rewrite a statute. *Id.* at 1668-69 (Thomas, J. dissenting).

Ruling Protects Whistleblowers Who Collect Evidence in Claims Against Employers

This decision not only protects the average American from overzealous prosecutors and vindictive employers but also provides protection for whistleblowers and other employees with claims against their employers. Making any sort of claim against an employer – discrimination, retaliation, or unpaid wages – requires that the employee collect evidence to support the claim, and whistleblowers who intend to file an SEC tip or initiate a [qui tam lawsuit](#) under the False Claims Act need to acquire evidence to prove the fraud on which they will be reporting. It is well established that whistleblowers, particularly those reporting on fraud, can take from their employers the documents necessary to prove the fraud and make their case, *see, e.g., U.S. ex rel. Yesudian v. Howard Univ.*, 153 F.3d 731, 740 (D.C. Cir. 1998) (citing plaintiff's collecting evidence and documentation as FCA-protected activity), but there has been an open question as to how much information is too much to take. *See, e.g., JDS Uniphase Corp. v. Jennings*, 473 F. Supp.2d 697, 703-704 (E.D. Va. 2007) (applying California law) (holding that SOX "is not a license to steal documents and break contracts," that document copying and transmission must be reasonable under the circumstances to be protected under [SOX](#), and that a showing that the documents would have been destroyed would demonstrate reasonableness); *Xyngular Corporation v. Schenkel*, 200 F. Supp.3d 1273, 1318 (D. Utah 2016) (finding that defendant's "willful and improper acquisition of documents

to support his claims in anticipated litigation is not immunized by separate whistleblowing activity”).

Prior to the decision in *Van Buren*, in addition to leaning on trade secrets laws, employers could file counterclaims against whistleblowing plaintiffs under the CFAA, alleging that those whistleblowers “exceeded their authorized access” when taking documents. See *Siebert v. Gene Security Network, Inc.*, 2013 WL 5645309 (N.D. Cal. Oct. 16, 2013) (citing *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) and dismissing counterclaim for exceeding authorized access); *Erhart v. Bofi Holding, Inc.*, 387 F.Supp.3d 1046 (S.D. Cal. 2019) (questioning whether employee had authorized access); see also *Ahlers v. CFMOTO Powersports, Inc.*, 2014 WL 2574747 (D. Minn. June 9, 2014); *Direct Supply, Inc. v. Pedersen*, 2011 WL 1131092 (E.D. Wis. March 28, 2011). By threatening or filing a CFAA counterclaim, employers could chill whistleblowing since not only has the whistleblower lost her job due to her protected activity but also might face legal liability for attempting to collect sufficient evidence to prove her claim.

Ruling Provides Limitations for Counterclaims Against Whistleblowers

Van Buren removes the CFAA from the tool belt of retaliating employers. While trade secrets laws still provide employers a robust defense against employees who seek to misappropriate their former employers’ proprietary information for personal pecuniary gain, trade secrets laws apply in a much narrower set of circumstances than the “exceeds authorized access” portion of the CFAA. Without the limitations imposed by *Van Buren*, a whistleblower who mistakenly takes documents unrelated to her claim, despite having authorized access to those documents, could face liability since her employer could claim the documents were taken for an “improper” purpose. By limiting the CFAA to situations where an employee did not have any authorized access to the documents (e.g. borrowing a co-worker’s login information), the risk to a whistleblower of finding herself in unanticipated litigation related to her efforts to gather evidence is substantially reduced.

What Whistleblowers Need to Know When Gathering Evidence of Criminal Conduct

Because *Van Buren* applies to both criminal and civil causes of action, not only does this ruling help protect whistleblowers in the private sector, but it also helps government whistleblowers who fear prosecution for taking government documents to expose governmental improprieties. The government is not stymied in its ability to prosecute illegal, non-whistleblowing conduct. The government can still levy charges for wire fraud and honest services fraud, as it did in the *Van Buren* case. What this means is that the government can still prosecute government officials who abuse their authorized governmental access for personal gain.

Potential whistleblowers – or anyone seeking to bring claims against her employer – ought to note that, while *Van Buren* may protect against an employer’s suing an employee for improperly using their authorized access, it does not stop such an employer from terminating an employee for that improper use, especially if it violates the stated policies of the company. Even if the termination is proven to be for unlawful, discriminatory reasons, the “after acquired evidence” doctrine may limit an employee’s recovery for a wrongful termination claim if the employer, after illegally terminating an employee, learns that she

had improperly used company property, and it can prove that it would have terminated her for that reason if it had known of her misconduct. See *McKennon v. Nashville Banner Pub. Co.*, 513 U.S. 352 (1995).

While employees with claims against their employers still face obstacles to pursuing their claims free of the risk of their employers' counterclaims, *Van Buren* eliminates a key barrier to ensuring justice for those whose rights have been violated and to battling fraud perpetrated upon investors, the government, and the public at large.