Data Privacy and Cybersecurity

DOJ Revises CFAA Charging Policy to Provide Clarity for Cybersecurity Research and Terms of Use

By: David Bitkower, Aaron R. Cooper, Shoba Pillay, and Ashwini Bharatkumar

On May 19, 2022, the Department of Justice (DOJ) issued revisions to its existing policy for charging offenses under the Computer Fraud and Abuse Act (CFAA) (2022 CFAA Policy).[1] The revisions state that "good-faith" security research will not be charged as a criminal CFAA violation. Comments accompanying the revised policy statement also highlight the importance of technical barriers—in addition to contractual limits—to determinations of when access exceeds authorization. Although the announcement regarding security research made a splash in the press, it is unclear to what degree the policy represents a change in how DOJ will approach cases. Nor can security researchers rely on the guidance for concrete assurances against liability, because the policy revision has no effect on civil CFAA liability or state laws that provide for criminal or civil liability for unauthorized access to computer systems. The revision may also introduce uncertainty for system owners, who may be left wondering how the new policy will be applied, and how federal law enforcement will react to conduct viewed by some as good-faith research and by others as in a gray area.[2]

The Policy's Background

The 2022 CFAA Policy updates a 2014 policy that outlined the factors DOJ considered when charging CFAA violations. A point of tension recurring both before and after introduction of the 2014 policy has been the theoretical applicability of the CFAA to legitimate work by computer security researchers, and more generally whether DOJ would prosecute violations of a website's terms of service or data use policies under the CFAA's "exceeds authorized access" prong.

Although DOJ does not have a regular practice of charging security researchers criminally (despite some controversial matters), to address concerns about security research-related liability, the 2014 charging policy required DOJ prosecutors to consult with its Computer Crime and Intellectual Property Section before initiating any charges under the "exceeds authorized access" prong of the CFAA, observing that "[c]ases under the CFAA are often complex, and analysis of whether a particular investigation or prosecution is warranted often requires a nuanced understanding of technology, the sensitivity of information involved, tools for lawful evidence gathering. . . ."[3] The 2014 policy outlined several factors to guide DOJ's assessment of whether such a prosecution should be initiated. A comment to the policy explained special factors that DOJ would consider in charging "exceeds authorized access" cases, including: "if the defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website, federal prosecution may not be warranted."[4]

Despite the policy, researchers continued to assert that DOJ's interpretation of the CFAA is overly broad and creates a chilling effect on their work. Most recently, in an *amicus* brief submitted to the Supreme Court in *Van Buren v. United States*, cybersecurity researchers argued that, under an interpretation of the CFAA that would prohibit accessing a computer for an unauthorized purpose (in that case, a police officer accessing a license plate database to sell non-public information), "standard security research practices—such as accessing publicly available data in a manner beneficial to the public yet prohibited by the owner of the data—can be highly risky."[5] Thus, the argument went, "the government's reliance on this broad interpretation of the statute conditions security improvements on

researchers' tolerance of the risk of being sued or prosecuted for reporting vulnerabilities."[6]

As noted in Jenner & Block's client alert on the *Van Buren* decision, the Court ultimately ruled against DOJ and in favor of the police officer (and following the analogy in the *amicus* brief, in favor of computer security researchers): the Court held that accessing data a person is authorized to access, but for an improper purpose, does not violate the CFAA. Rather, authorization is a "gates-up-or-down" inquiry; either a person has authorization to access a computer or a part thereof, or they do not. However, the *Van Buren* decision left open the question of whether this "gates-up-or-down" inquiry requires the existence of a technical barrier, like a username and password, or whether a "gate" can be based on limits imposed solely by contract or policy.

The 2022 CFAA Policy

The May 19, 2022 policy update makes two notable changes. First, the DOJ policy now expressly includes good faith computer research amongst the factors considered when determining whether to authorize prosecution of a CFAA violation. Specifically, the updated policy states that DOJ should not pursue prosecution if a "defendant's conduct consisted of, and the defendant intended, good-faith security research."[7] The policy adopts the US Copyright Office's definition of "good-faith security research," which is:

> accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.[8]

Deputy Attorney General Lisa O. Monaco commented that the policy statement revision "promotes cybersecurity by providing clarity for good-faith security researchers who root out vulnerabilities for the common good."[9] She added that merely claiming that research is being conducted in "good faith" does not provide "a free pass," and DOJ said that it would scrutinize whether conduct is consistent with a claim of good faith security research purposes. Certain conduct, such as identifying vulnerabilities for the purpose of extorting system owners, will obviously fall outside the exception. But it remains unclear where DOJ will draw the line in harder cases.

Second, the policy addresses how terms of service versus digital barriers will be treated—an issue the *Van Buren* decision left undecided. With respect to contractual terms, the policy underscores that a defendant must act knowingly or intentionally, meaning that a defendant "was aware of the facts that made the defendant's access unauthorized at the time of the defendant's conduct." This awareness may be demonstrated via "the presence of technology intended. . . to limit unauthorized access."[10] It might also be demonstrated by "written or oral communications sent to the defendant that unambiguously informed him that he is not authorized to access a protected computer or particular areas of it."[11] In theory, this category includes a policy or contract. Or, "the defendant's own statements or behaviors reflecting knowledge that his actions were unauthorized" can demonstrate awareness.[12] The policy emphasizes that, in many CFAA prosecutions involving conduct exceeding authorized access, technical measures have been taken to protect information and "signal[] the importance or sensitivity of that information,"[13] suggesting this will be an important factor in DOJ's evaluation of any prosecution. At the same time, the technology need not create an "impenetrable 'technological barrier.'"[14]

However, with respect to information that is "available to the general public," the policy rejects CFAA violations based solely on contractual or terms of service restrictions:[15]

> A CFAA prosecution may not be brought on the theory that a defendant exceeds authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or web service available to the general public—including public websites (such as social-media services) that allow for free or paid registration without human intervention. . . However, an "exceeds authorized access" CFAA prosecution may be brought, for example, against a defendant who accesses a multi-user computer or web service, and is authorized to access only his own account on that computer or web service, but instead accesses someone else's account.

Implications

The policy statement's revisions provide some clarity on the nature of conduct likely to give rise to federal criminal prosecution under the CFAA. The policy's security research provision offers some transparency on how DOJ will treat "good faith" cybersecurity research efforts, and the comments indicate that terms of service and contractual provisions alone—absent technical measures underpinning such provisions—are unlikely to support charges of exceeding authorized access to publicly available information under the CFAA.

But the policy's definition of "good faith" leaves much to be determined. For example, the policy requires that a person act "solely for purposes of good faith" research; yet, how strictly DOJ interprets the word "solely," and whether it permits a secondary purpose, is unstated. In addition, the policy requires that the activity be "carried out in a manner designed to avoid any harm," but it does not specify whether such harm would include, for instance, viewing—and therefore violating the confidentiality of—sensitive personal information or intellectual property. The policy requires that the information gathered be "used primarily to promote the security or safety" of the system, but it does not identify a standard for determining when that is the case. While extortion is clearly not in "good faith," there are likely a variety of instances in which the boundaries between good faith research and less noble goals are blurred, and application of the policy is ambiguous.

We expect DOJ may be asked to specify some of those details. But even if DOJ does so, it is important to note that this charging policy only represents an expression of how DOJ expects to exercise its own prosecutorial discretion. The policy does not change the legal standard for a CFAA violation, including in civil suits, which may be an option for system owners even if DOJ declines to prosecute a case. Moreover, many states have criminal and civil laws analogous to the CFAA that do not depend on DOJ policy guidance.

Meanwhile, system owners may be left scratching their heads about some of the same questions: for example, if a person or company who accessed their data without authorization can plausibly claim to have done so in the name of good-faith research, will that affect the system owner's assessment of whether to report the conduct to law enforcement? Particularly at a time when DOJ has encouraged victims to come forward to reap the benefits of vigorous law enforcement (and has observed that victims too frequently do not do so)[16] the policy's mixed message may have unintended effects. Pending additional guidance, both system owners and prospective security researchers should consider ways to mitigate risk and make sure they are aware of the contours of civil liability and state statutes: those considering engaging in security research may be best served by ensuring they have sufficient understanding of the scope of any authorization and that they are prepared to point to facts establishing that their conduct constitutes good faith research, and system owners may want to evaluate their relative use of technical barriers and contract or policy to impose and clearly communicate access restrictions.

Contact Us

David Bitkower

dbitkower@jenner.com | Download V-Card

Aaron R. Cooper

acooper@jenner.com | Download V-Card

Shoba Pillay

spillay@jenner.com | Download V-Card

Ashwini Bharatkumar

abharatkumar@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card

Shoba Pillay
Co-Chair
spillay@jenner.com
Download V-Card

[1] *U.S. Department of Justice, Justice Manual, Title 9: Criminal, 9-48.00 – Computer Fraud and Abuse Act* 4 (2022), https://www.justice.gov/opa/press-release/file/1507126/download ("2022 CFAA Policy").
[2] *See, e.g., United States v. Auernheimer*, 748 F.3d 525, 530-31 (3d Cir. 2014).
[3] Memorandum from the Attorney General to the United States Attorneys and Assistant Attorney Generals for the Criminal and National Security Divisions, Intake and Charging Policy for Computer Crime Matters 5 (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download ("2014 CFAA Policy").
[4] 2014 CFAA Policy at 5.
[5] Brief of Amici Curiae Computer Security Researchers, Electronic Frontier Foundation, Center For Democracy & Technology, Bugcrowd, Rapid7, Scythe, and Tenable in Support of Petitioner at 5, *Nathan Van Buren v. United States*, No. 19-783 (July 8, 2020).
[6] *Id*. at 22– 23. *See generally id.* at 16–29.
[7] 2022 CFAA Policy at 4.
[8] *Id*. (citing U.S. Copyright Office, S*ection 1201 Rulemaking, Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention* (2021), https://cdn.loc.gov/copyright/1201/2021/2021_Section_1201_Registers_Recommendation.pdf.
[9] News Release, U.S. Department of Justice, *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act* (May 19, 2022), https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act#:~:text=Department of Justice Announces New Policy for Charging,that good-faith security research should not be charged.
[10] 2022 CFAA Policy at 5.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.* at 4.
[16] *See, e.g.*, Lisa O. Monaco, Deputy U.S. Attorney General, *Op-Ed: America Needs Congress's help to stop the ransomware threat*, CNBC (Oct. 6, 2021) ("Too often after a cyberattack, the victim company struggles with how, whether, and when to contact law enforcement. But if you have an intruder in your home you do not hesitate to call 911, and it is time to think about cyberattacks with the same instinctive response."). Federal legislation now requires the Department of Homeland Security to implement mandatory reporting requirements for cyber incidents by certain covered entities. *See* Jenner and Block's client alert on the Cyber Incident Reporting for Critical Infrastructure Act of 2022. In addition, on May 5, 2022, President Biden signed into law the Better Cybercrime Metrics Act, S. 2629, which is intended to help the federal government track, analyze, and prosecute cybercrime. *See* The White House Briefing Room, *Bills Signed: S. 233 and S. 2629* (2022), https://www.whitehouse.gov/briefing-room/legislation/2022/05/05/bills-signed-s-233-and-s-2629/.