Crowell

Client Alert

DOJ's Revised Prosecutorial Guidelines: The "Ethical" Hacker Exemption

June 3, 2022

For the first time in nearly a decade, the U.S. Department of Justice (DOJ) has revised its **prosecutorial guidelines** for bringing criminal charges under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. Under the revised guidelines, federal prosecutors should not pursue CFAA violations if available evidence shows an individual's conduct consisted of, and the defendant intended, "good faith security research." *See* Justice Manual (J.M.) § 9-48.000 (Revised CFAA Guidelines). These policy changes, effective immediately, provide some welcome clarity for so-called "white-hat" or "ethical" hackers, such as cyber researchers and penetration testers.

Why revise the Justice Manual now?

The CFAA has been on the books since 1986, and was enacted by Congress as a **direct response** to the classic hacker movie, *WarGames* (1983). The law's scope is exceptionally broad, criminally sanctioning most forms of unauthorized, intentional third-party access of any computer (including, for instance, any computer connected to the internet). It also created a private right of action for anyone who suffers significant damage or loss as a result of such unauthorized access.

The DOJ policy revision comes less than a year after the **Supreme Court narrowed** the scope of the CFAA, in the process rejecting DOJ's broad interpretation of what conduct can be charged criminally as "exceeding unauthorized access" under the statute. *Van Buren v. United States*, 141 S.Ct. 1648, 1662 (2021).This broad view was reflected in DOJ's **previous version** of the Justice Manual relating to the CFAA, issued in 2014.

In **announcing** its Revised CFAA Guidelines, DOJ emphasized that prosecutors should not bring charges under the CFAA for "good-faith security research." *See* DOJ Press Release (PR) No. 22-533. This revision memorializes the statement of Deputy Attorney General Lisa Monaco that the "department has never been interested in prosecuting good-faith computer security research as a crime." *Id.* The revised policy also instructs DOJ attorneys to "focus [] the department's resources on cases where a defendant is either not authorized at all to access a computer or . . . despite knowing about [a] restriction, accessed a part of [a] computer to which his authorized access did not extend." *Id.*

The "ethical" hacker exemption

The DOJ exemption for good-faith security research recognizes the substantial—and growing—**contributions of ethical hackers** to the broader cybersecurity community. Ethical hackers regularly help protect networks by simulating adversary tactics to identify vulnerabilities before threat actors do. Indeed, expert ethical hackers have recently **commanded large sums** for their services from tech companies.

The Revised CFAA Guidelines instruct DOJ attorneys to "apply the definition of 'good-faith security research' recommended by the Register of Copyrights" pursuant to 17 U.S.C. § 1201, part of the Digital Millennium Copyright Act (DMCA). J.M. § 9-48.000. Thus, "good-faith security research" means "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." *Id.*; *see also* Register of Copyrights,***Section 1201 Rulemaking***, at 258 (Oct. 2021).

What does this mean?

The Revised CFAA Guidelines provide that "[s]ecurity research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services—might be called 'research' but is not in good faith." J.M. § 9-48.000. To ensure uniformity of charging decisions, DOJ attorneys, including federal prosecutors at all U.S. Attorneys' Offices, must consult with DOJ's Computer Crimes and Intellectual Property Division prior to bringing criminal charges. *Id.*

The Revised CFAA Guidelines also partially adopt the Supreme Court's limitations of the CFAA articulated in the Court's 2021 *Van Buren* opinion—although DOJ did not cite *Van Buren* as the basis for the policy change. In *Van Buren*, the Court rejected DOJ's application of the CFAA's "exceeds authorized access" prong to conduct that violates "purpose-based limits contained in [private] contracts and workplace policies." 141 S.Ct. at 1662. The Court held that an individual does not criminally violate the CFAA merely by "obtain[ing] information" from a computer network in violation of a company's written "computer-use policy." *Id.* at 1659.

Implicitly addressing concerns articulated in *Van Buren* (*see* 141 S.Ct. at 1662), DOJ noted in its announcement that "hypothetical CFAA violations that have concerned some courts and commentators are not to be charged. Embellishing an online dating profile contrary to the terms of service of the dating website; creating fictional accounts on hiring, housing, or rental websites; using a pseudonym on a social networking site that prohibits them; checking sports scores at work; paying bills at work; or violating an access restriction contained in a term of service are not themselves sufficient to warrant federal criminal charges." PR 22-533.

However, DOJ preserved a "narrow exception" to this logic among its policy changes: violations of "contracts, agreements, or policies that entirely prohibit defendants from accessing particular files, databases, folders, or user accounts on a computer in all circumstances," and not just for certain uses, may still result in criminal charges under the CFAA. *See* "C. Comment," in J.M. § 9-48.000.

While *Van Buren* did not directly address the effect of such an agreement or policy (where users are "entirely prohibit[ed]" from accessing or using certain information), DOJ's exception may ultimately run afoul of the Court's overall logic. In *Van Buren*, the Court cautioned that it "would inject arbitrariness into the assessment of criminal liability" if government attorneys chose to interpret "purpose-based limits on access" only in access-related terms, as opposed to their applicable use-based terms. 141 S.Ct. at 1662. If an authorized computer user

is practically able to access certain off-limits information, then private policies "entirely prohibit[ing]" such access would arguably be purpose-based, not access-based, restrictions.

Moreover, the Revised CFAA Guidelines apply only to DOJ decisions to bring criminal charges. They do not impact theories of civil liability under the CFAA.

Takeaways

While the DOJ policy changes regarding criminal CFAA charges are groundbreaking from an enforcement perspective, they do not constitute a change in the CFAA itself, and, therefore, do not create any new rights. While DOJ attorneys are bound to follow the Justice Manual—including the Revised CFAA Guidelines—when considering potential criminal CFAA charges, any given prosecutor may see facts and circumstances differently than even the most well-intentioned of security researchers. The CFAA will continue to be a complicated and nuanced law subject to multiple interpretations.

It remains to be seen how DOJ will apply the Revised CFAA Guidelines in the context of ethical hacking in the digital assets and cryptocurrency spaces. Third-party coders working to unearth bugs in blockchain codes and smart contracts sometimes **"prove" such vulnerabilities** by transferring cryptocurrency, digital assets, or non-fungible tokens (NFTs) to themselves. However, some of these self-proclaimed white-hat hackers have **demanded bounties** prior to returning co-opted digital assets to the original owners on the blockchain—where demands can be carried out effectively due to the nature and pseudo-anonymity of digital asset ownership. Given the explosive growth of the digital assets sector in the past few years, it is worth monitoring whether DOJ views such conduct as "good faith security research" or not.

DOJ's narrowed view of CFAA-violative conduct is a positive development for white-hat researchers. For example, in 2011, DOJ **brought criminal CFAA charges** against internet neutrality advocate and hacktivist Aaron Swartz, for systemically downloading academic journal articles in violation of private computer-use policies. Those charges were viewed by many as an **expansive use** of the CFAA, and Swartz **took his own life** in 2013, two days after prosecutors rejected a plea deal counter-offer from Swartz's counsel. Given the policy changes and consultation requirements under the Revised CFAA Guidelines, it is possible that the *Swartz* case would today be viewed differently as a matter of prosecutorial discretion.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Nimrod Haim Aviad
Partner – Los Angeles
Phone: +1.213.443.5534
Email: naviad@crowell.com

Stephen M. Byers
Partner – Washington, D.C.
Phone: +1.202.624.2878
Email: sbyers@crowell.com

Matthew B. Welling
Partner – Washington, D.C.
Phone: +1.202.624.2588
Email: mwelling@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Alexander Urbelis
Senior Counsel – New York
Phone: +1.212.895.4254
Email: aurbelis@crowell.com

Anand Sithian
Counsel – New York
Phone: +1.212.895.4270
Email: asithian@crowell.com