BRACEWELL

INSIGHTS

More Wiggle Room for White Hat Hackers?

June 8, 2022

*By: **Seth D. DuCharme** and **Anissa L. Adas***

On May 19, 2022, the Department of Justice ("DOJ") ***announced*** significant clarifications to its policy on charging Computer Fraud and Abuse Act ("CFAA") violations that give some comfort to cyber security consultants who engage in network testing and related operations. Such activity has long been a gray area for "white hat" hackers.

The CFAA, 18 U.S.C., §1030, provides the government with the authority to prosecute cyber-based crimes by making it a crime to "intentionally access[ ] a computer without authorization or exceed[ ] authorized access and thereby obtain[ ] (A) information contained in a financial record of a financial institution…(B) information from any department or agency of the United States; or, (C) information from any protected computer." Most computers have the potential to fall under Section 1030's definition of a "protected computer," which includes any computer "used in or affecting interstate or foreign commerce or communication." The new guidance demonstrates an evolving view of how the statute should be enforced with the ultimate aim of leaving the public safer as an overall result of government action. In this regard, the DOJ directive expressly states that good faith security research should not be prosecuted.

Good faith security research is defined by the DOJ as "accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability." The update further clarifies that "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."

The updated policy further explains that, generally speaking, security research is not per se conducted in good faith. For example, research conducted for the purposes of identifying security flaws in devices and then profiting from the owners of such devices, does not constitute security research in good faith. This is significant, as much of the cyber security industry was built on the model of identifying exploits and selling fixes.

Following the Supreme Court's decision in *Van Buren v. United States*, the update also aims to quell concerns about the scope of the DOJ's enforcement of Section 1030.[1] For example, in a ***press release*** issued May 19, 2022, the DOJ recognized that "hypothetical CFAA violations," such as, "[e]mbellishing 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," should not on its own result in federal criminal charges. Due to lingering ambiguity about precisely what conduct should justify federal enforcement actions, prosecutors have been encouraged to consult with the Criminal Division's Computer Crime and Intellectual Property Section in deciding whether to prosecute such offenses, hopefully providing some consistency in the manner in which this guidance is interpreted in the field.

Consistent with the current administration's focus on emerging technologies, and cyber enforcement in particular, Deputy Attorney General Lisa Monaco observed that "[c]omputer security research is a key driver of improved cybersecurity," and that the announcement "promotes cybersecurity by providing clarity for good-faith security researchers who root out vulnerabilities for the common good." The revision also addressed the Department's prioritization of resources for violations of the CFAA.

Despite criticism from some industry professionals that the clarification does not go far enough to protect security researchers, the update signals the continuing evolution in DOJ policy, while individuals and corporations devote increasing resources to finding the safe pathway between the carrot of rewards for sound cyber security practices and the stick of regulatory and enforcement action.

---

1. *Van Buren v. United States*, 141 S. Ct. 1648 (2021).