Published on *The National Law Review* https://natlawreview.com

DOJ's New CFAA Policy: Relief for White Hat Hackers and Web Scrapers?

Article By:

Scott Ferber

Todd S. McClelland

Robert Duffy

David Sorenson

In an effort to "promote privacy and cybersecurity by upholding the legal right of individuals, network owners, operators, and other persons to ensure the confidentiality, integrity, and availability of information stored in their information systems," the US Department of Justice (DOJ) recently announced an updated policy directing that good-faith security research not be charged under the federal Computer Fraud and Abuse Act (CFAA), provided that:

- The activity involves accessing a computer solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability;
- Such activity is carried out in a manner designed to avoid any harm to individuals or the public; and
- 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.[1]

Security "research" for the purpose of discovering security holes in devices, machines or services in order to "extort" the owners of such devices, machines or services is not considered in good faith.

The new policy also provides further clarity on CFAA charging in the wake of the US Supreme Court's decision in *Van Buren v. United States*, 141 S. Ct. 1648 (2021). The DOJ has announced that it will not charge defendants with:

- Accessing computers "without authorization" unless when, at the time of the defendant's conduct, (1) the defendant was not authorized to access the protected computer under any

circumstances by any person or entity with the authority to grant such authorization; (2) the defendant knew of the facts that made the defendant's access without authorization; and (3) prosecution would serve the DOJ's goals for CFAA enforcement; and

- "Exceeding authorized access" unless, at the time of the defendant's conduct, (1) a protected computer is divided into areas, such as files, folders, user accounts or databases; (2) that division is established in a computational sense, that is, through computer code or configuration, rather than through contracts, terms of service agreements or employee policies; (3) a defendant is authorized to access some areas, but unconditionally prohibited from accessing other areas of the computer; (4) the defendant accessed an area of the computer to which his authorized access did not extend; (5) the defendant knew of the facts that made his access unauthorized; and (6) prosecution would serve the DOJ's goals for CFAA enforcement.

The DOJ's new policy provides needed clarity to a dynamically evolving area of the law, but questions remain about the distinction between "extortion" and legitimate remuneration for discovered vulnerabilities, the boundaries of permissible offensive cybersecurity activities, and civil relief under the CFAA and state CFAA analogues, among other areas.

FOOTNOTES

[1] DOJ's new CFAA policy complements other helpful guidance that the Department has issued in the area of cybersecurity, including: Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources (Feb. 2020), Best Practices for Victim Response and Reporting of Cyber Incidents (Sep. 2018) and A Framework for a Vulnerability Disclosure Program for Online Systems (July 2017).

National Law Review, Volume XII, Number 146