GT GreenbergTraurig

Alert | White Collar Defense & Special Investigations/ Data, Privacy & Cybersecurity

May 2022

DOJ Limits Application of Computer Fraud and Abuse Act, Providing Clarity for Ethical Hackers and Employees Paying Bills at Work Alike

This GT Alert covers the following:

- DOJ's announcement that it will decline prosecution under the Computer Fraud and Abuse Act (CFAA) of good-faith security research by so-called "white hat" hackers
- Exemption from prosecution for certain computer activity that may violate contractual terms of service or workplace rules, in conformity with recent Supreme Court precedent
- Coordination of certain charging decisions under the CFAA by Main Justice

On May 19, 2022, the Department of Justice announced it would not charge good-faith hackers who expose weaknesses in computer systems with violating the Computer Fraud and Abuse Act (CFAA or Act), 18 U.S.C. § 1030. Congress enacted the CFAA in 1986 to promote computer privacy and cybersecurity and amended the Act several times, most recently in 2008. However, the evolving cybersecurity landscape has left courts and commentators troubled by potential applications of the CFAA to circumstances unrelated to the CFAA's original purpose, including prosecution of so-called "white hat" hackers. The new charging policy, which became effective immediately, seeks to advance the CFAA's original purpose by clarifying when and how federal prosecutors are authorized to bring charges under the Act.

© 2022 Greenberg Traurig, LLP

DOJ to Decline Prosecution of Good-Faith Security Research

The new policy exempts activity of white-hat hackers and states that "the government should decline prosecution if available evidence shows the defendant's conduct consisted of, and the defendant intended, good-faith security research." The policy defines "good-faith security research" as "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."

In practice, this policy appears to provide, for example, protection from federal charges for the type of ethical hacking a *St. Louis Post-Dispatch* reporter performed in 2021. The reporter uncovered security flaws in a Missouri state website that exposed the Social Security numbers of over 100,000 teachers and other school employees. The Missouri governor's office initiated an investigation into the reporter's conduct for unauthorized computer access. While the DOJ's policy would not affect prosecutions under state law, it would preclude federal prosecution for the conduct if determined to be good-faith security research.

The new policy also promises protection from prosecution for certain arguably common but contractually prohibited online conduct, including "[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." Such activities resemble the facts of *Van Buren v. United States*, No. 19-783, which the Supreme Court decided in June 2021. In *Van Buren*, the 6-3 majority rejected the government's broad interpretation of the CFAA's prohibition on "unauthorized access" and held that a police officer who looked up license plate information on a law-enforcement database for personal use—in violation of his employer's policy but without circumventing any access controls—did not violate the CFAA. The DOJ did not cite *Van Buren* as the basis for the new policy. Nor did the DOJ identify any another impetus for the change.

To Achieve More Consistent Application of Policy, All Federal Prosecutors Must Consult with Main Justice Before Bringing CFAA Charges

In addition to exempting good-faith security research from prosecution, the new policy specifies the steps for charging violations of the CFAA. To help distinguish between actual good-faith security research and pretextual claims of such research that mask a hacker's malintent, federal prosecutors must consult with the Computer Crime and Intellectual Property Section (CCIPS) before bringing any charges. If CCIPS recommends declining charges, prosecutors must inform the Office of the Deputy Attorney General (DAG) and may need to obtain approval from the DAG before initiating charges.

Authors

This GT Alert was prepared by the following attorneys on behalf of the firm's White Collar Defense & Special Investigations Practice and Data, Privacy & Cybersecurity Practice:

- Kyle R. Freeny | +1 202.331.3118 | freenyk@gtlaw.com
- Linda M. Ricci | +1 617.310.5278 | riccil@gtlaw.com

© 2022 Greenberg Traurig, LLP

- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com
- Brittany M. Fisher | +1 617.310.5287 | fisherb@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2022 Greenberg Traurig, LLP. All rights reserved.*