Proskauer

DOJ Revises Policy for CFAA Prosecution to Reflect Developments in Web Scraping and Other Matters

New Media and Technology Law Blog on **May 24, 2022**

On May 19, 2022, the Department of Justice (DOJ) announced that it had revised its policy regarding prosecution under the federal anti-hacking statute, the Computer Fraud and Abuse Act (CFAA). Since the DOJ last made changes to its CFAA policy in 2014, there have been a number of relevant developments in technology and business practices, most notably related to web scraping. Among other things, the revised policy reflects aspects of the evolving views of this sometimes-controversial statute and the outcome of two major CFAA court decisions in the last year (the Ninth Circuit *hiQ* decision and the Supreme Court's *Van Buren* decision), both of which adopted a narrow interpretation of the CFAA in situations beyond a traditional outside computer hacker scenario.

While the DOJ's revised CFAA policy is only binding on federal CFAA criminal prosecution decisions (and could be amended by subsequent Administrations) and does not directly affect state prosecutions (including under the many state versions of the CFAA) or civil litigation in the area, it is likely to be relevant and influential in those situations as well, and in particular, with respect to web scraping. It seems that even the DOJ has conceded that the big *hiQ* and *Van Buren* court decisions have mostly (but not entirely) eliminated the threat of criminal prosecution under the CFAA when it comes to the scraping of "public" data. Still, as described below, the DOJ's revisions to its policy, as written, are not entirely consistent with the *hiQ* decision.

CFAA Background

The CFAA was enacted in 1984 and has been repeatedly amended since then, and provides, in pertinent part, that anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains. . . information from any protected computer" commits a crime. 18 U.S.C. § 1030(a)(2)(C). It defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The DOJ's policy change essentially attempts to put into place the Supreme Court's "gates-up-or-down" analogy that clarified both "without authorization" and "exceeds authorized access" under the CFAA – one either can or cannot access a computer system (i.e., with or without "authorization"), and one either can or cannot access certain areas within the system (i.e., did or did not "exceeds authorized access"), exempting from CFAA liability certain behaviors where a person rightfully accesses a computer network but uses the information from the database for an improper purpose. It also appears to attempt to quell some persistent fears of prosecution overreach in this area where literal violations of website terms of use might become CFAA criminal violations, which, according to the Ninth Circuit in *Nosal I*, "would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."

Some highlights of the CFAA policy revision include the following:

"Exceeds Unauthorized Access"

- Reflecting the Supreme Court decision in *Van Buren*, the revised policy states that the DOJ will not charge defendants with "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."
- In commenting on this six-part charging policy for "exceeds authorized access" cases, the DOJ states that that it will not take the position that a computer user's mere contractual violation causes authorization to access that computer to be

automatically revoked and cites some examples of such situations (e.g., embellishing an online dating profile contrary to the terms of service; using a pseudonym on a social networking site that prohibits them, or creating fictional accounts on hiring, housing, or rental websites, such as for anti-discrimination research).

- The policy noted above expressly contemplates user access permissions to be dictated or partitioned through "computer code or configuration" – thus, for example, an employee might have access to certain files on the network, but limited network access privileges would block access to other files and databases. User authorization dictated in this manner marks a clearer boundary for determining when a user may have exceeded their authorized access, rather than relying solely on written agreements (but open networks). Still, the DOJ policy leaves open the possibility to bring an "exceeds authorized access" case in the "narrow exception" of contracts, agreements or policies that "entirely prohibit defendants from accessing particular files, databases, folders, or user accounts on a computer *in all circumstances*." [emphasis added]. Thus, it seems the DOJ has left itself the option to bring prosecutions against users that violate blanket written restrictions on access to particular files and databases.
- The DOJ policy now states that the DOJ will not prosecute cases based on the theory that an employee has used a computer generally designated for his or her exclusive use in a way the employer's policy prohibits, such as by checking sports scores or paying bills at work in literal violation of a computer use policy.
- The DOJ maintains that CFAA "exceeds authorized access" prosecutions may still be brought 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 (e.g., reflecting the Ninth Circuit's *Nosal* decision).

With a clear reference to web scraping and reflecting the recent landmark Ninth Circuit decision in the *hiQ* case, the revised policy now states that: "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)…." As noted below, however, the DOJ revised policy retains prosecutorial flexibility that should give some web scrapers and others pause. And it is important to note that this reservation of flexibility appear to apply equally to proprietary databases or password-protected websites and publicly available sites:

- The DOJ policy notes that after a contractual violation occurs (e.g., a breach of web site terms of use), the DOJ will not contend that the user's previous authorization is automatically withdrawn (and cause the user to be in violation of the CFAA). However, the revised policy goes on to state that if the authorizing party later expressly revokes authorization ("for example, through unambiguous written cease and desist communications that defendants receive and understand"), the DOJ will consider access from that point onward to not be authorized. Thus, contrary to the Ninth Circuit's *hiQ* decision, which concerned scraping of a publicly available website and where the court did not find a written cease and desist letter to the data scraper to be an effective revocation of access, the DOJ is leaving room for the argument that a "cease and desist" letter can in fact revoke permission to access a website.
- The policy also states that in a CFAA prosecution, the government may be able to prove that the defendant was aware of restrictions on access in a number of ways, including: through the presence of technology intended to limit unauthorized access (though, as the DOJ noted, it is not necessary that this technological effort succeed in its intended purpose); written or oral communications sent to the defendant that unambiguously informed it that it is not authorized to access a protected computer or particular areas of it; or the defendant's own statements or behaviors reflecting knowledge that his actions were unauthorized. Here again, the DOJ appears to be suggesting that CAPTCHAs, IP address blocks and other technological attempts to block scraping may be relevant to the analysis. When applied to the scraping context, one wonders how ignoring robots.txt, which is a protocol that allows website owners to indicate whether, and to what extent, they consent to having their sites crawled and cached by web crawlers and spiders, would factor into any analysis of "authorized" access.

So, we are left with the question, is the DOJ's revised policy consistent with the Ninth Circuit's *hiQ* decision? It would appear that the DOJ's revised policy incorporates much – but not all – of *hiQ*. The DOJ policy appears to diverge by suggesting the DOJ might consider a CFAA prosecution in instances where a defendant has received a clear revocation of access or knowingly bypassed technical blocking measures to access a site – such as the cease and desist letter sent by LinkedIn to hiQ.

At this point, any perceived gray areas would likely be filtered through the overall departmental purposes that CFAA prosecutions must serve and the DOJ's "goals of enforcement," which take into account the "sensitivity of the affected computer system or the information transmitted by or stored on it" and the extent to which damage or unauthorized access affects "national security, critical infrastructure, public health and safety, market integrity," or other important "national or economic interests."

Access "Without Authorization"

The CFAA provides for a criminal cause of action when a defendant accesses a protected computer "without authorization." The revised DOJ policy states that the DOJ will not charge defendants for accessing "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 Department's goals for CFAA enforcement.

Given these big changes, one will not know the new parameters of the DOJ's revised CFAA policy until they are implemented in the real world. We will see if the DOJ's inconsistencies with the *hiQ* decision end up being meaningful in further prosecutions.

Security research:

- Beyond the scraping- and employee-related CFAA authorization scenarios, the DOJ's revised policy for the first time directs that "good faith security research" should not be charged criminally.
- Under the revised policy, "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."
- This is in contrast to bad faith security research, which the policy states would be for the purpose of "discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services."

- While the two ends of this good faith/bad faith spectrum are fairly understandable, one imagines there are some reputable (or semi-reputable) motives that fall in between that may come up in the future.

Despite what might be a little nuance regarding exactly what is a “good faith” researcher, given the prevalence of security researchers, cybersecurity testing and bug bounties today, the policy certainly lifts a cloud over “good faith” testing of cybersecurity flaws and is a general boost to continued research everywhere to improve the cybersecurity of computer networks.

View Original

Related Professionals

Jeffrey D. Neuburger
Partner