DOJ Launches Major Offensive Against Computer Hackers as U.S. Supreme Court Agrees to Hear Case That Could Limit Liability Under Federal Anti-Hacking Statute

04.29.20

On April 22, the United States Department of Justice announced an ongoing multi-agency, multi-jurisdictional offensive targeting hundreds of online scams and phishing, spoofing, and malware schemes related to the novel coronavirus (COVID-19) pandemic.[1] Only days earlier, however, on April 20, the Supreme Court of the United States agreed to review an unrelated case brought under the Computer Fraud and Abuse Act of 1986 (CFAA)—the DOJ's primary weapon against computer hacking—for the first time in the statute's nearly 35-year history.[2] The case could significantly limit the CFAA's scope; rein in certain aggressive positions taken by the DOJ; and provide much-needed guidance to companies, practitioners, and prosecutors attempting to assess potential civil and criminal liability under this controversial statute.

DOJ's April 22 Cybercrime Announcement

In its April 22 announcement, the DOJ provided examples of some of the hundreds of COVID-19-related cybercrime schemes that recently have been disrupted through coordination by, and in collaboration with, the private sector and the Federal Bureau of Investigation, the U.S. Secret Service, the DOJ's Computer Crime and Intellectual Property Section and Consumer Protection Branch, the U.S. Postal Inspection Service, and the Food and Drug Administration. Examples of the schemes include an illicit website pretending to solicit and collect donations to the American Red Cross for COVID-19 relief efforts; fraudulent websites that spoofed government programs and organizations to trick victims into entering personally identifiable information, including bank account information, such as look-alike domains for Internal Revenue Service stimulus payments; and websites of legitimate companies and services used by hackers to facilitate the distribution or control of malicious software.

The DOJ's announcement also offers tips to help companies and individuals avoid falling victim to COVID-19-related cybercrimes, such as:

- Independently verifying the identity of any company, charity, or individual that contacts you regarding COVID-19;
- Double-checking websites and email addresses offering information, products, or services related to COVID-19, recognizing that scammers often employ similar or look-alike domains

(*e.g.*, “cdc.com” or “cdc.org” instead of “cdc.gov”);

- Ignoring links or email attachments from unknown or unverified sources, which could cause a virus to be downloaded onto your computer or device;
- Ensuring that your anti-malware and anti-virus software are operating and up to date;
- Ignoring offers for a COVID-19 vaccine, cure, or treatment, as a true vaccine or cure will not be announced through an unsolicited sales pitch; and
- Checking online reviews of any company offering COVID-19 products or supplies to verify that customers have not complained about not receiving their orders.

Finally, the announcement provides contact information and different means through which to report COVID-19 cybercrime schemes to law enforcement.

U.S. Supreme Court’s April 20 Grant of Certiorari in *Van Buren v. United States*

Lurking behind the scenes, however, is a Supreme Court case that could derail other aspects of the DOJ’s cybercrime prosecution agenda: *Van Buren v. United States*. In *Van Buren*, the Court will have its very first opportunity to examine the CFAA, 18 U.S.C. § 1030, in the context of a federal circuit split over what it means to access a computer without authorization or to exceed authorized access to a computer.

Congress enacted the CFAA in 1986, inspired in part by the Cold War-era motion picture, *WarGames*,[3] in which a teenaged hacker unwittingly gained control of the U.S. nuclear arsenal and nearly triggered a nuclear war with the Soviet Union.[4] The CFAA primarily was intended to target computer hackers attempting to infiltrate, damage, or steal information from federal government computer systems,[5] though Congress amended the statute over the years to prohibit such hacking crimes against any “protected computer,” generally interpreted to mean almost any public or private Internet-connected computer or computer system.[6] The statute also has been amended to enable businesses and individuals to file private civil damages claims.[7]

Despite the CFAA’s original focus on computer intrusions, with increasing frequency—and controversy—the DOJ has used the CFAA to target company and government employees for misusing workplace computers. The DOJ has relied on CFAA provisions imposing civil and criminal liability on any person who “intentionally accesses a computer without authorization or exceeds authorized access” and, thereby, obtains certain types of information or things of value, or causes damage.[8] Although the CFAA does not define “[w]ithout authorization,” it defines “exceeds authorized access” to mean “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.”[9] Alleging that employees violated internal computer-use or conduct policies, the DOJ has pursued and secured the felony convictions of numerous individuals for obtaining sensitive company or government information from workplace computers and systems that they were otherwise allowed to access, on grounds that such access exceeded their employer’s authorization.

But critics and courts have pushed back hard, resulting in a federal circuit split. Four federal appellate courts (the First, Fifth, Seventh, and Eleventh circuits) interpret the CFAA to criminalize an individual accessing data outside the scope of his or her employer’s authorization so long as the individual did so for an improper purpose; whereas, three federal appellate courts (the Second, Fourth, and Ninth circuits) interpret the CFAA to apply only where an individual accesses

information on a computer that he or she was never authorized to access at all, opining, for example, that "we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."[10]

In *Van Buren*, the Supreme Court will have the opportunity to resolve this debate. *Van Buren* involves the felony prosecution of a metropolitan Atlanta-area police officer in the Northern District of Georgia under the CFAA for accessing and obtaining information from a law enforcement database that he was authorized to access as part of his job—the Georgia Crime Information Center (GCIC) database—to run a license plate number for someone in exchange for a personal loan.[11] It was undisputed that the purpose of Van Buren's GCIC database access was improper.[12] But Van Buren argued (unsuccessfully) in the trial court and on appeal to the Eleventh Circuit that he still could not be convicted under the CFAA because his job permitted him to access the GCIC database, and imposing liability under these circumstances would "allow [] employers or other parties to legislate what counts as criminal behavior through their internal policies or their terms of use."[13] The specific question presented in Van Buren's successful petition for certiorari to the Supreme Court, granted on April 20, is "[w]hether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose."[14]

Our analysis of *Van Buren* and related developments under the CFAA are ongoing, and we intend to monitor the case as it proceeds to oral argument and an eventual decision. If tradition holds, we expect the Supreme Court to interpret the statute narrowly, to rein in the DOJ's prosecutorial discretion to some extent, and to provide much-needed guidance to companies, practitioners, and prosecutors. It also is likely that the Court's interpretation of the CFAA will have ramifications beyond the workplace and impact a variety of cybercrime prosecutions in different contexts.

If you wish to discuss *Van Buren* or possible criminal or civil liability under the Computer Fraud and Abuse Act, please contact one of our White Collar and Government Investigations team members.

---

[1] Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams, DOJ.gov (Apr. 22, 2020) (available at https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams).

[2] *Van Buren v. United States*, No. 19-783 (Apr. 20, 2020 order granting certiorari (available at https://www.supremecourt.gov/orders/courtorders/042020zor_dc8f.pdf).

[3] *WarGames* (MGM/United Artists 1983).

[4] H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695-96.

[5] H.R. REP. NO. 99-612, at 3 (1986) (focusing on "the technologically sophisticated criminal who breaks into computerized data files"); *see also hiQ Labs, Inc. v. LinkedIn Corp*., 938 F.3d 985, 1000 (9th Cir. 2019) ("The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking.").

[6] 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" to mean, in relevant part, a computer "which is used in or affecting interstate or foreign commerce or communication"); *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015) (opining that "protected computer" under Section 1030 means "effectively all computers with Internet access.").

[7] 18 U.S.C. § 1030(g).

[8] 18 U.S.C. §§ 1030(a)(1) – (a)(5).

[9] 18 U.S.C. § 1030(e)(6).

[10] *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012).

[11] United States v. Van Buren, 940 F.3d 1192, 1208 (11th Cir. 2019), cert. granted, No. 19-783, 2020 WL 1906566 (U.S. Apr. 20, 2020).

[12] Id.

[13] Id.

[14] Pet'n for Cert. at 1 (available at https://www.scotusblog.com/case-files/cases/van-buren-v-united-states/).

Contacts

David M. Chaiken
Partner
david.chaiken@troutman.com
404.885.2587

Michael A. Schwartz
Partner
michael.schwartz@troutman.com
215.981.4494

Related Professionals

Tiffany N. Bracewell

Timothy A. Butler

Chelsea Lamb

Matthew White

Related Practices and Industries

White Collar and Government Investigations

Cybersecurity, Information Governance and Privacy