New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 15
MONDAY, JULY 24, 2017

International Criminal Law and Enforcement

Expert Analysis

The Global Reach Of the U.S. Computer Intrusion Law

By **Nicholas M. De Feis**

And **Philip C. Patterson**

Most computer users likely assume that the United States has laws against hacking or otherwise intruding into computers. What those surfing the Internet may not realize, however, is that the language of the U.S. computer intrusion law is so broadly defined and interpreted as to potentially criminalize conduct involving virtually every computer in the world. Moreover, an equally broad definition of what constitutes a "computer," combined with a vague definition of what constitutes "unauthorized access" to such a computer, means that usage of almost any electronic device worldwide could theoretically form the basis of a crime.

The global reach of U.S. computer intrusion laws is illustrated in a recent opinion from the U.S. District Court for the Eastern District of New York. The opinion, which characterizes the prosecution as "unique" and "cutting-edge," demonstrates that a computer intrusion violation can be pleaded even when an individual never sets foot in the United States. The opinion also illustrates how, as technological innovation increasingly blurs any remaining lines between a computer and other electronic devices, U.S. computer anti-intrusion laws may eventually come to cover conduct involving virtually every electronic device in the world.

> The language of the U.S. computer intrusion law is so broadly defined and interpreted as to potentially criminalize conduct involving virtually every computer in the world.

The CFAA

U.S. computer intrusion laws are found in the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. §1030. The CFAA was enacted in 1986 and subsequently amended in a number of significant ways. The CFAA generally prohibits individuals from obtaining information through intrusions into federal government and financial institution computers. Section 1030(a)(2)(C) of the CFAA, however, also makes it a crime for a person to "intentionally accesses a computer without authorization or exceed[] authorized access, and thereby obtain[] … information from any protected computer." Each of these terms has been broadly defined and interpreted, both factually and geographically.

For example, §1030(e)(1) of the CFAA defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage

NICHOLAS M. DE FEIS *is a partner and* PHILIP C. PATTERSON *is counsel at De Feis O'Connell & Rose, where they practice white-collar criminal defense and international investigations. Mr. De Feis is a former federal prosecutor.*

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]" In 2011, the Supreme Court denied a petition for certiorari from a U.S. Court of Appeals for the Eighth Circuit opinion holding that a cell phone used only to make calls and text constituted a "computer." *United States v. Kramer*, 631 F.3d 900 (8th Cir. 2011), cert. denied, 563 U.S. 1039 (2011). Under this reading, everything from flip phones to smart phones thus qualifies as a "computer." Moreover, the Eighth Circuit opinion quoted a law review article noting that the term "computer" now means "coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players."

The CFAA contains an equally broad definition of the phrase "protected computer." A "protected computer" is defined in §1030(e)(2)(B) to include a computer that is "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." As the U.S. Court of Appeals for the Second Circuit observed in a 2015 opinion, this definition of a "protected computer" thus includes "effectively all computers with Internet access." *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015).

Ambiguity in the CFAA further expands its reach. For example, the phrases "without authorization" or "exceed[ing] authorized access" are not specifically defined, which has resulted in a significant amount of litigation. The 2011 prosecution of so-called "hacktivist" Aaron Swartz became something of a cause célèbre, partly because Swartz unfortunately committed suicide while under indictment, but also because of the government's expansive reading of the "exceed[ing] authorized access" language.

Swartz was indicted in Massachusetts pursuant to the CFAA for allegedly accessing MIT's computer network to download thousands of academic journals from digital library JSTOR, apparently to make the journals publicly available for free. *United States v. Swartz*, 11 CR 10260 (D. Ma. filed July 14, 2011). Some perceived Swartz as a victim of over-criminalization because his indictment partly relied on JSTOR's terms of service (i.e., website terms we all routinely accept without reading) to argue that Swartz's downloads exceeded authorization. Some legislators subsequently proposed amending the CFAA via "Aaron's Law" to ensure that such standard computer activity cannot form the basis of criminal charges.

In short, the CFAA as currently defined potentially makes it a crime to obtain information without authorization from almost any electronic device anywhere in the world, with the bar for "exceeding authorization" set very low. The net effect of these definitions is reflected in a recent opinion from the Eastern District of New York.

'U.S. v. Gasperini'

In August 2015, Fabio Gasperini was charged in the Eastern District of New York with CFAA, wire fraud and money laundering violations. *United States v. Gasperini*, No. 16 CR 441 (E.D.N.Y.). He was arrested in Amsterdam and extradited to the United States. Gasperini is accused of using a "botnet" to perpetrate a "click fraud." A botnet is created when a programmer uses malware to secretly infect and control multiple computers. See, e.g., Nicholas M. De Feis and Philip C. Patterson, "'Botnets' and the Battle Against Cybercrime," N.Y.L.J., April 30, 2015. The programmer can use the resulting network for various purposes, such as sending spam or carrying out denial of service attacks (directing so much Internet traffic to a website at the same time that it crashes). Gasperini was allegedly hired by advertising firms that paid him based on the amount of traffic he drummed up for certain websites. The government alleges that he used a botnet he created to generate fake traffic to those sites, resulting in overpayments for his services.

Click frauds unfortunately are increasingly common, but the case against Gasperini reveals the expansive reach of the CFAA, both as to its jurisdiction and its definitions. According to filings by his counsel, Gasperini is an Italian citizen who has never set foot in America. He was apparently in Rome throughout the duration of the alleged scheme.

Moreover, the advertising firms he allegedly defrauded are Italian. In addition, the majority of the servers Gasperini allegedly infected were located overseas. Although the government asserts that his malware was found on U.S. servers, Gasperini apparently never actually "took" anything off the servers—at least in the traditional sense of the word. Instead, he is essentially accused of gathering information that helped him carry out his scheme.

Gasperini moved to dismiss the indictment. For the CFAA charges, he argued a failure to plead the elements plus a due process violation. He also argued that the wire fraud charges cannot apply extraterritorially. The government responded by asserting, among other things, that Gasperini used servers leased in the United States to further his scheme, and that the scheme included clicks on advertisements by U.S. firms. The government also asserted that he used a U.S. online payment firm to launder the proceeds. The government added that it expects to prove that a piece of Gasperini's malware that helped facilitate the scheme was present on over 800 servers in the United States, including more than 100 in the Eastern District of New York.

Judge Nicholas Garaufis denied Gasperini's motion, noting that what Gasperini was really arguing was failure of proof. Garaufis concluded that the indictment sufficiently pleaded CFAA violations, and that a failure to actually prove such violations must be left for trial. Garaufis, after an extensive analysis, also held that the charges do not violate due process or the prohibition on extraterritorial application of U.S. laws. Garaufis did, however, grant a portion of Gasperini's motion seeking a bill of particulars. Specifically, Gasperini was entitled to greater detail on how he purportedly "obtained" information from a computer as required by §1030(a). Garaufis, noting the government's acknowledgment that this is a "cutting-edge" case, expressed concerns that Gasperini thus could not look to other prosecutions for guidance on how the government might seek to satisfy the "obtain" element of the CFAA charges.

> 'Gasperini' illustrates how, as technological innovation increasingly blurs any remaining lines between a computer and other electronic devices, U.S. computer anti-intrusion laws may eventually come to cover conduct involving virtually every electronic device in the world.

The government subsequently produced a bill of particulars, which identified highly technical material as the information "obtained" from a computer. The information obtained included, among other things, IP addresses, usernames, ports available for networking, and information about computer settings and vulnerabilities. This information allegedly helped reveal to Gasperini what networking avenues were available to carry out the scheme.

Gasperini filed a second motion to dismiss again arguing, among other things, that the government failed to identify what information was "obtained" in violation of the CFAA. The government filed its opposition and Judge Garaufis denied the motion during a July 6, 2017 status conference. No opinion has been docketed yet. As Garaufis noted in his first opinion, however, Gasperini's arguments seem to have more to do with the sufficiency of evidence at trial than they do the elements of the CFAA.

Gasperini's arguments do, however, raise interesting questions about what the thresholds are for satisfying the "obtain" and "information" elements of the CFAA. Regardless, given the broad interpretations courts have already afforded the "without authorization" elements, the Gasperini prosecution likely will not come to stand as the outer limits of the CFAA.

Conclusion

One does not have to strain to imagine countless hypotheticals that might test the CFAA's limits. For the moment, at least, computer users globally should proceed with caution and hope that courts or legislators are eventually able to clearly define the full scope and reach of the CFAA.