Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

From Clickwrap to RAP Sheet: Criminal Liability under the Computer Fraud and Abuse Act for Terms of Service Violations

March 19, 2020

Computers and the internet are ubiquitous, and so too are contractual restrictions on their use. Users of smartphones, tablets, personal computers, social media websites, apps, online shopping platforms, streaming services, and more are generally bound by terms of service (ToS) agreements—contracts that govern the use of a product. Often, ToS agreements take the form of clickwrap agreements requiring users to click a box indicating that they are aware of, and agree to, certain terms on a website. In other instances ToS agreements may simply amount to a written notification that by using a product, the user agrees to be bound by the product's ToS. Either way, ToS agreements are now so prevalent that, at least according to some empirical studies, users generally do not read them. That is perhaps unsurprising given that ToS agreements are often lengthy, covering everything from the number of authorized users of a product to the types of content that may be shared through a device or service. But providers of computer and internet products and services rely on ToS for a variety of purposes, including limiting liability, protecting proprietary data, and preventing their products or services from being used in a harassing, threatening, or abusive manner. Against this backdrop, federal courts have diverged on the issue of whether an individual may—under certain circumstances—be criminally liable under federal law for ToS violations.

The judicial disagreement stems from two conflicting interpretations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030—a civil and criminal cybersecurity law prohibiting certain computer-related activities. Federal appellate courts are divided on when an individual who violates a ToS agreement runs afoul of the CFAA and is subject to liability under the statute.

This Sidebar begins with background on the relevant provisions of the CFAA, before examining the split among the federal appellate courts over when, if ever, the CFAA imposes criminal liability for violations of ToS agreements. The Sidebar concludes with some considerations for Congress.

The CFAA: Background and Key Provisions

The CFAA prohibits a number of activities where a person illicitly accesses a qualifying computer if he is "without authorization" or if he "exceeds authorized access." The phrases appear in a number of the

Congressional Research Service
https://crsreports.congress.gov
LSB10423

CFAA's subsections, such as § 1030(a)(2), which prohibits an individual intentionally accessing a computer without authorization or in excess of authorization and obtaining information from a financial institution, the federal government, or "any protected computer" (construed by courts to include any computer connected to the internet). Similarly, § 1030(a)(4) makes it a crime to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access" and obtain something of at least $5,000 in value. Other sections use the same language.

The CFAA was enacted in 1984 to address growing concerns over the dangers of hacking—intrusions or trespasses "into computer systems or data"—and has been primarily used to combat that threat. The law protects a broad range of technology including most websites, and nearly any "devices with embedded processors and software" other than "typewriters, typesetters, and handheld calculators." The CFAA has been amended several times since 1984, but it is still described as an anti-hacking law. The law has been invoked in successful hacking prosecutions, including in the high-profile case of one hacker who used a phishing scam to access private email and cloud accounts, through which he obtained nude photographs of celebrities, which were later leaked online.

Although such examples of hacking fit squarely within the CFAA's scope, federal appellate courts have disagreed over whether the law criminalizes the violation of ToS agreements. The circuit split is the result of differing interpretations of the phrases "without authorization" and "exceeds authorized access." The statute does not define "without authorization." As for "exceeds authorized access," § 1030(e)(6) defines the phrase as "access[ing] 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 . . . ." However, that definition hinges on the meaning of "with authorization," which the CFAA also does not define. As discussed below, the federal appellate courts disagree over the breadth of these phrases, and whether they permit criminal liability for ToS violations.

The Split: Criminal Liability for ToS Violations

Under a broad interpretation of the two phrases, an individual who violates a contract limiting the uses of a computer—such as a ToS agreement—may be acting without authorization or in excess of authorization under the CFAA, triggering criminal liability. The First, Fifth, Seventh, and Eleventh Circuits have adopted this view, often in cases focusing not on ToS violations, but rather on employer/employee computer use agreements. These cases generally involve an employee or former-employee who is authorized to access a work computer for limited purposes, but who uses that computer for other reasons. For example, in *United States v. Rodriguez* an employee accessed his employer's database to obtain "sensitive personal information" for his personal use, despite the employer's policy prohibiting database use for nonbusiness purposes. The Eleventh Circuit concluded in *Rodriguez* that the employee "exceeded authorized access" under the CFAA because, although the employee was authorized to access the database, he was not authorized to do so for personal purposes. In other words, "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'" Although many of these cases focus primarily on the meaning of the phrase "exceeds authorized access," the broad interpretation has been applied to "without authorization" as well. Thus, under the broad view, if a contract limits authorization to certain uses, and a user exceeds the bounds of those contractual restrictions, he may have exceeded authorized access or be without authorization in criminal violation of the CFAA.

Although these courts generally do not expressly articulate a policy rationale in adopting the broad interpretation, they appear concerned not just with hacking, but also other computer-based harms such as the misappropriation of confidential information by rogue employees or former-employees. For example, in concluding that CFAA liability could extend to an employee who accessed and removed "highly sensitive and confidential" customer account information that she was not authorized to access, the Fifth Circuit noted the harm the employee caused to the employer and its customers.

While several of the cases adopting the broad interpretation have not arisen in the context of ToS agreements, some courts have clarified that the broad interpretation would extend criminal liability under the CFAA to at least some ToS violations. For example, the First Circuit observed that "[a] lack of authorization could be established by an explicit statement on the website restricting access . . . ." such as a website's "lengthy limiting conditions." That said, federal district courts in at least one circuit employing the broad interpretation have declined to extend criminal liability to individuals who merely violated a website's ToS.

Several other courts, including the Second, Fourth, and Ninth Circuits, have adopted a narrower interpretation of "without authorization" and "exceeds authorized access," grounded in an understanding that the purpose of the CFAA is to criminalize hacking. These courts would apply CFAA liability only to those who lack any authorization to access a computer or website. For example, courts applying the narrow view would exclude from CFAA liability those who have merely violated ToS agreements. CFAA liability could only apply to such individuals if their permission to access a computer or website "has been revoked explicitly," such as through a cease and desist letter. In the employer/employee context, courts applying the narrow interpretation would limit the applicability of the phrase "exceeds authorized access" to hackers who are "authorized to access only certain data or files" but who access "unauthorized data or files." For example, if an "employee is permitted to access only product information on the company's computer but [he] accesses customer data" he would have exceeded authorized access by "look[ing] at the customer lists." But, if that employee were permitted to access the customer data for certain reasons (e.g., business purposes) and he did so for other *purposes* (e.g., personal curiosity), he would not have exceeded authorized access under the narrow view.

The Second, Fourth, and Ninth Circuits all concluded that the rule of lenity requires the narrow interpretation. That canon of construction counsels that penal statutes should "be construed strictly" in favor of "the interpretation least likely to impose penalties unintended by Congress." According to courts applying the narrow interpretation, the broad interpretation of "exceeds authorized access" or "without authorization" would cause significant risk of the unintended consequences that the rule of lenity seeks to avoid. As the Ninth Circuit observed, the broad interpretation would define authorized access by the terms of contracts that "most people are only dimly aware of," that "virtually no one reads or understands," and that are subject to change without notice. According to the courts adopting this view, the broader view of the CFAA could "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime." For example, one court cautioned that the broad interpretation would turn "every conscious [ToS violation into] . . . a CFAA misdemeanor" under § 1030(a)(2), which prohibits intentionally accessing a protected computer without authorization or in excess of authorization and obtaining information. The court explained that intent under the subsection requires only intent "to obtain unauthorized access to a protected computer," and that "obtaining information" includes "mere observation of the data."

Many of the cases adopting the broad view of the CFAA predate the Second, Fourth, and Ninth Circuit opinions, and do not expressly respond to the concerns expressed in those opinions regarding over-criminalization. Nevertheless, some jurists have expressed skepticism that that the broad view would actually criminalize routine ToS violations. Dissenting from a key Ninth Circuit opinion adopting the narrow view of the CFAA, two judges observed that even under a broad reading of the CFAA an individual would not be criminally liable unless he acted with the intent required by the statute. The judges noted that under § 1030(a)(4)—which prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization" or doing so in excess of authorization—a defendant would be liable *only* if he acted with "the requisite mens rea and the specific intent to defraud . . . ." The judges declined, however, to examine whether such limitations would apply under other CFAA subsections, such as § 1030(a)(2), which were not at issue in the case.

Considerations for Congress

The circuit split exists against a backdrop of a broader debate about the merits of various interpretations of the CFAA. Several commentators have raised concerns that the broad interpretation of "exceeds authorized access" and "without authorization" employed by some courts leaves the CFAA vague and susceptible to "[a]rbitrary and discriminatory enforcement." The general concern is that if criminal liability under the CFAA hinges on onerous contracts that few read, then the CFAA does not "define . . . criminal offense[s] [under the statute] with sufficient definiteness that ordinary people can understand what conduct is prohibited . . . ." At least one court echoed such concerns in adopting the narrow interpretation of the CFAA. Relatedly, some courts have expressed concern that "by utilizing violations of [ToS agreements] as the basis for [a CFAA] crime," the broad interpretation "makes the website owner-in essence-the party who ultimately defines the criminal conduct." According to some, that not only contributes to the possibility of arbitrary enforcement, but it also makes behavior that is traditionally the domain of state tort and contract claims the subject of federal criminal law.

Criticism of the broad interpretation of the CFAA is not universal. For example, some individuals and businesses have advocated for the broad interpretation, because it permits civil CFAA lawsuits to enforce contractual rights, such as those embodied in a ToS agreement. Businesses have invoked the CFAA's civil provisions to remedy injuries relating to contractual violations, such as misappropriation of confidential information—often in the context of disputes with rogue employees or former employees who abuse computer privileges at their employer's expense. In public comments, a Department of Justice (DOJ) official agreed that the CFAA should protect against such threats. He described opinions adopting the narrow view as an "obstacl[e]" to prosecuting such cases, which the government has done in the past. In addition, in a recent brief opposing certiorari on the meaning of "exceeds authorized access," the Solicitor General contested the argument that the broad interpretation creates uncertainty and criminalizes commonplace computer behavior. The Solicitor General noted that such concerns are purely hypothetical because of a DOJ policy that limits prosecutorial discretion in CFAA cases. The DOJ policy requires, among other things, that before bringing charges prosecutors consider "whether the defendant knowingly violated restrictions on his authority to obtain or alter information stored on a computer, and not merely that the defendant subsequently misused information or services that he was authorized to obtain from the computer at the time he obtained it . . . ."

Currently, the extent of criminal liability for ToS violations varies by jurisdiction. Although a pending petition for a writ of certiorari seeks Supreme Court clarification of the ongoing circuit split, in the past the Court has denied review of the issue. In the absence of Supreme Court review, the current split could continue, which to some suggests there may be a role for legislation to the extent Congress is interested in clarifying the statute's reach.

Some Members in past Congresses introduced legislation that sought to modify the "without authorization" and "exceeds authorized access" language in the CFAA. One example, Aaron's Law, was "named in honor of the late Internet innovator and activist Aaron Swartz," who committed suicide while undergoing CFAA prosecution. First introduced in the 113th Congress, Aaron's Law would have replaced the phrase "exceeds authorized access" with "access without authorization," which it defined as obtaining "information on a protected computer . . . that the accesser lacks authorization to obtain" by "knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information." That proposal would have limited the CFAA's breadth in a manner more consistent with the understanding of courts applying the narrow view of the statute. No bills have been introduced in this Congress addressing the split.

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer