Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Van Buren v. United States: Supreme Court Holds Accessing Information on a Computer for Unauthorized Purposes Not Federal Crime

July 1, 2021

On June 3, 2021, the United States Supreme Court issued its opinion in *Van Buren v. United States*, holding that an individual does not violate the Computer Fraud and Abuse Act (CFAA) if he is authorized to obtain information on a computer for specific purposes only, and he then accesses that information for other unauthorized purposes. Rather, in a 6-3 opinion authored by Justice Barrett, the Court determined that in order to violate the CFAA, an individual must access an area of a computer or *information* on a computer that is completely "off limits to him," as opposed to accessing a computer or information that he is entitled to use in at least some circumstances. In so holding, the Court appears to have resolved an issue that has divided lower courts—whether obtaining information for an improper purpose is unlawful under the CFAA. Given the potentially wide-reaching implications of *Van Buren*, which marks the Court's first significant foray into a statute that has been described as the "nation's predominant anti-hacking law," this Sidebar provides an overview of the Court's holding and analysis. The Sidebar concludes with a summary of some possible implications stemming from *Van Buren*, as well as various issues for congressional consideration. A summary of relevant legal background, as well as the parties' arguments in *Van Buren*, may be found in a previous CRS product: CRS Legal Sidebar LSB10423, *From Clickwrap to RAP Sheet: Criminal Liability Under the Computer Fraud and Abuse Act for Terms of Service Violations*, by Peter G. Berris.

Holding and Analysis

Van Buren stems from the conviction of former police sergeant Nathan Van Buren for violating, among other things, 18 U.S.C. § 1030(a)(2)—a provision of the CFAA which makes it a crime to intentionally access a computer *without authorization* or to *exceed authorized access* and obtain information from a financial institution, the federal government, or "any protected computer" (any computer connected to the internet). Another subsection of the CFAA—§ 1030(e)(6)—defines "exceeds authorized access" as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Van Buren used a law enforcement database, which he was authorized to use "only for law enforcement purposes," to search for license plate

Congressional Research Service
https://crsreports.congress.gov
LSB10616

information for personal profit. Van Buren was not "without authorization" to use the law enforcement database, because he did so with "valid credentials to log into the law enforcement database." Rather, the question for the Court was whether he *exceeded* authorized access in violation of § 1030(a)(2) by obtaining license plate information from the database for personal purposes, as prohibited by department policy.

Despite the prominence of policy considerations and constitutional principles in briefs and oral arguments, the Court resolved *Van Buren* through textualism (a concept discussed in other CRS products). In particular, the Court examined the phrase "exceeds authorized access" as defined in § 1030(e)(6), and focused specifically on the language "entitled so to obtain," and particularly the word "so." Van Buren argued that the phrase requires only that an individual "has the right to acquire the information in the manner described in the statute—via computer—as opposed to via some other method, such as by calling on the phone or procuring hard copies." Thus, in Van Buren's view, an individual is "entitled so to obtain" information if he has permission to access it by computer, even if he does so for an unauthorized purpose. In contrast, the government claimed that an individual is entitled to do something "only when he has been granted a right to do it," and that an individual is "entitled *so*" to "do something only when he has been granted the right to do it in a particular manner or circumstance." On this reading, if a computer-use restriction like the department policy at issue in *Van Buren* restricts access to a particular manner or circumstance (e.g., law enforcement purposes), an individual would exceed authorized access if he accessed information for a purpose contrary to that restriction (e.g., personal profit). The government's interpretation of "entitled so to obtain," imbued the CFAA with a broader scope than Van Buren's; effectively defining the limits of authorization—and liability under the CFAA—by reference to a broad array of potential restrictions such as terms of service [ToS] or other contractual computer-use policies. The Court determined that the government's interpretation of "so" would "capture[] *any* circumstance-based limit appearing *anywhere*—in the United States Code, a state statute, a private agreement, or anywhere else." Instead, the Court found Van Buren's interpretation "more plausible," interpreting "so" as a word that refers back to the preceding text in a manner that explains the method by which the information must be obtained. Thus, the Court held "[t]he phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access."

Incorporating the textual analysis of § 1030(e)(6) into § 1030(a)(2), the Court held that the "provision covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend." In contrast, the Court held that § 1030(a)(2) "does not cover those who . . . have improper motives for obtaining information that is otherwise available to them." To illustrate, the Court reiterated one of Van Buren's arguments: a computer user who is authorized to "access information stored in a computer—e.g., in 'Folder Y,'" does not "violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose." However, an individual would exceed authorized access, potentially in violation of § 1030(a)(2), if he instead obtains information "located in prohibited 'Folder X,' to which the person lacks access." In other words, a mere improper purpose alone is insufficient to make obtaining information on a computer a CFAA violation.

Justice Thomas, joined by Chief Justice Roberts and Justice Alito, dissented, determining that Van Buren exceeded authorized access under §1030(a)(2) by accessing information from the law enforcement database "under circumstances that were expressly forbidden." Turning to the crux of the issue—i.e., "whether Van Buren was 'entitled so to obtain' the . . . license-plate information"—the dissenting justices placed particular emphases on the word "entitled." They contended that a "person is entitled to do something only if he has a 'right' to do it." Justice Thomas noted that this is a "necessarily circumstance dependent" evaluation: "a person is entitled to do something only when 'proper grounds' or facts are in place." According to the dissent, an individual lacks proper grounds to access information when he does so for an unauthorized *purpose*. For additional support, the dissent analogized to other legal contexts like

property law where "an entitlement to use another person's property is circumstance specific." For example, the dissenting justices looked to trespass, arguing that a person trespasses when he is "authorized to enter land and entitled to use that entry for one purpose but does so for another." According to the dissent, "[w]hat is true for land is also true in the computer context; if a company grants permission to an employee to use a computer for a specific purpose, the employee has no authority to use it for other purposes."

Implications and Congressional Considerations

Given the ubiquity of computers, and the broad swath of computers and computer-enabled technology governed by the CFAA, the implications of *Van Buren* could be considerable. Most immediately, *Van Buren* appears to resolve a long-standing circuit split regarding the scope of the CFAA. Prior to *Van Buren*, a number of federal appellate courts including the First, Fifth, Seventh, and Eleventh Circuits had adopted a broad view of the CFAA where "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'" In contrast, several other courts, including the Second, Fourth, and Ninth Circuits, had more narrowly interpreted "exceeds authorized access," based on an understanding that the CFAA's central purpose is to criminalize hacking. These courts applied CFAA liability only to those who lacked any authorization to access a computer or website or those who were "authorized to access only certain data or files" but accessed "unauthorized data or files." In *Van Buren*, the Court appears to have interpreted the CFAA's scope in a manner roughly consistent with courts that had applied a narrow interpretation of the statute—reading "exceeds authorized access" to exclude an individual who merely obtains information from a computer for an inappropriate reason. *Van Buren* leaves questions regarding the scope of the statute unresolved: particularly whether an individual's authorization to use a computer or information on a computer may be limited solely by technological barriers such as password requirements, or also by contractual terms such as computer use policies or terms of service [ToS].

Terms of Service [ToS]/Contractual Violations Following *Van Buren*

In *Van Buren*, an issue that the government and Van Buren addressed in their briefs, and that arose at oral argument, was the extent to which a broader interpretation of the CFAA—authorizing criminal liability where an individual accesses information on a computer for improper *purposes*—would criminalize violating contractual computer-use restrictions such as ToS agreements or employer computer-use policies. The question could have significant ramifications given the prevalence of such contractual restrictions on the internet, in the workplace, and elsewhere.

In many respects, *Van Buren* appears to foreclose imposing CFAA liability for mere violations of contractual computer-use or ToS violations. To the extent a contractual restriction such as a ToS limits the *purposes* for which an individual may access information on a computer—such as Van Buren's employer policy limiting access to the law enforcement database for official purposes—violating such restrictions would not incur CFAA liability under *Van Buren*.

However, in footnote eight of *Van Buren*, the Court seemingly left open the possibility that violations of ToS or other contractual limitations could run afoul of the CFAA in at least *some* circumstances. There, the Court expressly declined to consider whether authorization "turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." Although the majority describes authorization under the CFAA as "a gates-up-or-down inquiry" where "one either can or cannot access a computer system, and one either can or cannot access certain areas within the system," footnote eight appears to blur the contours of "authorization." The footnote suggests that the limits of authorization—the "gate"—may be set by technology *or* language—such as through ToS or other contractual restrictions.

Various interpretations of footnote eight are possible. One is that an individual may incur CFAA liability if he violates ToS or other contractual restrictions when those limitations apply not to the *purposes* for which information may be accessed, but rather the scope of accessible *information* itself. For example, under *Van Buren*, an employee who plays a game on his work computer in violation of an employer policy restricting computer use to business purposes would not violate the CFAA. Conversely, footnote eight suggests that at least theoretically, that same employee could violate the statute if he "plays a round of solitaire" in violation of an employer policy that "categorically prohibits accessing the 'games' folder in Windows," even if that folder were not also separately protected by a technological barrier like a password requirement. However, numerous passages in *Van Buren* seemingly contradict such a reading of footnote eight, such as excerpts suggesting that CFAA violations require some kind of hacking—that is, "trespassing into computer systems or data." In addition, the Court's summary of the adverse policy consequences of permitting CFAA liability for ToS violations and similar conduct provides some additional evidence that the Court may have intended to foreclose application of the statute in that context. A legal scholar cited throughout *Van Buren* has speculated about a second possible interpretation of footnote eight—"a mostly technological test" that may also "be impacted by written restrictions." This inquiry could involve looking to not just the technological restrictions in place, but also the context in which they are imposed, including the presence of other contractual limitations or permissions. For example, an entity may use a password requirement to restrict access. However, the extent to which that password requirement restricts authorization for CFAA purposes could conceivably be limited if, for instance, that entity shares the password and has a policy permitting individuals to use it. A third possibility is that footnote eight accommodates lower court precedential decisions that held that a company may sometimes revoke an individual's authorization by sending a cease and desist letter for conduct in violation of a ToS, presumably even without imposing a technological barrier. Shortly after the *Van Buren* opinion, the Court vacated and remanded (for further consideration in light of *Van Buren*) a Ninth Circuit decision addressing the issue of whether a cease and desist letter was sufficient to cut off a user's authorization for CFAA purposes. *Van Buren* leaves at least some ambiguity remaining with respect to whether violations of contractual restrictions like ToS may incur CFAA liability, an issue Congress might examine. More generally, Congress might examine amending the definitions of "without authorization" and "exceeds authorized access" to indicate whether an individual must bypass a technological barrier.

The CFAA and the Insider Threat After *Van Buren*

One concern that punctuated the briefs and oral argument in *Van Buren* was the applicability of the CFAA to the threats posed by insiders such as rogue employees with access to sensitive or confidential information on a computer, who use that access to misappropriate or disclose that information. For example, at oral arguments, Justice Alito asked whether a narrow reading of the CFAA would leave inadequate protection against insiders such as government employees or "the person in the fraud detection section of a bank" from using their access to sensitive information for nefarious purposes. Under *Van Buren*, the CFAA would reach insider conduct if it involves the use of a computer or information on a computer that the insider has no right to access. However, *Van Buren* clarifies that the CFAA does not extend to insider threats where the insider obtains information he is permitted to access, even if he does so for impermissible purposes. In the context of the rogue employee, for instance, if he is authorized to obtain his employer's business records for an official purpose such as billing, he will not violate the CFAA if he instead obtains them to sell to a competitor or foreign government.

Such conduct could still have adverse consequences. Most obviously, the individual may be terminated—which happened to Van Buren. In addition, state laws such as those governing trade secrets could conceivably apply. At the federal level, various statutes might be relevant depending on the nature of the conduct and information. Espionage statutes protect certain classified material and defense information, for example. Alternatively, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

limits disclosure of "protected health information." Federal criminal law prohibits the theft of trade secrets. Also, if the misappropriation of information involves the internet and a scheme to defraud—interpreted by courts to include depriving someone of money or property by "dishonest methods" such as trickery or deceit—it could implicate the federal wire fraud statute. Not all data misappropriation by an insider will necessarily involve such motives or information subject to specific protections as a trade secret, defense information, protected health information, or under another statute. To the extent this leaves a gap where certain aspects of the insider threat are not covered by federal law, Congress might examine whether legislation is needed to address the insider threat. Recent proposals examining specific aspects of this threat include the Safeguarding American Innovation Act (S. 1351; 117th Congress) and the Keep America Secure Act (H.R. 8390; 116th Congress), both of which focus on certain categories of insiders with access to government data.

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer