AN A.S. PRATT PUBLICATION
JANUARY 2021
VOL. 7 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 1** **JANUARY 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Could Filling Out a Fantasy Football Lineup Land You in Federal Prison?

By Josh H. Roberts [*]

In a case currently before the U.S. Supreme Court, the Court has been asked to interpret what it means to "exceed authorized access" to a computer under the Computer Fraud and Abuse Act. Whether a citizen can be criminally convicted of a federal felony, or subject to a civil judgment, hinges on how that phrase is interpreted. The author of this article discusses the arguments on both sides.

It is not the job of the U.S. Supreme Court to fix opaque statutes. That is Congress's job. But in deciding *Van Buren v. United States* (oral argument was heard on November 30, 2020), the nine Justices were called upon to decide the meaning of a phrase in a federal statute that could be interpreted to criminalize conduct as pedestrian as filling out a fantasy football lineup from your company computer. The case requires the Supreme Court to interpret what it means to "exceed authorized access" to a computer under the Computer Fraud and Abuse Act[1] ("CFAA").

The interpretation of this phrase has sharply divided the U.S. Circuit Courts of Appeals over the last decade. The resolution of the split will require a majority of the Court to either agree on the plain meaning of a phrase over which there is broad disagreement or apply substantive canons of statutory interpretation on the outer limits of textualism.

Among other things, CFAA creates criminal and civil liability for any person who "intentionally accesses a computer without authorization or *exceeds authorized access*, and thereby obtains . . . information from any protected computer."[2] The statute defines the term "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."[3] Whether a citizen can be criminally convicted of a federal felony, or subject to a civil judgment, hinges on how that phrase is interpreted. And there are good arguments on both sides.

---

[*] Josh H. Roberts, a partner at Holland & Knight LLP, and the executive partner of the Jacksonville office, is a civil trial attorney with broad commercial litigation experience throughout Florida's state and federal courts. Mr. Roberts represents clients in trade secrets litigation, real estate and construction litigation, banking litigation, class actions and typical business disputes. He may be contacted at joshua.roberts@hklaw.com.

[1] 18 U.S.C. § 1030.

[2] 18 U.S.C. § 1030(a)(2) (emphasis added); *see also* 18 U.S.C. § 1030 (e)(2) (a protected computer is one "used in . . . interstate or foreign commerce or communication" which is any computer connected to the internet).

[3] *Id.* § 1030(e)(6).

THE PLAIN LANGUAGE OF THE STATUTE'S TEXT IS INCONCLUSIVE, BUT TIPS IN FAVOR OF A BROAD INTERPRETATION

The interpretation of a federal statute begins with the plain language of the statute itself. Some contend that this is a "plainly written statute" under which it "is perfectly clear" that "an individual who is authorized to use a computer *for certain purposes* but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.'"[4] However, a person obtains information from a website whenever it is visited and that person's computer downloads digital content and other information from the host server. Thus under a broad interpretation, if an employee is permitted to log into his computer to conduct legal research, but then uses his web browser to visit ESPN.com to check sports scores and fill out a fantasy football lineup in violation of a computer use policy, he may have committed a federal crime.

Other courts contend that the text "clearly" indicates a much more restrictive meaning: that "one who is authorized to access a computer does not exceed her authorized access by violating an employer's restrictions on the *use* of information once it is validly accessed."[5]

Many courts disagree that the language is susceptible to only a single meaning. The U.S. Court of Appeals for the Second Circuit found that whether an individual "exceeds authorized access" to a computer could reasonably be interpreted in either of two ways: (i) when, with an improper and unpermitted *purpose*, one accesses a computer to obtain or alter information that he is otherwise authorized to access (i.e., broad), or (ii) only when he obtains or alters information that he *does not have authorization to access for any purpose* which is located on a computer that he is otherwise authorized to access (i.e., narrow).[6]

In other words, under the broad interpretation of "exceeding authorized access," one's authority to obtain information can be conditional, based upon the reason or purposes for which the person is accessing the information. On the other hand, the phrase can be interpreted narrowly as an all-or-nothing proposition wherein, if one has authorization to access a computer at all, his use of the information that he obtains from that computer is irrelevant.

---

[4] *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012) (en banc) (Silverman, J., dissenting) (emphasis added).

[5] *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft,* 974 F.3d 756, 761 (6th Cir. 2020), *petition for cert. filed*, ---- U.S.L.W. --- (U.S. Oct. 30, 2020) (20-575).

[6] *United States v. Valle*, 807 F.3d 508, 511-12 (2d Cir. 2012); *see also Nosal*, 676 F.3d at 856–57.

The Interpretation of This Phrase Has Deeply Divided the Circuit Courts of Appeals

Eight circuits have wrestled over the interpretation of this phrase for more than a decade.[7] The current trend among circuit courts is to apply a narrow interpretation.

Most recently, the U.S. Court of Appeals for the Sixth Circuit adopted a narrow interpretation of the phrase, relying on the statute's text alone.[8] In doing so, it joined the U.S. Courts of Appeals for the Second, Fourth, and Ninth Circuits which have all adopted a narrow interpretation; although they based their holdings on a substantive canon used in statutory interpretation referred to as the rule of lenity.[9]

On the other hand, the U.S. Courts of Appeals for the First, Fifth, Seventh, and Eleventh Circuits have adopted a broad interpretation.[10] The first step often taken by these courts and others in exploring the meaning of this elusive phrase is to analyze the statute's plain text.

Attempt to Ascertain Intent from Use of the Word "Authorization"

In trying to discern the meaning of "exceeds authorized access" through a textual analysis, the Second Circuit focused on the word "authorization" in the statutory clause that defines who is liable as anyone who "intentionally accesses a computer without authorization or exceeds authorized access. . . ."[11] The court found that the phrase "'without authorization' most naturally refers to a scenario where a user lacks permission to access the computer *at all*. . . ."[12] Accordingly, "one sensible reading of the statute is that 'exceeds authorized access' is complementary, referring to a scenario where a user has permission to access *the computer*, but proceeds to 'exceed' the parameters of authorized access by entering an area of the computer to which his authorization does not extend."[13] An example would be a secretary who has authority to log into a company

[7] *Valle*, 807 F.3d at 524 (emphasis added).

[8] *Royal Truck*, 974 F.3d at 760 (concluding that CFAA's aim "is penalizing those who breach cyber barriers without permission, rather than policing those who misuse the data they are authorized to obtain").

[9] *See id.* at 527-28; *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012), *cert. dismissed*, 568 U.S. 1079 (2013); *Nosal*, 676 F.3d at 862-63.

[10] *See United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (finding that employee's breach of duty of loyalty immediately terminated his agency, and with it, his authority to access the laptop); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (finding that former employee exceeded authorized access by improperly using information gleaned during prior employment in violation of broad confidentiality agreement to make sense of data "scraped" from plaintiff's website).

[11] 18 U.S.C. § 1030(a)(2).

[12] *Valle*, 807 F.3d at 524 (emphasis added).

[13] *Id.*

computer network to check emails and save basic research memorandums, but uses that access to enter the restricted human resource drive that houses sensitive data containing employees medical records and salary information.

Courts justify this narrow interpretation on the basis that both prohibitions apply to hackers: "Without authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access information or files that they are prohibited from accessing).[14]

Under a similar text-based analysis, the Fourth Circuit found that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer.[15] According to the *WEC* court, an employee accesses a computer "without authorization" when he gains admission to a computer without approval and "exceeds authorized access" when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access.[16] Walking a fine line, the *WEC* court focused on physical constraints to access, noting that "neither of these definitions extends to the improper *use* of information validly accessed."[17]

The problem with limiting the definition of "exceeds authorized access" to scenarios in which the accesser has no authority *whatsoever* to access the information is that nothing in the text of the statute limits the definition in this way. Instead, the definition appears broader, and applies to accessers who use their authorized access to a computer in order to obtain or alter information that they are "not entitled so to obtain or alter." Arguably, entitlement to obtain or alter information can be conditioned upon the purpose for which one is obtaining or altering that information.

What Can Be Gleaned from Use of the Word "Entitled"?

Analysis of the statute must then move to use of the word "entitled" in the phrase's definition "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." Proponents of a broad interpretation turn to the *Webster's New Riverside University Dictionary*, which defines "entitle" as "to furnish with a right."[18] A computer use policy furnishes certain limited rights to access computers to obtain or alter information on

[14] *Id*. (citing *Nosal*, 676 F.3d at 858).

[15] *WEC*, 687 F.3d at 204 (basing its finding on the *Oxford English Dictionary*'s definition of the "authorization" as a "formal warrant, or sanction").

[16] *Id*.

[17] *Id*.

[18] *Nosal*, 676 F.3d at 857.

that computer system, but when data is obtained for a prohibited purpose, such as to send it to a competitor, a user has no right (i.e., no entitlement) to obtain or alter the data.[19] Placing conditions upon one's rights to obtain or alter information seems like a reasonable proposition. "This is not an esoteric concept."[20] However, according to the *Nosal* majority, this argument fails because "entitled" in the statutory text refers to *how an accesser obtains* the information, while the computer policy limits *how the information is used* after it is obtained.[21] On further scrutiny, this appears to be a dubious distinction based on an assumption that entitlement to obtain information cannot be conditioned upon intended use of the information.

Conflicting Interpretations of the Significance of the Word "So"

A third textual approach to unlock the statute's meaning focuses on the word "so" in the definition "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."[22] In *Royal Truck*, the Sixth Circuit found Congress's use of the word "so" "particularly instructive," explaining that it operates as an adverb meaning "in the way or manner described, indicated, or suggested."[23] The court found that the placement of "so" near the end of the definition refers back to the antecedent "with authorization" found earlier in the definition.[24] According to the court's analysis, "one who exceeds authorized access has permission to enter a computer for specific purposes, yet later obtains (or alters) information for which access has not been authorized."[25] Here, the Sixth Circuit reframes, and fundamentally changes, the definition of "exceeds authorized access" to apply only when one obtains or alters information "for which *access has not been authorized.*"

If Congress intended the definition to apply narrowly, only when one obtains (or alters) information from computers or files for which access has not been authorized whatsoever, it could have easily said so. But it did not. Resort to changing the definition highlights the shortcomings of the Sixth Circuit's analysis. The definition provided by Congress prohibits the accesser from obtaining or altering data which it "*is not entitled*"

[19] *Id.*

[20] *Id.* at 865 (Silverman, J., dissenting) ("A bank teller is entitled to access a bank's money for legitimate banking purposes, but not to take the bank's money for himself. . . . A person of ordinary intelligence understands that he may be totally prohibited from doing something *altogether*, or authorized to do something but prohibited from going *beyond* what is authorized.").

[21] *Id.* at 857.

[22] *Royal Truck*, 974 F.3d at 760 (adopting the narrow interpretation based on the text of the statute alone); *see also WEC*, 687 F.3d at 205.

[23] *Id.*

[24] *Id.*

[25] *Id.*

to obtain or alter. There is a fundamental difference between obtaining information from a location "for which *access has not been authorized*" and obtaining information which one is "not entitled" to obtain.

On the other end of the spectrum, advocates for a broad interpretation also cite the significance of the word "so" and agree that it means "in a manner or way that is indicated or suggested."[26] However, under their analysis, an employee would exceed authorized access if he uses such access to obtain or alter information on the computer that he is not entitled in that manner to obtain or alter.[27] Under this reasoning, a person violates CFAA if he obtains or alters information in a manner inconsistent with the computer policy.

Even if the word "so" is interpreted to mean "in that manner," it does not necessarily refer to violations of use policies. It could also be interpreted to refer to the physical manner in which the person accessed the computer and information. For instance, an employee has complete access to information with his own username and password, but accesses information using another employee's username and password in violation of company policy.[28] In that case, the employee obtains information "in a manner" that is not authorized, but that has nothing to do with the purpose for which he accessed the data.[29]

Resolving the interpretation of CFAA based upon the use and placement of the word "so" places too great of a "weight on a two-letter word that is essentially a conjunction."[30]

If this sharp division among the Circuits' interpretation of "exceeds authorized access" means anything, "it is that the statute is readily susceptible to different interpretations."[31] In such cases, courts turn to the legislative history and motivating policies for guidance.

THE LEGISLATIVE HISTORY AND MOTIVATING POLICIES ARE INCONCLUSIVE, BUT SHIFT THE BALANCE SLIGHTLY TOWARD A NARROW READING

Congress enacted the predecessor to CFAA in 1984 to address "computer crime," which was then principally understood as "hacking" or trespassing into computer systems or data.[32]

---

[26] *WEC*, 687 F.3d 204-05.

[27] *Id*. (discussing analysis found in the panel decision in *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012)).

[28] *WEC*, 687 F.3d 205.

[29] *Id*.

[30] *Nosal*, 676 F.3d at 857 ("If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions – which may well include everyone who uses a computer – we would expect it to use language better suited to that purpose.").

[31] *Valle,* 807 F.3d at 524-25.

[32] *Valle,* 807 F.3d at 525 (citing H.R. Rep. No. 98-894, at 3691-92, 3695-97 (1984); S. Rep. No. 99-432, at 2480 (1986)).

To put the timing of this law in context, CFAA was originally enacted in 1984. At that time, a standard protocol for the internet had yet to be established, and Apple had just introduced its Macintosh computer, which was the first mouse-driven computer with a graphical user interface.[33]

The House Committee Report to the original bill:

> (i) warned of "'hackers' who have been able to access (trespass into) both private and public computer systems;"[34]
>
> (ii) noted the "recent flurry of electronic trespassing incidents;"[35]
>
> (iii) described one instance of "computer crime" in which an individual "stole confidential software by tapping into the computer system of a previous employer from [the] defendant's remote terminal;"[36] and
>
> (iv) advised that "section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering'. . . ."[37]

The Senate Committee Report to the 1986 amendments to CFAA shed some additional light on the subject. There, the Senate: (i) described "exceeds authorized access" in terms of trespassing into computer systems or files;[38] (ii) clarified that it did not want to hold liable those "who inadvertently 'stumble into' someone else's computer file or computer data . . . in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer or data file that happens to be accessible from the same terminal;"[39] and (iii) explains that the premise of § 1030(a)(2) is privacy protection, and physical removal of the data from its original location need not be proved to establish a violation of the subsection.[40]

In short, the legislative history "consistently characterizes the evil to be remedied – computer crime – as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend."[41] Throughout the Senate and House Reports, reference is made to

---

[33] *See Timeline of Computer History*, Computer History Museum, https://www.computerhistory.org/timeline/1984/ (last visited on Oct. 30, 2020).

[34] *See* H.R. Rep. No. 98-894, at 3695.

[35] *Id.* at 3696.

[36] *Id.* at 3691-92.

[37] *Id.* at 3706.

[38] *Valle*, 807 F.3d at 525.

[39] S. Rep. 99-432, at 2483.

[40] *Id.* at 2484.

[41] *Valle*, 807 F.3d at 525.

accessing computer terminals that one is not permitted to access.[42] The Senate Report referred to "authorization in spatial terms, namely, an employee going beyond the parameters of his access rights" or logging into a database that he had no right to access.[43]

Accordingly, the legislative history tips in favor of the narrow interpretation, focused on the right of access to the computer or data in the first place. This approach punishes unauthorized access that is akin to the crimes of trespassing, or breaking and entering. One could argue that Congress, through its silence, left the misappropriation or prohibited use of the data to the law governing contracts and torts, along with state statutes governing trade secrets. However, Congress was also clearly concerned about the theft and abuse of electronically stored data.[44] Downloading sensitive customer information to provide it to a competitor implicates this concern, even if the existing employee used an active username and password to access the data, and would have otherwise been permitted to access the data for business purposes. The legislative history shifts the balance slightly in favor of a narrow interpretation, but does not definitively resolve the question.

FAIRNESS AND NOTICE CONCERNS FAVOR A NARROW INTERPRETATION, BUT THESE ARE ISSUES MORE APPROPRIATELY DETERMINED BY THE LEGISLATURE THAN THE JUDICIARY

The hand-wringing over the interpretation of "exceeds authorized access" is due in large part to the unfortunate ramifications of a broad interpretation of the phrase. It is reasonable to believe that entitlement to obtain or alter information can be conditional on one's purpose for obtaining or altering the information, and one exceeds authorized access when they obtain or alter the information for an unpermitted purpose. However, when applied in the real world, the broad interpretation goes too far, is unjust, and creates vagueness and notice problems, allowing federal criminal and civil liability to be based upon the fine print in private corporate policies that are subject to change without notice.

The fairness concerns played a prominent role in the *Nosal*, *WEC*, and *Valle* decisions, in which the courts found that a broad interpretation "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute" and "would expand its scope far beyond computer hacking to criminalize any unauthorized use of

[42] *See* S. Rep. No. 99-432, at 2486 ("The danger existed that [the bill amending CFAA], as originally introduced, might cover every employee who happens to sit down, within his department, at a computer terminal which he is not officially authorized to use.").

[43] *Valle*, 807 F.3d at 526.

[44] *See* S. Rep. No. 99-432, at 2480 ("The proliferation of computers and computer data has spread before the nation's criminals a vast array of property that, in many cases, is wholly unprotected against crime.").

information obtained from a computer."[45] The *Nosal* court was concerned that such an interpretation would "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[46] It framed its concern as a notice issue:

> Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read. Consider the typical corporate policy that computers can be used only for business purposes. What exactly is a "nonbusiness purpose"? If you use the computer to check the weather report for a business trip? For the company softball game? For your vacation to Hawaii? And if minor personal uses are tolerated, how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?[47]

The impact that "CFAA has on workplace conduct pales by comparison with its effect on everyone else who uses a computer, smart-phone, iPad, Kindle, Nook, X-box, Blu–Ray player or any other Internet-enabled device."[48] In 1984, Congress could not have imagined what nearly 35 years of technological advancements would bring. It is unlikely that it anticipated logging into a computer would put the world of information at your fingertips or the internet of things, in which, as is the case today, even lightbulbs and refrigerators are connected to the internet. "Whenever we access a web page, commence a download, post a message on somebody's Facebook wall, shop on Amazon, bid on eBay, publish a blog, rate a movie on IMDb, read www.NYT.com, watch YouTube and do the thousands of other things we routinely do online, we are using one computer to send commands to other computers at remote locations."[49] Access to those computers is often governed by private policies.[50] The *Nosal* court provided some examples:

- Google forbade minors from using its services;
- Facebook's policies prohibited allowing others to log into your account;

[45] *Nosal*, 676 F.3d at 857-59; *see also WEC*, 687 F.3d at 207 ("[W]e 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."); *Valle*, 807 F.3d at 527 ("We agree with the Ninth and Fourth Circuits that courts that have adopted the broader construction looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access." (internal quotations omitted)).

[46] *Nosal*, 676 F.3d at 859.

[47] *Id.* at 860.

[48] *Id.* at 860–61.

[49] *Id.* at 861.

[50] *Id.*

- The dating site eHarmony's terms of service state that "[y]ou will not provide inaccurate, misleading or false information to eHarmony or to any other user"; and
- eBay and Craigslist make it a violation of the terms of use to post items in an inappropriate category.[51]

Arguably, violation of any of those policies could subject one to criminal liability. This has "the odd effect of allowing employers, rather than Congress, to define the scope of criminal liability by operation of their employee computer-use policies."[52] If Congress intended to effectively criminalize violations of an employee handbook, it would have said so in clear terms.[53] The *Nosal* court rightly rejected the government's assurances that prosecutors will not pursue minor violations, refusing to accept a position that rises or falls on the "mercy of our local prosecutor."[54]

After reviewing the statute's text, legislative history, and motivating principles, and finding that the phrase "exceeds authorized access" is susceptible to two different interpretations, the Second, Fourth, and Ninth Circuits applied the rule of lenity. Under that "long-standing principle," when ordinary tools of legislative construction fail to establish that an interpretation of a criminal statute is unambiguously correct, the rule of lenity requires courts to "construe ambiguous criminal statutes narrowly so as to avoid making criminal law in Congress's stead."[55]

The Sixth Circuit, finding that the text was sufficiently clear, adopted the narrow interpretation.[56]

The First, Fifth, Seventh, and Eleventh Circuits also relied on the text of the statute, but came out the opposite way, adopting a broad interpretation in which violations of private computer use policies can lead to criminal and civil liability.[57]

---

[51] *Id*. at 861-62.

[52] *Royal Truck*, 974 F.3d 762.

[53] *Id*.

[54] *Id.* at 862.

[55] *Nosal*, 676 F.3d at 862-63 (internal quotations and citations omitted); *see also WEC*, 687 F.3d at 207; *Valle*, 807 F.3d at 526.

[56] *Royal Truck*, 974 F.3d at 761 ("Given this plain understanding of the CFAA's terms, we need not rely on the rule of lenity. . . . Out of respect for Congress's textual choices, we turn to the rule of lenity only when, unlike here, statutory language cannot otherwise be reconciled.").

[57] *See John*, 597 at 272; *Rodriguez*, 628 F.3d at 1258; *Int'l Airport Ctrs.*, 440 F.3d at 418 *EF Cultural Travel*, 274 F.3d at 577.

IN LIGHT OF THIS SHARP DIVIDE, *VAN BUREN V. UNITED STATES* WILL PRESENT AN INTERESTING TEST FOR A COURT GUIDED BY TEXTUALISM

A resolution to the circuit split is on the horizon. The U.S. Supreme Court granted certiorari in *Van Buren v. United State*s, a case out of the Eleventh Circuit hinging on the interpretation of what it means to "exceed authorized access."[58]

In *Van Buren*, petitioner Nathan Van Buren, a sergeant with the city police department in Cumming, Georgia, developed a relationship with a man named Andrew Albo.[59] Van Buren's relationship with Albo strengthened over time such that Van Buren felt comfortable asking Albo for a loan.[60] However, Albo surreptitiously recorded his conversations with Van Buren and presented the recording of Van Buren's loan request to a detective in the Forsyth County Sheriff's Office.[61] Albo told the detective that Van Buren was shaking him down for his money, which spurred an investigation that came to the attention of the FBI.

As part of a FBI sting operation, Albo recorded another conversation with Van Buren wherein Albo asked if, in exchange for the money, Van Buren would determine whether a woman who Albo had met at a strip club was an undercover police officer.[62] Ultimately, Van Buren searched for the woman using the Georgia Crime Information Center ("GCIC") database, an official government databased maintained by the Georgia Bureau of Investigation and connected to the National Crime Information Center.[63]

Although Van Buren was authorized to use the GCIC for law-enforcement purposes only, the government claimed that he was not permitted to use the database to perform searches for his friend. On the basis that he "exceeded authorized access," Van Buren was tried and convicted of, *inter alia*, a felony under the CFAA.[64]

On appeal to the Eleventh Circuit, Van Buren argued that a person with *authority to access* a computer cannot be guilty of violating CFAA by accessing the information for an improper purpose or subsequently *misusing* the information obtained.[65] Van Buren claimed that obtaining information from a computer that one is authorized to access does not violate CFAA, even if the information was obtained for a nonbusiness

[58] *See United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667, 206 L. Ed. 2d 822 (2020).

[59] *Id*. at 1197.

[60] *Id*.

[61] *Id*.

[62] *Id*.

[63] *Id*. at 1198.

[64] *Id*. at 1205.

[65] *Id.* at 1206.

or inappropriate reason.[66] The Eleventh Circuit was constrained by *United States v. Rodriguez*,[67] where it held that "even a person with authority to access a computer can be guilty of computer fraud if that person subsequently misuses the computer."[68]

In *Rodriguez* and *Van Buren*, the Eleventh Circuit applied the broad interpretation, holding that one "exceeds authorized access" to a computer under CFAA when he obtains or alters information in violation of the rules, restrictions and policies governing use of the computer and data. Van Buren was authorized to access the GCIC to run the plates of a car pulled over for a traffic stop, but when he entered the same GCIC database to do research on a person for purposes unrelated to his professional duties, he exceeded authorized access.

WILL THE SUPREME COURT'S FINAL DECISION IN *VAN BUREN* MAKE FEDERAL CRIMINALS OF US ALL?

Now, the Supreme Court is poised to weigh in, and hopefully resolve the circuit split. *Van Buren* will present an interesting test for the self-described textualist Court. As Justice Kagan declared in her eulogy of Antonin Scalia: "We are all textualists now." The newly configured Supreme Court with the addition of staunch textualist Justice Amy Coney Barrett only increases the Court's allegiance to textualism. Justice Barrett has observed that the rule of lenity, which the Second, Fourth, and Ninth Circuits relied upon in reaching their narrow interpretation, could be in tension with a strict textualist approach.[69] But obtaining broad agreement about the plain meaning of the statute's text will be difficult. Will the nine Justices agree on the "plain meaning" of the statute, despite wide disagreement in the lower courts? Or will the statute's ambiguity persuade the Court to apply the substantive canon of lenity to avoid the unfortunate consequences of a broad interpretation left unresolved by Congress?

---

[66] *Id.* at 1207.

[67] 628 F.3d 1258 (11th Cir. 2010).

[68] *Id.*

[69] *See* Amy Coney Barrett, *Substantive Canons and Faithful Agency*, 90 B.U. L. Rev. 109, 110, 166-67 (2010).