Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.,* 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

VAN BUREN *v.* UNITED STATES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

No. 19–783. Argued November 30, 2020—Decided June 3, 2021

Former Georgia police sergeant Nathan Van Buren used his patrol-car computer to access a law enforcement database to retrieve information about a particular license plate number in exchange for money. Although Van Buren used his own, valid credentials to perform the search, his conduct violated a department policy against obtaining database information for non-law-enforcement purposes. Unbeknownst to Van Buren, his actions were part of a Federal Bureau of Investigation sting operation. Van Buren was charged with a felony violation of the Computer Fraud and Abuse Act of 1986 (CFAA), which subjects to criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access." 18 U. S. C. §1030(a)(2). The term "exceeds authorized access" is defined 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." §1030(e)(6). A jury convicted Van Buren, and the District Court sentenced him to 18 months in prison. Van Buren appealed to the Eleventh Circuit, arguing that the "exceeds authorized access" clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have. Consistent with Eleventh Circuit precedent, the panel held that Van Buren had violated the CFAA.

Held: An individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to him. Pp. 5–20.

(a) (1) The parties agree that Van Buren "access[ed] a computer with authorization" and "obtain[ed] . . . information in the computer." They

dispute whether Van Buren was "entitled so to obtain" that information. Van Buren contends that the word "so" serves as a term of reference and that the disputed phrase thus asks whether one has the right, in "the same manner as has been stated," to obtain the relevant information. Black's Law Dictionary 1246. He also notes that the only manner of obtaining information already stated in the definitional provision is by a computer one is authorized to access. Thus, he continues, the phrase "is not entitled so to obtain" plainly refers to information one is not allowed to obtain *by using a computer that he is authorized to access*. The Government argues that "so" sweeps more broadly, reading the phrase "is not entitled so to obtain" to refer to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*. And the manner or circumstances in which one has a right to obtain information, the Government says, are defined by any "specifically and explicitly" communicated limits on one's right to access information. Van Buren's account of "so" best aligns with the term's plain meaning as a term of reference, as further reflected by other federal statutes that use "so" the same way. Pp. 5–8.

(2) The Government contends that Van Buren's reading renders the word "so" superfluous. "So" makes a valuable contribution, the Government insists, only if it incorporates all of the circumstances that might qualify a person's right to obtain information. The Court disagrees because without "so," the statute could be read to incorporate all kinds of limitations on one's entitlement to information. Pp. 8–9.

(3) The dissent accepts Van Buren's definition of "so," but would arrive at the Government's result by way of the word "entitled." According to the dissent, the term "entitled" demands a "circumstance dependent" analysis of whether access was proper. But the word "entitled" is modified by the phrase "so to obtain." That phrase in turn directs the reader to consider a specific limitation on the accesser's entitlement: his entitlement to obtain the information "in the manner previously stated." And as already explained, the manner previously stated is using a computer one is authorized to access. To arrive at its interpretation, the dissent must write the word "so" out of the statute. Pp. 9–10.

(4) The Government contends that in "common parlance," the phrase "exceeds authorized access" would be understood to mean that Van Buren "exceed[ed] his authorized access" to the law enforcement database when he obtained license-plate information for personal purposes. The relevant question, however, is not whether Van Buren exceeded his authorized access but whether he exceeded his authorized access *as the CFAA defines that phrase*. For reasons given elsewhere, he did not. Nor is it contrary to the meaning of the defined term to

equate "exceed[ing] authorized access" with the act of entering a part of the system to which a computer user lacks access privileges. Pp. 11–12.

(b) The statute's structure further cuts against the Government's position. Subsection (a)(2) specifies two distinct ways of obtaining information unlawfully—first, when an individual "accesses a computer without authorization," §1030(a)(2), and second, when an individual "exceeds authorized access" by accessing a computer "with authorization" and then obtaining information he is "not entitled so to obtain," §§1030(a)(2), (e)(6). Van Buren contends that the "without authorization" clause protects computers themselves from outside hackers, while the "exceeds authorized access" clause provides complementary protection for certain information within computers by targeting so-called inside hackers. Under Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system. This treats the clauses consistently and aligns with the computer-context understanding of access as entry. By contrast, the Government proposes to read the first phrase "without authorization" as a gates-up-or-down inquiry and the second phrase "exceeds authorized access" as dependent on the circumstances—a reading inconsistent with subsection (a)(2)'s design and structure. The Government's reading leaves unanswered why the statute would prohibit accessing computer information, but not the computer itself, for an improper purpose.

Another structural problem for the Government: §1030(a)(2) also gives rise to civil liability, §1030(g), with the statute defining "damage" and "loss" to specify what a plaintiff in a civil suit can recover. §§1030(e)(8), (11). Both terms focus on technological harms to computer data or systems. Such provisions make sense in a scheme aimed at avoiding the ordinary consequences of hacking but are ill fitted to remediating "misuse" of sensitive information that employees permissibly access using their computers. Pp. 12–16.

(c) The Government's claims that precedent and statutory history support its interpretation are easily dispatched. This Court's decision in *Musacchio* v. *United States*, 577 U. S. 237, did not address the issue here, and the Court is not bound to follow any dicta in the case. As for statutory history, the Government claims that the original 1984 Act's precursor to the "exceeds authorized access" language—which covered any person who, "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend"—supports its reading. But that Congress removed any reference to "purpose" in the CFAA cuts against reading the statute to cover purpose-based limitations. Pp. 16–17.

Syllabus

(d) The Government's interpretation of the "exceeds authorized access" clause would attach criminal penalties to a breathtaking amount of commonplace computer activity. For instance, employers commonly state that computers and electronic devices can be used only for business purposes. On the Government's reading, an employee who sends a personal e-mail or reads the news using a work computer has violated the CFAA. The Government speculates that other provisions might limit its prosecutorial power, but its charging practice and policy indicate otherwise. The Government's approach would also inject arbitrariness into the assessment of criminal liability, because whether conduct like Van Buren's violated the CFAA would depend on how an employer phrased the policy violated (as a "use" restriction or an "access" restriction). Pp. 17–20.

940 F. 3d 1192, reversed and remanded.

BARRETT, J., delivered the opinion of the Court, in which BREYER, SOTOMAYOR, KAGAN, GORSUCH, and KAVANAUGH, JJ., joined. THOMAS, J., filed a dissenting opinion, in which ROBERTS, C. J., and ALITO, J., joined.

NOTICE: This opinion is subject to formal revision before publication in the preliminary print of the United States Reports. Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Washington, D. C. 20543, of any typographical or other formal errors, in order that corrections may be made before the preliminary print goes to press.

SUPREME COURT OF THE UNITED STATES

No. 19–783

NATHAN VAN BUREN, PETITIONER *v.*
UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

[June 3, 2021]

JUSTICE BARRETT delivered the opinion of the Court.

Nathan Van Buren, a former police sergeant, ran a license-plate search in a law enforcement computer database in exchange for money. Van Buren's conduct plainly flouted his department's policy, which authorized him to obtain database information only for law enforcement purposes. We must decide whether Van Buren also violated the Computer Fraud and Abuse Act of 1986 (CFAA), which makes it illegal "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."

He did not. This 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. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them.

I

A

Technological advances at the dawn of the 1980s brought

computers to schools, offices, and homes across the Nation. But as the public and private sectors harnessed the power of computing for improvement and innovation, so-called hackers hatched ways to coopt computers for illegal ends. After a series of highly publicized hackings captured the public's attention, it became clear that traditional theft and trespass statutes were ill suited to address cybercrimes that did not deprive computer owners of property in the traditional sense. See Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N. Y. U. L. Rev. 1596, 1605–1613 (2003).

Congress, following the lead of several States, responded by enacting the first federal computer-crime statute as part of the Comprehensive Crime Control Act of 1984. §2102(a), 98 Stat. 2190–2192. A few years later, Congress passed the CFAA, which included the provisions at issue in this case. The Act subjects to criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access," and thereby obtains computer information. 18 U. S. C. §1030(a)(2). It defines the term "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." §1030(e)(6).

Initially, subsection (a)(2)'s prohibition barred accessing only certain financial information. It has since expanded to cover any information from any computer "used in or affecting interstate or foreign commerce or communication." §1030(e)(2)(B). As a result, the prohibition now applies—at a minimum—to all information from all computers that connect to the Internet. §§1030(a)(2)(C), (e)(2)(B).

Those who violate §1030(a)(2) face penalties ranging from fines and misdemeanor sentences to imprisonment for up to 10 years. §1030(c)(2). They also risk civil liability under the CFAA's private cause of action, which allows persons suffering "damage" or "loss" from CFAA violations to sue for

money damages and equitable relief. §1030(g).

B

This case stems from Van Buren's time as a police sergeant in Georgia. In the course of his duties, Van Buren crossed paths with a man named Andrew Albo. The deputy chief of Van Buren's department considered Albo to be "very volatile" and warned officers in the department to deal with him carefully. Notwithstanding that warning, Van Buren developed a friendly relationship with Albo. Or so Van Buren thought when he went to Albo to ask for a personal loan. Unbeknownst to Van Buren, Albo secretly recorded that request and took it to the local sheriff's office, where he complained that Van Buren had sought to "shake him down" for cash.

The taped conversation made its way to the Federal Bureau of Investigation (FBI), which devised an operation to see how far Van Buren would go for money. The steps were straightforward: Albo would ask Van Buren to search the state law enforcement computer database for a license plate purportedly belonging to a woman whom Albo had met at a local strip club. Albo, no stranger to legal troubles, would tell Van Buren that he wanted to ensure that the woman was not in fact an undercover officer. In return for the search, Albo would pay Van Buren around $5,000.

Things went according to plan. Van Buren used his patrol-car computer to access the law enforcement database with his valid credentials. He searched the database for the license plate that Albo had provided. After obtaining the FBI-created license-plate entry, Van Buren told Albo that he had information to share.

The Federal Government then charged Van Buren with a felony violation of the CFAA on the ground that running the

license plate for Albo violated the "exceeds authorized access" clause of 18 U. S. C. §1030(a)(2).[1] The trial evidence showed that Van Buren had been trained not to use the law enforcement database for "an improper purpose," defined as "any personal use." App. 17. Van Buren therefore knew that the search breached department policy. And according to the Government, that violation of department policy also violated the CFAA. Consistent with that position, the Government told the jury that Van Buren's access of the database "for a non[-]law[-]enforcement purpose" violated the CFAA "concept" against "using" a computer network in a way contrary to "what your job or policy prohibits." *Id.,* at 39. The jury convicted Van Buren, and the District Court sentenced him to 18 months in prison.

Van Buren appealed to the Eleventh Circuit, arguing that the "exceeds authorized access" clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have. While several Circuits see the clause Van Buren's way, the Eleventh Circuit is among those that have taken a broader view.[2] Consistent with its Circuit precedent, the panel held that Van Buren had violated the CFAA by accessing the law enforcement database for an "inappropriate reason." 940 F. 3d 1192, 1208 (2019). We

---

[1] Van Buren also was charged with and convicted of honest-services wire fraud. In a separate holding not at issue here, the United States Court of Appeals for the Eleventh Circuit vacated Van Buren's honest-services fraud conviction as contrary to this Court's decision in *McDonnell* v. *United States*, 579 U. S. 550 (2016).

[2] Compare *Royal Truck & Trailer Sales & Serv., Inc.* v. *Kraft*, 974 F. 3d 756 (CA6 2020); *United States* v. *Valle*, 807 F. 3d 508 (CA2 2015); *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F. 3d 199 (CA4 2012); *United States* v. *Nosal*, 676 F. 3d 854 (CA9 2012) (en banc), with *United States* v. *Rodriguez*, 628 F. 3d 1258 (CA11 2010); *United States* v. *John*, 597 F. 3d 263 (CA5 2010); *International Airport Centers, L.L.C.* v. *Citrin*, 440 F. 3d 418 (CA7 2006); *EF Cultural Travel BV* v. *Explorica, Inc.*, 274 F. 3d 577 (CA1 2001).

granted certiorari to resolve the split in authority regarding the scope of liability under the CFAA's "exceeds authorized access" clause. 590 U. S. ___ (2020).

II

A

1

Both Van Buren and the Government raise a host of policy arguments to support their respective interpretations. But we start where we always do: with the text of the statute. Here, the most relevant text is the phrase "exceeds authorized access," which means "to access a computer with authorization and to use such access to obtain . . . information in the computer that the accesser is not entitled so to obtain." §1030(e)(6).

The parties agree that Van Buren "access[ed] a computer with authorization" when he used his patrol-car computer and valid credentials to log into the law enforcement database. They also agree that Van Buren "obtain[ed] . . . information in the computer" when he acquired the license-plate record for Albo. The dispute is whether Van Buren was "entitled so to obtain" the record.

"Entitle" means "to give . . . a title, right, or claim to something." Random House Dictionary of the English Language 649 (2d ed. 1987). See also Black's Law Dictionary 477 (5th ed. 1979) ("to give a right or legal title to"). The parties agree that Van Buren had been given the right to acquire license-plate information—that is, he was "entitled to obtain" it—from the law enforcement computer database. But was Van Buren "entitled *so* to obtain" the license-plate information, as the statute requires?

Van Buren says yes. He notes that "so," as used in this statute, serves as a term of reference that recalls "the same manner as has been stated" or "the way or manner described." Black's Law Dictionary, at 1246; 15 Oxford Eng-

lish Dictionary 887 (2d ed. 1989). The disputed phrase "entitled so to obtain" thus asks whether one has the right, in "the same manner as has been stated," to obtain the relevant information. And the only manner of obtaining information already stated in the definitional provision is "via a computer [one] is otherwise authorized to access." Reply Brief 3. Putting that together, Van Buren contends that the disputed phrase—"is not entitled *so* to obtain"—plainly refers to information one is not allowed to obtain *by using a computer that he is authorized to access*. On this reading, if a person has access to information stored in a computer—*e.g.,* in "Folder Y," from which the person could permissibly pull information—then he does not violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose. But if the information is instead located in prohibited "Folder X," to which the person lacks access, he violates the CFAA by obtaining such information.

The Government agrees that the statute uses "so" in the word's term-of-reference sense, but it argues that "so" sweeps more broadly. It reads the phrase "is not entitled *so* to obtain" to refer to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*. The manner or circumstances in which one has a right to obtain information, the Government says, are defined by any "specifically and explicitly" communicated limits on one's right to access information. Brief for United States 19. As the Government sees it, an employee might lawfully pull information from Folder Y in the morning for a permissible purpose—say, to prepare for a business meeting—but unlawfully pull the same information from Folder Y in the afternoon for a prohibited purpose—say, to help draft a resume to submit to a competitor employer.

The Government's interpretation has surface appeal but proves to be a sleight of hand. While highlighting that "so"

refers to a "manner or circumstance," the Government simultaneously ignores the definition's further instruction that such manner or circumstance already will "'ha[ve] been stated,'" "'asserted,'" or "'described.'" *Id.,* at 18 (quoting Black's Law Dictionary, at 1246; 15 Oxford English Dictionary, at 887). Under the Government's approach, the relevant circumstance—the one rendering a person's conduct illegal—is not identified earlier in the statute. Instead, "so" captures *any* circumstance-based limit appearing *anywhere*—in the United States Code, a state statute, a private agreement, or anywhere else. And while the Government tries to cabin its interpretation by suggesting that any such limit must be "specifically and explicitly" stated, "express," and "inherent in the authorization itself," the Government does not identify any textual basis for these guardrails. Brief for United States 19; Tr. of Oral Arg. 41.

Van Buren's account of "so"—namely, that "so" references the previously stated "manner or circumstance" in the text of §1030(e)(6) itself—is more plausible than the Government's. "So" is not a free-floating term that provides a hook for any limitation stated anywhere. It refers to a stated, identifiable proposition from the "preceding" text; indeed, "so" typically "[r]epresent[s]" a "word or phrase already employed," thereby avoiding the need for repetition. 15 Oxford English Dictionary, at 887; see Webster's Third New International Dictionary 2160 (1986) (so "often used as a substitute . . . to express the idea of a preceding phrase"). Myriad federal statutes illustrate this ordinary usage.[3] We agree

[3] See, *e.g.*, 7 U. S. C. §171(8) (authorizing Secretary of Agriculture "[t]o sell guayule or rubber processed from guayule and to use funds so obtained in replanting and maintaining an area"); 18 U. S. C. §648 (any person responsible for "safe-keeping of the public moneys" who "loans, uses, or converts to his own use . . . any portion of the public moneys . . . is guilty of embezzlement of the money so loaned, used, converted, deposited, or exchanged"); §1163 ("[W]hoever embezzles, steals, [or] knowingly converts to his use" money or property "belonging to any Indian tribal organization," or "[w]hoever, knowing any such moneys . . . or

with Van Buren: The 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.[4]

2

The Government's primary counterargument is that Van Buren's reading renders the word "so" superfluous. Recall the definition: "to access a computer with authorization and to use such access to obtain . . . information in the computer that the accesser is not entitled *so* to obtain." §1030(e)(6) (emphasis added). According to the Government, "so" adds nothing to the sentence if it refers solely to the earlier stated manner of obtaining the information through use of a computer one has accessed with authorization. What matters on Van Buren's reading, as the Government sees it, is simply that the person obtain information that he is not entitled to obtain—and that point could be made even if "so" were deleted. By contrast, the Government insists, "so" makes a valuable contribution if it incorporates all of the circumstances that might qualify a person's right to obtain information. Because only its interpretation gives "so"

---

other property to have been so embezzled, stolen, [or] converted . . . retains the same with intent to convert it to his use," is subject to punishment); §1708 ("[W]hoever steals, takes, or abstracts, or by fraud or deception obtains, or attempts so to obtain," parcels of mail is subject to punishment).

[4]The dissent criticizes this interpretation as inconsistent with "basic principles of property law," and in particular the "familiar rule that an entitlement to use another person's property is circumstance specific." *Post*, at 4–5 (opinion of THOMAS, J.). But common-law principles "should be imported into statutory text only when Congress employs a common-law term"—not when Congress has outlined an offense "analogous to a common-law crime without using common-law terms." *Carter* v. *United States*, 530 U. S. 255, 265 (2000) (emphasis deleted). Relying on the common law is particularly ill advised here because it was the failure of preexisting law to capture computer crime that helped spur Congress to enact the CFAA. See *supra,* at 2.

work to do, the Government contends, the rule against superfluity means that its interpretation wins. See *Republic of Sudan* v. *Harrison*, 587 U. S. ___, ___ (2019) (slip op., at 10).

But the canon does not help the Government because Van Buren's reading does not render "so" superfluous. As Van Buren points out, without "so," the statute would allow individuals to use their right to obtain information in nondigital form as a defense to CFAA liability. Consider, for example, a person who downloads restricted personnel files he is not entitled to obtain by using his computer. Such a person could argue that he was "entitled to obtain" the information if he had the right to access personnel files through another method (*e.g.,* by requesting hard copies of the files from human resources). With "so," the CFAA forecloses that theory of defense. The statute is concerned with what a person does on a computer; it does not excuse hacking into an electronic personnel file if the hacker could have walked down the hall to pick up a physical copy.

This clarification is significant because it underscores that one kind of entitlement to information counts: the right to access the information by using a computer. That can expand liability, as the above example shows. But it narrows liability too. Without the word "so," the statute could be read to incorporate all kinds of limitations on one's entitlement to information. The dissent's take on the statute illustrates why.

3

While the dissent accepts Van Buren's definition of "so," it would arrive at the Government's result by way of the word "entitled." One is "entitled" to do something, the dissent contends, only when "'proper grounds'" are in place. *Post*, at 3 (opinion of THOMAS, J.) (quoting Black's Law Dictionary, at 477). Deciding whether a person was "entitled"

to obtain information, the dissent continues, therefore demands a "circumstance dependent" analysis of whether access was proper. *Post*, at 3. This reading, like the Government's, would extend the statute's reach to any circumstance-based limit appearing anywhere.

The dissent's approach to the word "entitled" fares fine in the abstract but poorly in context. The statute does not refer to "information . . . that the accesser is not entitled to obtain." It refers to "information . . . that the accesser is not entitled *so to obtain*." 18 U. S. C. §1030(e)(6) (emphasis added). The word "entitled," then, does not stand alone, inviting the reader to consider the full scope of the accesser's entitlement to information. The modifying phrase "so to obtain" directs the reader to consider a specific limitation on the accesser's entitlement: his entitlement to obtain the information "in the manner previously stated." *Supra,* at 7. And as already explained, the manner previously stated is using a computer one is authorized to access. Thus, while giving lipservice to Van Buren's reading of "so," the dissent, like the Government, declines to give "so" any limiting function.[5]

The dissent cannot have it both ways. The consequence of accepting Van Buren's reading of "so" is the narrowed scope of "entitled." In fact, the dissent's examples implicitly concede as much: They all omit the word "so," thereby giving "entitled" its full sweep. See *post*, at 3–4. An approach that must rewrite the statute to work is even less persuasive than the Government's.

---

[5] For the same reason, the dissent is incorrect when it contends that our interpretation reads the additional words "under any possible circumstance" into the statute. *Post*, at 3 (emphasis deleted). Our reading instead interprets the phrase "so to obtain" to incorporate the single "circumstance" of permissible information access identified by the statute: obtaining the information by using one's computer.

The Government falls back on what it describes as the "common parlance" meaning of the phrase "exceeds authorized access." Brief for United States 20–21. According to the Government, any ordinary speaker of the English language would think that Van Buren "exceed[ed] his authorized access" to the law enforcement database when he obtained license-plate information for personal purposes. *Id.,* at 21. The dissent, for its part, asserts that this point "settles" the case. *Post*, at 9.

If the phrase "exceeds authorized access" were all we had to go on, the Government and the dissent might have a point. But both breeze by the CFAA's explicit definition of the phrase "exceeds authorized access." When "a statute includes an explicit definition" of a term, "we must follow that definition, even if it varies from a term's ordinary meaning." *Tanzin* v. *Tanvir*, 592 U. S. ___, ___ (2020) (slip op., at 3) (internal quotation marks omitted). So the relevant question is not whether Van Buren exceeded his authorized access but whether he exceeded his authorized access *as the CFAA defines that phrase*. And as we have already explained, the statutory definition favors Van Buren's reading.

That reading, moreover, is perfectly consistent with the way that an "appropriately informed" speaker of the language would understand the meaning of "exceeds authorized access." Nelson, What Is Textualism? 91 Va. L. Rev. 347, 354 (2005). When interpreting statutes, courts take note of terms that carry "technical meaning[s]." A. Scalia & B. Garner, Reading Law: The Interpretation of Legal Texts 73 (2012). "Access" is one such term, long carrying a "well established" meaning in the "computational sense"—a meaning that matters when interpreting a statute about computers. American Heritage Dictionary 10 (3d ed. 1992). In the computing context, "access" references the act of entering a computer "system itself" or a particular "part of a

computer system," such as files, folders, or databases.[6] It is thus consistent with that meaning to equate "exceed[ing] authorized access" with the act of entering a part of the system to which a computer user lacks access privileges.[7] The Government and the dissent's broader interpretation is neither the only possible nor even necessarily the most natural one.

B

While the statute's language "spells trouble" for the Government's position, a "wider look at the statute's structure gives us even more reason for pause." *Romag Fasteners, Inc.* v. *Fossil Group, Inc.*, 590 U. S. ___, ___–___ (2020) (slip op., at 2–3).

The interplay between the "without authorization" and "exceeds authorized access" clauses of subsection (a)(2) is particularly probative. Those clauses specify two distinct

---

[6] 1 Oxford English Dictionary 72 (2d ed. 1989) ("[t]o gain access to . . . data, etc., held in a computer or computer-based system, or the system itself"); Random House Dictionary of the English Language 11 (2d ed. 1987) ("*Computers*. to locate (data) for transfer from one part of a computer system to another . . . "); see also C. Sippl & R. Sippl, Computer Dictionary and Handbook 2 (3d ed. 1980) ("[c]oncerns the process of obtaining data from or placing data in storage"); Barnhart Dictionary of New English 2 (3d ed. 1990) ("to retrieve (data) from a computer storage unit or device . . . "); Microsoft Computer Dictionary 12 (4th ed. 1999) ("[t]o gain entry to memory in order to read or write data"); A Dictionary of Computing 5 (6th ed. 2008) ("[t]o gain entry to data, a computer system, etc.").

[7] The dissent makes the odd charge that our interpretation violates the "'presumption against'" reading a provision "contrary to the ordinary meaning of the term it defines." *Post*, at 9. But when a statute, like this one, is "addressing a . . . technical subject, a specialized meaning is to be expected." Scalia, Reading Law, at 73. Consistent with that principle, our interpretation tracks the specialized meaning of "access" in the computer context. This reading is far from "'repugnant to'" the meaning of the phrase "exceeds authorized access," *post*, at 9—unlike, say, a definitional provision directing that "'the word *dog* is deemed to include all horses.'" Scalia, *supra*, at 232, n. 29.

ways of obtaining information unlawfully. *First*, an individual violates the provision when he "accesses a computer without authorization." §1030(a)(2). *Second*, an individual violates the provision when he "exceeds authorized access" by accessing a computer "with authorization" and then obtaining information he is "not entitled so to obtain." §§1030(a)(2), (e)(6). Van Buren's reading places the provision's parts "into an harmonious whole." *Roberts* v. *Sea-Land Services, Inc.*, 566 U. S. 93, 100 (2012) (internal quotation marks omitted). The Government's does not.

Start with Van Buren's view. The "without authorization" clause, Van Buren contends, protects computers themselves by targeting so-called outside hackers—those who "acces[s] a computer without any permission at all." *LVRC Holdings LLC* v. *Brekka*, 581 F. 3d 1127, 1133 (CA9 2009); see also *Pulte Homes, Inc.* v. *Laborers' Int'l Union of North Am.*, 648 F. 3d 295, 304 (CA6 2011). Van Buren reads the "exceeds authorized access" clause to provide complementary protection for certain information within computers. It does so, Van Buren asserts, by targeting so-called inside hackers—those who access a computer with permission, but then "'exceed' the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend." *United States* v. *Valle*, 807 F. 3d 508, 524 (CA2 2015).

Van Buren's account of subsection (a)(2) makes sense of the statutory structure because it treats the "without authorization" and "exceeds authorized access" clauses consistently. Under Van Buren's reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.[8] And

[8] For present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies. Cf. Brief for Orin Kerr as *Amicus Curiae* 7 (urging adoption of code-based approach).

reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry. See *supra*, at 11–12.[9]

By contrast, the Government's reading of the "exceeds authorized access" clause creates "inconsistenc[ies] with the design and structure" of subsection (a)(2). *University of Tex. Southwestern Medical Center* v. *Nassar*, 570 U. S. 338, 353 (2013). As discussed, the Government reads the "exceeds authorized access" clause to incorporate purpose-based limits contained in contracts and workplace policies. Yet the Government does not read such limits into the threshold question whether someone uses a computer "without authorization"—even though similar purpose restrictions, like a rule against personal use, often govern one's right to access a computer in the first place. See, *e.g.*, *Royal Truck & Trailer Sales & Serv., Inc.* v. *Kraft*, 974 F. 3d 756, 757 (CA6 2020). Thus, the Government proposes to read the first phrase "without authorization" as a gates-up-or-down inquiry and the second phrase "exceeds authorized access" as one that depends on the circumstances. The Government does not explain why the statute would prohibit

---

[9] Van Buren's gates-up-or-down reading also aligns with the CFAA's prohibition on password trafficking. See Tr. of Oral Arg. 33. Enacted alongside the "exceeds authorized access" definition in 1986, the password-trafficking provision bars the sale of "any password or similar information through which a computer may be accessed without authorization." §1030(a)(6). The provision thus contemplates a "specific type of authorization—that is, authentication," which turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than on other, scope-based restrictions. Bellia, A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act, 84 Geo. Wash. L. Rev. 1442, 1470 (2016); cf. A Dictionary of Computing, at 30 (defining "authorization" as a "process by which users, having completed an . . . authentication stage, gain or are denied access to particular resources based on their entitlement").

accessing computer information, but not the computer itself, for an improper purpose.[10]

The Government's position has another structural problem. Recall that violating §1030(a)(2), the provision under which Van Buren was charged, also gives rise to civil liability. See §1030(g). Provisions defining "damage" and "loss" specify what a plaintiff in a civil suit can recover. "'[D]amage,'" the statute provides, means "any impairment to the integrity or availability of data, a program, a system, or information." §1030(e)(8). The term "loss" likewise relates to costs caused by harm to computer data, programs, systems, or information services. §1030(e)(11). The statutory definitions of "damage" and "loss" thus focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data. Limiting "damage" and "loss" in this way makes sense in a scheme "aimed at preventing the typical consequences of hacking." *Royal Truck*, 974 F. 3d, at 760. The term's definitions are ill fitted, however, to remediating "misuse" of sensitive information that employees may permissibly access using their computers. *Ibid.* Van Buren's situation is illustrative: His run of the license plate did not

---

[10] Unlike the Government, the dissent would read both clauses of subsection (a)(2) to require a circumstance-specific analysis. Doing so, the dissent contends, would reflect that "[p]roperty law generally protects against both unlawful entry *and* unlawful use." *Post*, at 7. This interpretation suffers from structural problems of its own. Consider the standard rule prohibiting the use of one's work computer for personal purposes. Under the dissent's approach, an employee's computer access would be *without* authorization if he logged on to the computer with the purpose of obtaining a file for personal reasons. In that event, obtaining the file would not violate the "exceeds authorized access" clause, which applies only when one accesses a computer "*with* authorization." §1030(e)(6) (emphasis added). The dissent's reading would therefore leave the "exceeds authorized access" clause with no work to do much of the time—an outcome that Van Buren's interpretation (and, for that matter, the Government's) avoids.

impair the "integrity or availability" of data, nor did it otherwise harm the database system itself.

C

Pivoting from text and structure, the Government claims that precedent and statutory history support its interpretation. These arguments are easily dispatched.

As for precedent, the Government asserts that this Court's decision in *Musacchio* v. *United States*, 577 U. S. 237 (2016), bolsters its reading. There, in addressing a question about the standard of review for instructional error, the Court described §1030(a)(2) as prohibiting "(1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Id.*, at 240. This paraphrase of the statute does not do much for the Government. As an initial matter, *Musacchio* did not address—much less resolve in the Government's favor—the "point now at issue," and we thus "are not bound to follow" any dicta in the case. *Central Va. Community College* v. *Katz*, 546 U. S. 356, 363 (2006). But in any event, Van Buren's interpretation, no less than the Government's, involves "using [one's] access improperly." It is plainly "improper" for one to use the opportunity his computer access provides to obtain prohibited information from within the computer.

As for statutory history, the Government claims that the original 1984 Act supports its interpretation of the current version. In a precursor to the "exceeds authorized access" clause, the 1984 Act covered any person who, "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend," and thus expressly alluded to the purpose of an insider's computer access. 18 U. S. C. §1030(a)(2) (1982 ed. Supp. III). According to the Government, this confirms that the amended CFAA—which makes no mention

of purpose in defining "exceeds authorized access"—likewise covers insiders like Van Buren who use their computer access for an unauthorized purpose.[11] The Government's argument gets things precisely backward. "When Congress amends legislation, courts must presume it intends the change to have real and substantial effect." *Ross* v. *Blake*, 578 U. S. 632, 641–642 (2016) (internal quotation marks and brackets omitted). Congress' choice to *remove* the statute's reference to purpose thus cuts *against* reading the statute "to capture that very concept." Brief for United States 22. The statutory history thus hurts rather than helps the Government's position.

III

To top it all off, the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity. Van Buren frames the far-reaching consequences of the Government's reading as triggering the rule of lenity or constitutional avoidance. That is not how we see it: Because the text, context, and structure support Van Buren's reading, neither of these canons is in play. Still, the fallout underscores the implausibility of the Government's interpretation. It is "extra icing on a cake already frosted." *Yates* v. *United States*, 574 U. S. 528, 557 (2015) (KAGAN, J., dissenting).

If the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of

---

[11] While the Government insists that Congress made this change "'merely to clarify the language'" of §1030(a)(2), Brief for United States 28, the dissent has a different take. In the dissent's telling, the 1986 amendment in fact "expand[ed]" the provision to reach "time and manner" restrictions on computer access—not just purpose-based ones. *Post*, at 10–11. The dissent's distinct explanation for why Congress removed §1030(a)(2)'s reference to "purpose" requires accepting that the "exceeds authorized access" definition supports a circumstance-specific approach. We reject the dissent's premise for the textual and structural reasons already discussed.

otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA. Or consider the Internet. Many websites, services, and databases—which provide "information" from "protected computer[s]," §1030(a)(2)(C)—authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers. And indeed, numerous *amici* explain why the Government's reading of subsection (a)(2) would do just that—criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook. See Brief for Orin Kerr as *Amicus Curiae* 10–11; Brief for Technology Companies as *Amici Curiae* 6, n. 3, 11; see also Brief for Reporters Committee for Freedom of the Press et al. as *Amici Curiae* 10–13 (journalism activity); Brief for Kyratso Karahalios et al. as *Amici Curiae* 11–17 (online civil-rights testing and research).

In response to these points, the Government posits that other terms in the statute—specifically "authorization" and "use"—"may well" serve to cabin its prosecutorial power. Brief for United States 35; see Tr. of Oral Arg. 38, 40, 58 ("instrumental" use; "individualized" and "fairly specific" authorization). Yet the Government stops far short of endorsing such limitations. Cf. Brief for United States 37 (concept of "authorization" "may not logically apply"); *id.,* at 38 ("'use'" might be read in a more "limited" fashion, even though it "often has a broader definition"); see also, *e.g., post*, at 11–12 (*mens rea* requirement "might" preclude liability in some cases). Nor does it cite any prior instance in

which it has read the statute to contain such limitations—to the contrary, Van Buren cites instances where it hasn't. See Reply Brief 14–15, 17 (collecting cases); cf. *Sandvig* v. *Barr*, 451 F. Supp. 3d 73, 81–82 (DC 2020) (discussing Department of Justice testimony indicating that the Government could "'bring a CFAA prosecution based'" on terms-of-service violations causing "'de minimis harm'"). If anything, the Government's current CFAA charging policy shows why Van Buren's concerns are far from "hypothetical," *post*, at 12: The policy instructs that federal prosecution "*may not* be warranted"—not that it would be prohibited—"if the defendant exceed[s] authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website."[12] And while the Government insists that the intent requirement serves as yet another safety valve, that requirement would do nothing for those who intentionally use their computers in a way their "job or policy prohibits"—for example, by checking sports scores or paying bills at work. App. 39.

One final observation: The Government's approach would inject arbitrariness into the assessment of criminal liability. The Government concedes, as it must, that the "exceeds authorized access" clause prohibits only unlawful information "access," not downstream information "'misus[e].'" Brief in Opposition 17 (statute does not cover "'subsequen[t] misus[e of] information'"). But the line between the

---

[12] Memorandum from U. S. Atty. Gen. to U. S. Attys. & Assistant Attys. Gen. for the Crim. & Nat. Security Divs., Intake and Charging Policy for Computer Crime Matters 5 (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download (emphasis added). Although the Government asserts that it has "[h]istorically" prosecuted only "core conduct" like Van Buren's and not the commonplace violations that Van Buren fears, Brief for United States 40, the contrary examples Van Buren and his *amici* cite give reason to balk at that assurance. See Brief for Petitioner 32–33; Brief for Orin Kerr as *Amicus Curiae* 18–23; Brief for Technology Companies as *Amici Curiae* 11.

two can be thin on the Government's reading. Because purpose-based limits on access are often designed with an eye toward information misuse, they can be expressed as either access or use restrictions. For example, one police department might prohibit *using a confidential database* for a non-law-enforcement purpose (an access restriction), while another might prohibit *using information from the database* for a non-law-enforcement purpose (a use restriction). Conduct like Van Buren's can be characterized either way, and an employer might not see much difference between the two. On the Government's reading, however, the conduct would violate the CFAA only if the employer phrased the policy as an access restriction. An interpretation that stakes so much on a fine distinction controlled by the drafting practices of private parties is hard to sell as the most plausible.

IV

In sum, an individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him. The parties agree that Van Buren accessed the law enforcement database system with authorization. The only question is whether Van Buren could use the system to retrieve license-plate information. Both sides agree that he could. Van Buren accordingly did not "excee[d] authorized access" to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose. We therefore reverse the contrary judgment of the Eleventh Circuit and remand the case for further proceedings consistent with this opinion.

It is so ordered.

SUPREME COURT OF THE UNITED STATES

No. 19–783

NATHAN VAN BUREN, PETITIONER *v.*
UNITED STATES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

[June 3, 2021]

JUSTICE THOMAS, with whom THE CHIEF JUSTICE and JUSTICE ALITO join, dissenting.

Both the common law and statutory law have long punished those who exceed the scope of consent when using property that belongs to others. A valet, for example, may take possession of a person's car to park it, but he cannot take it for a joyride. The Computer Fraud and Abuse Act extends that principle to computers and information. The Act prohibits exceeding the scope of consent when using a computer that belongs to another person. Specifically, it punishes anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains" information from that computer. 18 U. S. C. §1030(a)(2).

As a police officer, Nathan Van Buren had permission to retrieve license-plate information from a government database, but only for law enforcement purposes. Van Buren disregarded this limitation when, in exchange for several thousand dollars, he used the database in an attempt to unmask a potential undercover officer.

The question here is straightforward: Would an ordinary reader of the English language understand Van Buren to have "exceed[ed] authorized access" to the database when he used it under circumstances that were expressly forbid-

den? In my view, the answer is yes. The necessary precondition that permitted him to obtain that data was absent.

The Court does not dispute that the phrase "exceeds authorized access" readily encompasses Van Buren's conduct. It notes, instead, that the statute includes a definition for that phrase and that "we must follow that definition, even if it varies from a term's ordinary meaning." *Tanzin* v. *Tanvir*, 592 U. S. ___, ___ (2020) (slip op., at 3) (internal quotation marks omitted). The problem for the majority view, however, is that the text, ordinary principles of property law, and statutory history establish that the definitional provision is quite consistent with the term it defines.

I

A

The Act defines "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." §1030(e)(6). For purposes of this appeal, it is agreed that Van Buren was authorized to log into a government database and that he used his entry to obtain fake license-plate information from that database. I thus agree with the majority that this case turns on whether Van Buren was "entitled so to obtain" the fake license-plate information. I also agree that "so" asks whether Van Buren had a right to obtain that information through the means identified earlier in the definition: (1) accessing a computer with authorization and (2) using that access to obtain information in the computer. In other words, Van Buren's conduct was legal only if he was entitled to obtain that specific license-plate information by using his admittedly authorized access to the database.

He was not. A person is entitled to do something only if he has a "right" to do it. Black's Law Dictionary 477 (5th ed. 1979); see also American Heritage Dictionary 437 (def. 3a) (1981) (to "allow" or to "qualify"). Van Buren never had

a "right" to use the computer to obtain the specific license-plate information. Everyone agrees that he obtained it for personal gain, not for a valid law enforcement purpose. And without a valid law enforcement purpose, he was *forbidden* to use the computer to obtain that information.

B

The majority postulates an alternative reading of this definitional provision: So long as a person is entitled to use a computer to obtain information in at least *one* circumstance, this statute does not apply even if the person obtains the data outside that circumstance. In effect, the majority reads the statute to apply only when a person is "not entitled [*under any possible circumstance*] so to obtain" information. This interpretation is flawed for a number of reasons.

1

Foremost, that interpretation is contrary to the plain meaning of the text. Entitlements are necessarily circumstance dependent; a person is entitled to do something only when "proper grounds" or facts are in place. Black's Law Dictionary, at 477. Focusing on the word "so," the majority largely avoids analyzing the term "entitled," concluding at the outset in a single sentence that Van Buren *was* entitled to obtain this license-plate information. *Ante*, at 5. But the plain meaning of "entitled" compels the opposite conclusion. Because Van Buren lacked a law enforcement purpose, the "proper grounds" did not exist. He was not entitled to obtain the data when he did so.

A few real-world scenarios illustrate the point. An employee who is entitled to pull the alarm in the event of a fire is not entitled to pull it for some other purpose, such as to delay a meeting for which he is unprepared. A valet who obtains a car from a restaurant patron is—to borrow the language from §1030(e)(6)—"entitled" to "access [the car]"

and "entitled" to "use such access" to park and retrieve it. But he is not "entitled" to "use such access" to joyride. See, *e.g.*, Ind. Code §35–43–4–3 (2020) (felonious criminal conversion to "knowingly or intentionally exer[t] unauthorized control over property of another" if "the property is a motor vehicle"); *In re Clayton*, 778 N. E. 2d 404, 405 (Ind. 2002) (interpreting this statute to cover misuse of property a person otherwise is entitled to access). And, to take an example closer to this statute, an employee of a car rental company may be "entitled" to "access a computer" showing the GPS location history of a rental car and "use such access" to locate the car if it is reported stolen. But it would be unnatural to say he is "entitled" to "use such access" to stalk his ex-girlfriend.

The majority offers no real response. It notes that "entitled" is modified by "so" and that courts must therefore consider whether a person is entitled to use a computer to obtain information. *Ante*, at 10. But if a person is not entitled to obtain information *at all*, it necessarily follows that he has no "right to access the information by using a computer." *Ante,* at 9. Van Buren was not entitled to obtain this information at all because the condition precedent needed to trigger an entitlement—a law enforcement purpose—was absent.

2

Next, the majority's reading is at odds with basic principles of property law. By now, it is well established that information contained in a computer is "property." Nobody doubts, for example, that a movie stored on a computer is intellectual property. Federal and state law routinely define "property" to include computer data. *E.g.,* 12 U. S. C. §5433; N. Y. Penal Law Ann. §155.00 (West 2010). And even the majority acknowledges that this statute is designed to protect property. *Ante*, at 2. Yet it fails to square its interpretation with the familiar rule that an entitlement

to use another person's property is circumstance specific.

Consider trespass. When a person is authorized to enter land and entitled to use that entry for one purpose but does so for another, he trespasses. As the Second Restatement of Torts explains, "[a] conditional or restricted consent to enter land creates a privilege to do so only in so far as the condition or restriction is complied with." §168, p. 311 (1964). The Restatement includes a helpful illustration:

> "3. A grants permission to B, his neighbor, to enter A's land, and draw water from A's spring for B's own use. A has specifically refused permission to C to enter A's land and draw water from the spring. At C's instigation, B enters A's land and obtains for C water from the spring. B's entry is a trespass." *Ibid.*, Comment *b*.

What 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.

Consider, too, the common understanding of theft. A person who is authorized to possess property for a limited purpose commits theft the moment he "exercises unlawful control over" it, which occurs "whenever consent or authority is exceeded." ALI, Model Penal Code §223.2(1), pp. 162, 168 (1980). To again borrow the language from §1030(e)(6), a police officer may have authority to "access" the department's bank account and "use such access" to cover law enforcement expenses, but he is nonetheless guilty of embezzlement if he "uses such access" to line his pockets. He would not be exonerated simply because he would be "entitled so to obtain" funds from the account under other circumstances.

Or take bailment. A bailee commits conversion—which many jurisdictions criminalize—when he, "having no authority to use the thing bailed, nonetheless uses it, or, hav-

ing authority to use it in a particular way, uses it in a different way." 8 C. J. S., Bailments §43, pp. 480–481 (2017) (footnote omitted). A computer technician may have authority to access a celebrity's computer to recover data from a crashed hard drive, but not to use his access to copy and leak to the press photos stored on that computer.

The majority makes no attempt to square its interpretation with this familiar principle. Instead, it sweeps away this context by stating that Congress did not include in this statute any common-law terms. *Ante*, at 8, n. 4. But the statute *does* use words like "exceed" and "authority" that are common to other property contexts. And the majority never identifies any particular property-law buzzwords that it thinks Congress was obliged to include.

The majority next says that relying on pre-existing concepts of property law is "ill advised" because Congress enacted this law in light of a "failure of pre-existing law to capture computer crime." *Ante,* at 2, 8, n. 4 (citing Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N. Y. U. L. Rev. 1596 (2003)). Yet the reasons why pre-existing law was considered inadequate undermine the majority's position. First, state laws *were* used to cover conduct like Van Buren's, but doing so "require[d] considerable creativity" because those laws typically required either "physical" entry (which fit poorly with computers) or "depriv[ing]" a victim of property (which fit poorly where a person "merely copied" data or engaged in forbidden "personal uses"). *Id.,* at 1607–1608, 1610–1611. Second, the fit was even more awkward for federal laws, which were "more limited in scope." *Id.,* at 1608. Congress did not enact this law to eliminate the established principle that entitlements to use property are circumstance specific, but instead to eliminate the deprivation and physical-entry requirements.

Unable to square its interpretation with established prin-

ciples of property law, the majority contends that its interpretation is more harmonious with a separate clause in the statute that forbids "access[ing] a computer without authorization." §1030(a)(2). In the majority's telling, this clause requires "a gates-up-or-down inquiry—one either can or cannot access a computer system," so it makes sense to read the "exceeds authorized access" clause in the same sentence to include the same approach. *Ante*, at 13–14.

I agree that the two clauses should be read harmoniously, but there is no reason to believe that if the gates are up in a single instance, then they must remain up indefinitely. An employee who works with sensitive defense information may generally have authority to log into his employer-issued laptop while away from the office. But if his employer instructs him not to log in while on a trip to a country where network connections cannot be trusted, he accesses the computer without authorization if he logs in anyway. For both clauses, discerning whether the gates are up or down requires considering the circumstances that cause the gates to move.

In fact, my reading harmonizes *both* clauses with established concepts of property law. Property law generally protects against both unlawful entry *and* unlawful use after entry. *E.g.,* Restatement (Second) of Torts §214, Comment *e*, at 408–409; 8 C. J. S., Bailments §43, at 480–481. The same is true here. The police department could protect information by prohibiting officers from logging in with an improper purpose, but that would do little good if an officer logged in at the start of his shift with proper intent and then, hours later while still logged in, conducted license-plate searches in exchange for payment. By including both the "without authorization" and "exceeds authorized access" clauses, Congress ensured protection against improper login as well as misuse *after* proper login.

The majority's interpretation—that criminality turns on whether there is a *single* exception to a prohibition—also leads to awkward results. Under its reading, an employee at a credit-card company who is forbidden to obtain the purchasing history of clients violates the Act when he obtains that data about his ex-wife—unless his employer tells him he can obtain and transfer purchase history data when an account has been flagged for possible fraudulent activity. The same is true of the person who, minutes before resigning, deletes every file on a computer. See *Royal Truck & Trailer Sales & Serv., Inc.* v. *Kraft*, 974 F. 3d 756, 758 (CA6 2020). So long as an employee could obtain or alter each file in some hypothetical circumstance, he is immune. But the person who plays a round of solitaire is a criminal under the majority's reading if his employer, concerned about distractions, categorically prohibits accessing the "games" folder in Windows. It is an odd interpretation to "stak[e] so much" on the presence or absence of a single exception. *Ante*, at 20.

The majority's interpretation is especially odd when applied to other clauses in the statute. Section 1030(a)(1) prohibits "exceeding authorized access" to obtain "restricted data . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation," and retaining or distributing that data. The term "restricted data" is defined to include "all data concerning (1) design, manufacture, or utilization of atomic weapons." 42 U. S. C. §2014(y). Under the majority's reading, so long as a scientist may obtain blueprints for atomic weapons in at least *one* circumstance, he would be immune if he obtained that data for the improper purpose of helping an unfriendly nation build a nuclear arsenal. It is difficult to see what force this provision—in place in substantially similar form since 1984—has under the majority's reading.

Were there any remaining doubt about which interpretation better fits the statute, the defined term settles it. When a definition is susceptible of more than one reading, the one that best matches the plain meaning of the defined term ordinarily controls. See, *e.g., Bond* v. *United States*, 572 U. S. 844, 861 (2014) (considering the "ordinary meaning of a defined term"); *id.*, at 870 (Scalia, J., concurring in judgment) (courts may "us[e] the ordinary meaning of the term being defined for the purpose of resolving an ambiguity in the definition" (emphasis deleted)). That is because "there is a presumption against" reading a provision contrary to the ordinary meaning of the term it defines. A. Scalia & B. Garner, Reading Law: The Interpretation of Legal Texts 232 (2012); see also *id.,* at 228 ("[T]he meaning of the definition is almost always closely related to the ordinary meaning of the word being defined").

The majority instead resolves supposed ambiguity in the definition *against* the plain meaning of the defined term. It adopts a "favor[ed]" interpretation of the definition and then asks whether the defined term can be interpreted in a way "consistent" with this "favor[ed]" view. *Ante*, at 11. But "[i]t should take the strongest evidence to make us believe that Congress has defined a term in a manner repugnant to its ordinary and traditional sense." *Babbitt* v. *Sweet Home Chapter, Communities for Great Ore.*, 515 U. S. 687, 719 (1995) (Scalia, J., dissenting). The majority identifies no such evidence. The most it says is that my reading of "exceeds authorized access" is not "necessarily" best because "access" can have a technical meaning: entering the computer system or a part of the computer system. *Ante*, at 11, 12, n. 6. But whatever meaning "access" might have, "authority"—like "entitled"—is circumstance dependent. The majority's reading of "access" confirms that point. The definitions the majority cites reference not mere entry, but *using* entry to obtain specific data. *Ante,* at 12, n. 6. That

accords with the definition here, which regulates a person's "use" of a computer after entering it. §1030(e)(6). Here, as in other contexts of property law, a person's authority to use his access to property is circumstance dependent. The majority's focus on the term "access"—at the expense of "authority" and "entitled"—harms, not helps, its argument.

II

What the text and established concepts of property law make clear, statutory history reinforces. The original text of this Act expressly prohibited accessing a computer with authorization and then "us[ing] the opportunity such access provides for purposes to which such authorization does not extend." 98 Stat. 2191. The Act thus applied when persons used computers for improper reasons—just like Van Buren indisputably did here.

The majority does not deny this. Instead, it notes that Congress amended the text in 1986 to its present definition, and it says that the Court can presume that Congress' decision to omit the term "purpose" necessarily eliminated any prohibition against obtaining information for an improper purpose. *Ante*, at 17.

But the majority cannot so easily evade this history. True, the statute previously included the term "purpose" and now does not, but the majority fails to consider *how* that change affected the statute. Often, deleting a word expands, rather than constricts, the scope of a provision. If a city changes a sign in a park from "no unleashed dogs" to "no dogs," nobody would presume that unleashed dogs are now allowed. The same is true when the specific is replaced by the general ("no dogs" to "no pets").

Congress' change to this statute similarly broadened the law. The original text prohibited accessing a computer with authorization then "us[ing] the opportunity such access provides for purposes to which such authorization does not extend." The term "purpose" limited that clause to purpose-

based constraints. It did not naturally include other constraints, such as time and manner restrictions. By replacing the specific, limited term "purposes" with the broader, more general phrase "not entitled," Congress gave force to those other kinds of constraints. Consider the previous example of the employee who violates an instruction not to log in while in an unfriendly foreign country with insecure networks. The original text would not cover him, so long as he logged in for a proper purpose like checking work e-mail. The newer text would cover him because his entitlement to obtain or alter data is context dependent. His purpose is innocent, but the time or manner of his use is not.

III

The majority ends with policy arguments. It suggests they are not needed. *Ante*, at 17 ("'extra icing on a cake already frosted'"). Yet, it stresses them at length. *Ante*, at 17–20. Regardless, the majority's reliance on these policy arguments is in error.

Concerned about criminalizing a "breathtaking amount of commonplace computer activity," the majority says that the way people use computers today "underscores the implausibility of the Government's interpretation." *Ante*, at 17. But statutes are read according to their "'ordinary meaning at the time Congress enacted the statute.'" *Wisconsin Central Ltd.* v. *United States*, 585 U. S. ___, ___ (2018) (slip op., at 2) (ellipsis omitted). The majority's reliance on modern-day uses of computers to determine what was plausible in the 1980s wrongly assumes that Congress in 1984 was aware of how computers would be used in 2021.

I also would not so readily assume that my interpretation would automatically cover so much conduct. Many provisions plausibly narrow the statute's reach. For example, the statute includes the strict *mens rea* requirement that a person must "intentionally . . . excee[d] authorized access." §1030(a)(2). The statute thus might not apply if a person

believes he is allowed to use the computer a certain way because, for example, that kind of behavior is common and tolerated. Cf. Restatement (Second) of Contracts §223(2) (1979) (discussing how an established "course of dealing" can erase written limitations in certain contractual contexts). The Act also concerns only "obtain[ing] or alter[ing] information *in* the computer," §1030(e)(6) (emphasis added), not using the Internet to check sports scores stored in some distant server (*i.e.,* a different computer). The majority does not deny that many provisions plausibly narrow the focus of this statute. It simply faults the government for not arguing the point more forcefully. *Ante,* at 18–19. I would not give so much weight to the hypothetical concern that the Government *might* start charging innocuous conduct and that courts *might* interpret the statute to cover that conduct.

The majority's argument also proves too much. Much of the Federal Code criminalizes common activity. Absent aggravating factors, the penalty for violating this Act is a misdemeanor. §1030(c)(2)(A). This Act thus penalizes mine-run offenders about as harshly as federal law punishes a person who removes a single grain of sand from the National Mall, 40 U. S. C. §8103(b); breaks a lamp in a Government building, *ibid.*; or permits a horse to eat grass on federal land, 18 U. S. C. §1857. The number of federal laws and regulations that trigger criminal penalties may be as high as several hundred thousand. Fields & Emshwiller, Many Failed Efforts To Count Nation's Federal Criminal Laws, Wall-Street Journal (July 23, 2011).* It is understandable to be uncomfortable with so much conduct being criminalized, but that discomfort does not give us authority to alter statutes.

---

* www.wsj.com/article/SB10001424052702304319804576389601079728920.html.

* * *

In the end, the Act may or may not cover a wide array of conduct because of changes in technology that have occurred since 1984. But the text makes one thing clear: Using a police database to obtain information in circumstances where that use is expressly forbidden is a crime. I respectfully dissent.