2017 WL 2391509 (U.S.) (Appellate Petition, Motion and Filing)
Supreme Court of the United States.

POWER VENTURES, INC. and Steven Vachani, Petitioners,
v.
FACEBOOK, INC., Respondent.

No. 16-1105.
May 25, 2017.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

Brief of the Cato Institute as Amicus Curiae Supporting the Petition for Certiorari

Ilya Shapiro, Devin Watkins, Cato Institute, 1000 Mass. Ave., N.W., Washington, D.C. 20001, (202) 842-0200, ishapiro@cato.org, dwatkins@cato.org.

*i QUESTION PRESENTED

Whether, under the Computer Fraud and Abuse Act, a user who owns the online content on a website can authorize a third party to access that content?

*ii TABLE OF CONTENTS

*iii TABLE OF AUTHORITIES

Cases

*1 INTEREST OF *AMICUS CURIAE*[1]

The Cato Institute is a non-partisan public policy research foundation that was established in 1977 to advance the principles of individual liberty, free markets, and limited government. Cato's Center for Constitutional Studies helps restore the principles of constitutional government that are the foundation of liberty. Toward those ends, Cato holds conferences and publishes books, studies, and the annual *Cato Supreme Court Review.* Cato's interest in this case stems from its substantial impact on the development of the online economy and property law.

SUMMARY OF ARGUMENT

Nearly two billion people use Facebook to post personal information and pictures. These users own their data (not Facebook), as Facebook freely acknowledges. When some of these users decided to allow a third-party company access to this - *their* - data, however, Facebook said no. Not because the company was doing harm to the system or other users, but because it was competing with Facebook in the online marketplace.

Facebook argues that the company, Power Ventures, was acting "without authorization" under the Computer Fraud and Abuse Act ("CFAA") because Facebook told it to stop. But Power Ventures was authorized by the data's owners. Isn't that enough?

The text of the CFAA is ambiguous as to whose permission is needed for access to be "authorized." Like ***2** many statutes, the Act implicitly relies on background legal principles. But there is a substantial circuit split here on which set of background legal principles to use. Some circuits apply contract law, others use agency law, and still others the common law of trespass. The Court should take this case to resolve this split.

Legislative history, while not dispositive regarding statutory interpretation, can suggest the background legal principles to apply. Committee reports and statements by members of Congress at the time the CFAA was enacted analogized computer crimes to common-law trespass. This suggests that property law, not agency or contract law, should inform what type of authorization is required - and from whom, Facebook or users, Power Ventures had to seek it.

Because the data is owned by the user, this case could be analogized to a landlord-tenant dispute over access by a third party. Applying traditional common-law trespass principles in the Restatement (Second) of Torts, the Facebook user by default would have the power to invite "guests" like Power Ventures. (This default rule can then be changed by contract between Facebook and the user.)

Using the landlord-tenant analogy also reflects public norms in this area. Millions of users share their social-media passwords without considering such actions to be criminal. This widespread practice implies a common understanding about third-party access authorized by the user. Such conduct should not be criminalized without a clear statement by Congress.

The Court should also take this case because of its importance to the digital economy. Many of the automated methods used by Power Ventures are also used ***3** by data-processing companies like Google. By allowing firms to compete against Facebook, the marketplace can let the most successful ideas flourish. Legal clarity will also allow online business to expand without fear of incurring civil liability or committing a crime.

ARGUMENT

I. THE COURT SHOULD USE COMMON-LAW TRESPASS DOCTRINE TO RESOLVE A CIRCUIT SPLIT ON THE MEANING OF THE CFAA'S PROHIBITION ON ACCESSING A COMPUTER "WITHOUT AUTHORIZATION"

The Court is asked to consider if Power Ventures accessed Facebook's website "without Authorization" under the CFAA. There is no definition of those words in the statute. *United States v. John,* 597 F.3d 263, 271 (5th Cir. 2010) ("The statute does not define 'authorized,' or 'authorization.' "). Power Ventures needed permission to access the website, but whose permission? The answer cannot be found in statutory text, nor in a dictionary alone, but in the legal background principles on which this statute was based.

Circuit courts across the country have chosen different guiding principles. The Fifth and Seventh Circuits used agency law in finding that an employee breached his fiduciary duty to the computer system owner. *United States v. John,* 597 F.3d 263, 272 (5th Cir. 2010) (holding that an employee was not authorized to access outside of limited purposes); *Int'l Airport Ctrs., LLC v. Citrin,* 440 F.3d 418, 420-21 (7th Cir. 2006) (holding that a breach of an employee's duty of loyalty automatically revoked his authorization). The First and Eleventh Circuits considered contract law in finding that an employee violated the statute by ***4** breaching a confidentiality agreement or established policies. *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577, 583-84 (1st Cir. 2001) (violating a confidentiality agreement or a contractual duty of good faith and fair dealing in accessing a website violates the CFAA); *United States v. Rodriguez,* 628 F.3d 1258, 1263 (11th Cir. 2010) (violating established policies against using the computer for non-business reasons violated the CFAA). The Second, Fourth, and Ninth Circuits, meanwhile, apply something like the common law of trespass to the CFAA. *United States v. Valle,* 807 F.3d 508, 526 (2d Cir. 2015) (applying rule of lenity to reject purpose-based analysis in favor

of trespass analysis); *WEC Carolina Energy Solutions v. Miller,* 687 F.3d 199, 207 (4th Cir. 2012) (rejecting cessation-of-agency or violation-of-established-policy theory in favor of permission-based analysis); *United States v. Nosal,* 676 F.3d 854, 858 (9th Cir. 2012) (rejecting agency- or established-policy-based analysis in favor of focus on hackers' digital trespass).

The Court should clear up this confusion.

A. The CFAA Prohibition on Accessing a Computer "Without Authorization" Is Ambiguous, Although Legislators Analogized It to Common-Law Trespass

As the lower-court divergence shows, analogies to several areas of law could help courts define "authorization" in the CFAA. Legislative history suggests that common-law trespass doctrine comes closest to explaining this digital dilemma.

The CFAA was crafted at the beginning of the modern internet era to deal with so-called "hackers." Hackers had been electronically breaking into government ***5** computer systems to access information without authorization, which problem the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 was designed to address. The House Judiciary Committee analogized the hacker's breaking into computer systems to criminal trespass. H.R. Rep. No. 98-894, at 10 (1984) ("[T]he advent of the activities of so-called 'hackers' who have been able to access (*trespass* into) both private and public computer systems, sometimes with potentially serious results.") (emphasis added).

Several senators and congressmen also analogized computer intrusion to physical trespass. Sen. Jeremiah Denton linked the question of authorization with trespass: "The bill makes it clear that *unauthorized* access to a Government computer is a *trespass* offense, as surely as if the offender had entered a restricted Government compound without proper *authorization.*" 132 Cong. Rec. 27639 (1986) (emphasis added). House Judiciary Committee member Rep. William Hughes agreed: "All of our criminal statutes are couched in terms of tangible property in terms of trespass as an actual entry. So this new phenomenon of *computer trespass* is a whole new area of the law that we are going to be wrestling with in the years ahead as the technology evolves." 130 Cong. Rec. 20645 (1984) (emphasis added). Rep. Bill Nelson described the "computer crime" being targeted by the bill as merely "sophisticated bank robbery, trespass, and burglary." 130 Cong. Rec. 20644 (1984). Rep. Thomas Sawyer also described the problem that the bill was trying to fix:

> [W]e have a similar situation in computer fraud as we do in copyright. We are really carrying forward very ancient doctrines that in copyright were designed primarily for the ***6** printed book and printed material and we are trying to work out applications of them for satellite communications and all kinds of electronic transmissions. We are in the same problem with the computer taking over from entering physical records or trespassing.

130 Cong. Rec. 20645 (1984).

The 1984 Act prohibited only entry into government computers. It wasn't until the 1986 Act that the prohibition was expanded to include the unauthorized access of any computer "affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). The House Judiciary Committee again linked the crime to one of trespass:

> One somewhat unique aspect of computer crime is the expanding group of *electronic trespassers*-the so called "hackers" who have been frequently glamorized by the media, perhaps because this image of the hacker is that of a bright, intellectually curious, and rebellious youth-a modern day Huck Finn. The fact is, these young thrill seekers are *trespassers*, just as much as if they broke a window and crawled into a home while the occupants were away.

H.R. Rep. No. 99-612, 99th Cong. 2d Sess. 5-6 (1986) (emphasis added).

While it's possible that all these legislative mentions of trespass were just rhetorical flourishes, they provide at least some evidence that trespass-based concepts informed the Act's drafting.

*7 B. When Users Own Their Data, Allowing a Third Party to Access that Data is Analogous to a Common-Law Landlord-Tenant Dispute Over a Guest's Authorization

While the lower court applied trespass law here, it failed to properly consider a critical fact: the users' ownership of the data at issue. Each user owns what he uploads to Facebook and merely grants Facebook a license to distribute. *Statement of Rights and Responsibilities,* Facebook, http://bit.ly/2qIPNwB (last accessed May 22, 2017) ("You own all of the content and information you post on Facebook."). Nothing in the terms of use limits the user's ability to allow Power Ventures to access his property. *Id.* If the Court applies common-law trespass doctrines to the modern electronic environment, then the user's ownership creates something like a landlord-tenant dispute here.

Like a residential building where each apartment is rented by a different user and Facebook is the complex owner, the user maintains his or her digital property inside a broader online structure owned by Facebook. The "lease" is the Statement of Rights and Responsibilities that contractually binds the two parties and define the ownership relationship. The user must log in to access his property by passing through and using the common property owned by Facebook.

Facebook's network can be contrasted with the kind of system considered by the Ninth Circuit in *Nosal.* 676 F.3d 854. There, a former employee at an executive-search service convinced current employees to use their logins to "download source lists, names and contact information from a confidential database on the company's computer" and then transfer the data to him. *Id.* at 856. Access to such systems requires ***8** the company's permission because the data at issue was entirely owned by the company. With a database completely owned by a single entity, trying to access data with a user's credentials - even with that user's consent - would lack the owner's authorization unless the owner explicitly allows users to treat its data as their own. The owner's consent is dispositive, not the employee-user's. Facebook is not a closed system as in *Nosal,* however, and the system owner's consent (or lack thereof) does not decide this case because the corporate owner doesn't own the information stored on its computer system. Put differently, it's the owner of the data that matters, not the owner of the network.

Landlord-tenant trespass doctrines can help define the relationship between Facebook users and a third party like Power Ventures. The common law first focuses on the rights of the tenant: "A lessee of premises is privileged to be at reasonable times and in a reasonable manner on those portions of the premises retained in the possession of the lessor which are maintained or held open by him for the common use of his tenants or for the particular use of the lessee." Restatement (Second) of Torts, § 189 (1). That is what allows the tenant access to the common areas of the property.

As applied to a third party like Power Ventures, "[p]ersons entering the premises in the right of the tenant have the same privilege as is stated in Subsection (1)." *Id.* § 189 (2). And as the comments explain, "the phrase 'in the right of the tenant' is used to denote that a person is privileged to enter the land because of the fact that he is a licensee or an invitee of the lessee of the premises." *Id.* § 189 cmt. b.

Although restatements are merely well-respected summaries of the common law without binding legal ***9** authority, these common-law rules have been applied consistently throughout the United States. *See, e.g., State v. Dixon,* 725 A.2d 920, 922 (Vt. 1999) ("The common law is clear that the landlord may not prevent invitees or licensees of the tenant from entering the tenant's premises by passing through the common area."); *L.D.L. v. State,* 569 So.2d 1310, 1312 (Fla. Dist. Ct. App. 1990) ("A landlord generally does not have the right to deny entry to persons a tenant has invited to come onto his property."); *Arbee v. Collins,* 463 S.E.2d 922, 925 (Ga. Ct. App. 1995) (holding that an invitee who enters the premises with the tenant's permission, even if forbidden by the landlord, is not a trespasser); *State v. Schaffel,* 229 A.2d

552, 561 (Conn. Cir. Ct. 1966) (stating that "it is the tenant, not the landlord, who has the final word as to the person or persons who may enter upon the demised premises").

A user's invitee, like Power Ventures, is thus allowed to enter the common areas of the Facebook website that are held open to users for data access, subject to using those areas in a reasonable manner (*e.g.*, not facilitating crime). This privilege is not unlimited but is "subject to the terms of the lease," which here is analogous to the terms of service. *See id.* § 189 cmt. c. It is also subject to reasonable regulations "for the protection of the premises themselves or of other tenants." *Id.* Here, the terms of service don't purport to limit users' ability to invite third parties to access their data.

To be fair, there is one provision of the Facebook terms of service that Power Ventures could be seen as violating but which did not apply here for the "protection of the premises themselves or of other tenants." The terms of service prohibit accessing Facebook via automated means, which is what Power Ventures did ***10** in one sense. *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1067 (9th Cir. 2016). But using such automated means does not harm Facebook or other users. Whatever the "automated means" provision envisions, it does not clearly contemplate accessing Facebook friends lists. An automated entrant could cause harm, to be sure, but not by mere method of entry. For instance, if Power Ventures accessed Facebook fast enough to overload the system, that could be prohibited. No provision of the terms of service would even be required to stop such behavior given the facial harm to Facebook's property. But a person could also use automation and access Facebook slowly, as a normal user would, and not cause any harm. Using automation neither causes harm - Facebook doesn't allege that Power Ventures' method of access harmed anyone - nor revokes users' consent to the company's access of data.

C. Like Invited Guests in a Landlord-Tenant Relationship, It Is Common for Users to Allow Third Parties to Access Their Account

In interpreting the common law's application, it is important to consider people's customs. William Blackstone even described customs as forming the common law and judicial decision as merely evidence of those customs. 1 W. Blackstone, Commentaries on the Laws of England *69 (1765) ("[J]udicial decisions are the principal and most authoritative evidence, that can be given, of the existence of such a custom as shall form a part of the common law."). Here, the analogy between Facebook users and housing tenants is consistent with public custom in these situations. To provide otherwise would open up large numbers of people to criminal sanction for commonly accepted actions.

***11** Such concerns informed even the Ninth Circuit's opinion in *Nosal*: "Were we to adopt the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Nosal,* 676 F.3d at 859. Similarly here, if the lower court's opinion is allowed to stand, millions of unsuspecting people would be unknowingly engaging in criminal conduct for allowing access to data that they unquestionably own and have Facebook's permission to access at any time.

"People share passwords all the time. A husband might give his wife his bank account login so she can pay a bill. A professor might ask a secretary to check emails." Alan Yu, "How A 'Nightmare' Law Could Make Sharing Passwords Illegal," NPR (July 14, 2016), http://n.pr/2qILvW0. According to a recent survey, 95 percent of people share up to six passwords with other people. LastPass, Keep Your Friends Close & Your Passwords Closer, http://bit.ly/2qItiHY (Feb. 18, 2016). Many of those are financial, email, social media related in which the user likely owns the underlying data. *Id.* This is normal behavior; many would be shocked that the "kind of password sharing that millions of Americans innocently engage in with family and friends - of social media sites, streaming video services and bank accounts - could leave them open to criminal prosecution." Dan Mangan, "Your Password Isn't Yours to Share, and Here's Why That's a Problem," CNBC, (Jul. 12, 2016), http://cnb.cx/2qIlBSm. The normal activities of millions of people should not become subject to liability without a clear mandate from Congress. *Cf. United States v. Nosal,* 844 F.3d 1024, 1049 (9th Cir. 2016) (Reinhardt, .J, dissenting) ("The CFAA should not be interpreted to criminalize the ordinary conduct of millions of citizens.")

***12** One reason Americans share their digital lives with others so freely is because they feel that they own their content. When it comes to Facebook, they certainly do. Similarly, tenants would normally not wonder whether their lease agreement allows guests to visit; such authorized entries are the common behavior of property owners. Because Congress is presumed to legislate with knowledge of these customs, such practices should not be made illegal without "a clear indication that Congress intended such a departure." *Pa. Dep't of Pub. Welfare v. Davenport,* 495 U.S. 552, 563 (1990). Just as in the common law, people's behavior should inform how the CFAA is interpreted.

D. Because "Unauthorized" Access Under the CFAA Can Carry Criminal Penalties, the Court Should Consider the Rule of Lenity

While this is a civil action, the CFAA also authorizes criminal prosecution for violating the same provision that anchors civil liability here. In such cases, to maintain a consistent interpretation of the statute the Court has applied the rule of lenity in resolving any ambiguity. *Leocal v. Ashcroft,* 543 U.S. 1, 11 n.8 (2004) (citing *United States v. Thompson/Center Arms Co.,* 504 U.S. 505, 517-518 (1992) (plurality op.)) (holding that where a statute "has both criminal and noncriminal applications … we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies"). So if the CFAA were ambiguous as to the particulars of this case, the rule of lenity would augur an interpretation that favors Power Ventures. *United States v. Universal C. I. T. Credit Corp.,* 344 U.S. 218, 221-22 (1952) ("[W]hen [a] choice has to be made between two readings of what conduct Congress has ***13** made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.").

Indeed, if Mr. Vachani were to be criminally prosecuted under the CFAA for Power Ventures' activities here, he would face up to five years in federal prison. 18 U.S.C. § 1030(c)(2)(B). He and others should not lose their liberty on an ambiguous interpretation of the statute. When there are multiple possible interpretations - including with regard to the meaning of "authorization" here - the rule of lenity requires that the statute be interpreted in the defendant's favor.

II. THE COURT SHOULD GRANT THIS PETITION BECAUSE OF ITS IMPORTANCE TO THE DIGITAL ECONOMY

Power Ventures' service competes with Facebook, which is probably one reason Facebook banned the company from accessing its site even though there was (and could be) no harm to the system or its users. The lower court ratified Facebook's decision to go after such businesses as if they were "hackers." If allowed to stand, that ruling would cut off a potential source of online innovation instead of allowing market dynamics to work out who has the better product.

Facebook is not alone in explicitly granting users ownership over the data stored on the company's computers. Another commonly used example is Dropbox, an online cloud-storage service. Dropbox's terms of service state that, "When you use our Services, you provide us with things like your files, content, messages, contacts and so on ('Your Stuff'). Your Stuff is yours. These Terms don't give us any rights to Your Stuff except for the limited rights that enable us to offer the ***14** Services." *Dropbox - Terms,* Dropbox, http://bit.ly/2qIJo4n (last accessed May 22, 2017).

New startups that are unsure of the legal environment may not be willing to take risks that could land them in prison. By reviewing this case, the Court can resolve the legal uncertainty among the circuit courts and potential entrepreneurs can know for sure what they can do online without committing a crime.

Moreover, the split between the circuit courts over how to interpret "authorization" in the CFAA has substantial effects on major internet operations. Power Ventures used automated tools to access Facebook's website. In many ways, Google is a larger version of Power Ventures that accesses more websites than just Facebook. Preston Gralla, *How the*

Internet Works 133 (1998) ("Although the specifics of how [Internet Search engines] operate differ somewhat, they are all composed of … at least one spider, which crawls across the Internet gathering information.").

The date of that last source shows that the tools that Power Ventures uses have long been common on the internet. *See also* David L. Baumer & Julius Carl Poindexter, *Legal Environment of Business in the Information Age* 154 (2003) ("Screen scrapers are commonly used by some firms to gather information available on internet websites."). The importance of these kinds of activities is evidenced by the many books that have been written about "spiders," "screen scrapers," and other automated-access devices. *See generally,, e.g.*, Michael Schrenk, *Webbots, Spiders, and Screen Scrapers, 2nd Edition* (2012); Ryan Mitchell, *Web Scraping with Python: Collecting Data from the Modern Web* (2015); Ryan Mitchell, *Instant Web Scraping* ***15** *with Java* (2013). Such tools allow companies to aggregate information easily. *Id.* This information can then be combined in new and unexpected ways to provide numerous benefits to users. Those potential and existing benefits will be negatively affected by the threat of potential lawsuits if the legal landscape is unclear.

Internet companies operate throughout the country, underscoring the need for nationwide rules. In the face of conflicting circuit precedents, many companies try to comply with all rules so that the same service can be provided everywhere. Having one set of consistent legal rules would facilitate the digital economy.

CONCLUSION

The Court should grant the petition to resolve the three-way split among seven circuits as to the legal context for interpreting the prohibition on accessing a computer "without authorization." It should also grant the petition to consider Facebook users' property interests in the face of the common law of trespass. At base, this case is really important to the New Economy.

Footnotes

1 Rule 37 statement: All parties were timely notified and consented to the filing of this brief. Further, no counsel for any party authored this brief in whole or in part and no person or entity other than *amicus* funded its preparation or submission.

End of Document