Nos. 13-17102, 13-17154

---

**IN THE**

# United States Court of Appeals For The Ninth Circuit

---

FACEBOOK, INC.,

*Plaintiff-Appellee,*

*v.*

POWER VENTURES, INC.
&
STEVEN SURAJ VACHANI,

*Defendants-Appellants.*

---

Appeal from the United States District Court
for the Northern District of California
Case No. 5:08-cv-05780-LHK, The Honorable Lucy Koh

---

## APPELLEE FACEBOOK'S RESPONSE TO APPELLANTS' PETITION FOR REHEARING AND REHEARING EN BANC

---

I. Neel Chatterjee
Monte Cooper
Brian P. Goldman
Robert L. Uriarte
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025

Eric A. Shumsky
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005
(202) 339-8400

*Counsel for Appellee Facebook, Inc.*

# TABLE OF CONTENTS

Page

# TABLE OF AUTHORITIES

**Page(s)**

## Cases



## Statutes & Rules



## Legislative Materials

**Other Authorities**

## INTRODUCTION

This case provides an unsuitable vehicle for exploring the outer boundaries of the Computer Fraud and Abuse Act. It involves a factbound application of this Court's established precedents to conduct that falls within the heartland of the CFAA: Power Ventures' blatant disregard of Facebook's personalized message to "keep out," and its deliberate circumvention of the technical barriers that Facebook erected to enforce that command.

As the panel unanimously held, this Court's decisions in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), and *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*"), establish that a person accesses a computer "without authorization" if the computer's owner has denied or rescinded permission to access the computer, yet the person does so anyway. Thus, as in the physical world, a person commits trespass in the digital world when she ignores a proprietor's command to keep out, and then continues to sneak back in. Violating a business's general rules may not itself amount to trespass, whether of a storefront or a computer system. But defying a targeted instruction to stay away does. *Accord United States v. Nosal*, ___ F.3d ____, Nos. 14-10037 & 14-10275, 2016 WL 3608752 (9th Cir. July 5, 2016) ("*Nosal II*"). And rarely will a computer trespasser be as defiant as Power was here.

Facebook detected that Power was "scraping" content from Facebook's

website, and bombarding users of Facebook with annoying commercial messages, in ways that could interfere with their experiences on Facebook and threaten the security of their personal information. So Facebook contacted Power directly to demand that it stay out of Facebook's system. Facebook reinforced that message by building technical barriers to prevent Power from accessing Facebook's servers. Having predicted that Facebook would employ these very measures, Power then deployed what its CEO, Steven Vachani, named "workaround solution 1" to circumvent them. The panel correctly found that this evasion constituted access "without authorization."

Power and its amici mostly ignore these extreme facts, focusing instead on hypothetical scenarios that are easily distinguished. The typical couple sharing an online bank account, or an academic researcher studying an internet platform, hasn't first received a cease-and-desist letter demanding that they keep out of the computer system. Nor do they ordinarily use an array of "proxy servers" to circumvent technical measures that were put in place to enforce such bans. Unlike in Power's hypotheticals, Power's access was plainly unauthorized—which Power fully understood, as its own internal documents make clear. The panel did not err in limiting its analysis to the narrow and stark facts of *this* case, and Power is wrong that rehearing is necessary for this Court to issue an advisory opinion on cases that involve very different facts than this one. The petition should be denied.

## STATEMENT

1. Facebook's popular social networking service attracts businesses hoping to connect with Facebook's global community of users. SER394. News outlets like the *Los Angeles Times*, for example, let readers "share" articles with their Facebook "friends" by posting articles directly from latimes.com to their personal Facebook "profile." To enable this to happen, Facebook welcomes third-party developers to incorporate social features in ways that ensure the security of the data on Facebook's website, and the integrity of Facebook's services. ER181 ¶28; SER422 ¶28.

Appellant Power Ventures saw itself as "a competitor in the market for social networking websites"; Appellant Steven Vachani was its CEO. SER434 ¶173; *see also* SER421 ¶¶10-11; Op. 5-6. According to Power's "Internet User Bill of Rights," it "believes in a borderless Internet"—and, having proclaimed this to be so, Power designed a business based on aggregating user information from, and co-opting the networks that users had built on, other social media websites. *See* SER413, 419, 485. Thus, Power developed a software program to collect (or "scrape") user information from sites like Facebook. SER92, 160, 396, 481-86; *see* SER37. Such scraping software typically is prohibited by website operators like Facebook. Unlike Facebook's sharing features, scraping may put users' privacy at risk by exposing their data, and may impair the proper functioning of the

service. ER180-81; SER37, 422 ¶28, 482.

Because scraping was central to Power's business, but Facebook forbade it, Power did not want to go through approved channels to access Facebook. SER37, 372-73. Instead, Power solicited Facebook users' login credentials. SER37, 278. Power knew that Facebook would disapprove for security reasons, and "anticipated attempts to block [its] access by network owners." ER62 (citing SER273-74).

2. Power's prediction proved true. In late 2008, Facebook detected scraping software operating on its network. Op. 7; SER396. Power was collecting data about Facebook users, then downloading it to Power's website. ER52; SER376, 382, 396. Expert analysis later revealed that Power's software was also automatically generating and sending tens of thousands of junk-mail messages to Facebook users. Op. 8; ER55-56, 61; SER376. Facebook immediately sent a letter informing Power that its conduct was unauthorized and a violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and demanded that Power stop. Op. 7; SER298-300. In a follow-up communication, Facebook told Power it had blocked the company's access to Facebook. Op. 7; SER305-06.

Undeterred, Power's CEO brazenly informed his team that "we need to be prepared for Facebook to try to block us and the[n] turn this into a national battle that gets us huge attention." Op. 17 (quoting SER285); SER330. To that end, Power designed and deployed "workaround solution 1"—Power's plan to use

"proxy servers" to change its IP address (the Internet equivalent of Power's telephone number or mailing address) to circumvent Facebook's block. SER88; *see* Op. 7. Power had designed this "solution" specifically to connect to Facebook through proxies that would relay data and thereby conceal its origin. ER60-61 (citing SER273-74); SER495-98. Facebook promptly blocked each new IP address, but Power would then change the addresses again, "in a game of cat and mouse." ER61; *see* SER398. Finally, Power adopted its "Amazon solution," SER292: switching to an IP address associated with the popular website amazon.com, which Facebook could not block without also blocking others' authorized access to its system. ER60-61; SER387, 399.

After weeks of this back-and-forth, Power informed Facebook that it had made the "business decision" to continue accessing Facebook, even though Power knew "this is not your desired action." SER302. And Power chided Facebook for what it called the "serious strategic mistake" of trying to block Power. SER303. Power then used its unauthorized access to Facebook to engage in a massive marketing campaign, which involved co-opting users' accounts to send over 60,000 junk messages to all of the Power users' Facebook "friends." Op. 8.

3. Having failed to stop Power's trespasses with cooperative discussion, formal demands, and technical blocks, Facebook ultimately brought suit at the end of 2008. Then-Chief Judge Ware granted summary judgment to Facebook. ER64.

With respect to Facebook's claims under the CFAA and California's analogous statute (Penal Code § 502), "the undisputed facts establish that Defendants circumvented technical barriers to access [the] Facebook site." ER62. The court relied on "Vachani's own statements," which "provide compelling evidence that he anticipated attempts to block access by network owners and intentionally implemented a system that would be immune to such barriers"—a system Power then "utilized ... to effectively circumvent these barriers." *Id.* Judge Koh, who received the case from Chief Judge Ware, agreed. ER3-36. For Power's computer fraud violations, she awarded compensatory damages for Facebook's cost of investigating and trying to stop Power's actions. SER26. Judge Koh also issued an injunction to prevent additional violations, citing Power's clear willingness to keep violating the law in the face of clear and repeated requests to stop. ER33.

4. This Court unanimously affirmed the judgment with respect to the CFAA. Citing *Nosal I*, it reaffirmed that "a violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA." Op. 15-16. However, this Court's established precedent makes clear that a party "can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." Op. 14-16 (citing *Brekka*, 581 F.3d at 1135-36; *Nosal I*, 676 F.3d at 862-63; *Nosal II*, 2016 WL 3608752, at *1). And here, "Facebook expressly rescinded" whatever permission Power had to

access Facebook "when Facebook issued its written cease and desist letter" and "imposed IP blocks in an effort to prevent Power's continued access." Op. 17. "Power knew that it no longer had authorization to access Facebook's computers, but continued to do so anyway." Op. 17. It "deliberately disregarded the cease and desist letter and accessed Facebook's computers without authorization," and thus violated the CFAA. Op. 19.[1]

## REASONS FOR DENYING THE PETITION

"'En banc courts are the exception, not the rule.' They are 'not favored,' Fed. R. App. P. 35, and 'convened only when extraordinary circumstances exist.'" *Makaeff v. Trump Univ., LLC*, 736 F.3d 1180, 1180 (9th Cir. 2013) (Wardlaw & Callahan, JJ., concurring in the denial of rehearing en banc) (citation omitted). Accordingly, this Court "only invoke[s] the en banc process to secure or maintain uniformity of our decisions or because a question of exceptional importance is involved." *Id.* at 1187. This case does not remotely present those circumstances.

[1] The panel also affirmed the district court's orders imposing discovery sanctions on Power, and holding Vachani personally liable for his central role in the misconduct. Op. 21-22; *see* ER20-23, 43. The district court had granted Facebook summary judgment on its claim under the CAN-SPAM Act, 15 U.S.C. § 7704(a)(1), because of Power's "egregious" spamming activity. ER25-26, 56-59. The panel reversed on that count, finding that Power's spam messages were not in fact misleading. Op. 9-12.

## I. The Panel Correctly Applied Settled Precedent To The Egregious Facts Of This Case.

A. The panel's decision relies upon and is fully consistent with *Brekka* and *Nosal I*. The CFAA prohibits "acts of computer trespass" by those who are not "authorized user[s]" of a computer system. S. Rep. No. 99-432, at 9-10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487. Thus, as *Nosal I* explains, the CFAA provides robust protection against "violations of restrictions on *access* to information," but stops short of enforcing "restrictions on its *use*." 676 F.3d at 864. Just as an intruder who jumps a fence or defies a direct order to "keep out" will be liable for trespass, *see* Model Penal Code § 221.2(2)(a), (c), the same is true in the digital domain. *Nosal I*, 676 F.3d at 863.

*Nosal I* (which addressed the CFAA's "exceeds authorized access" prong) reaffirmed and elaborated on *Brekka* (which addressed the "without authorization" prong at issue here). *Brekka* held that it is the computer owner's "decision to allow or to terminate a[] [user's] authorization to access a computer" that "determines whether the [user] is with or 'without authorization.'" 581 F.3d at 1133. Thus, under *Brekka*, "a person uses a computer 'without authorization' under [the CFAA] when the person has not received permission to use the computer for any purpose …, *or when the [owner] has rescinded permission to access the computer and the defendant uses the computer anyway*." *Id.* at 1135 (emphasis added); *accord Nosal II*, 2016 WL 3608752, at *8.

That is precisely what occurred here. "Facebook expressly rescinded [Power's] permission [to access Facebook] when Facebook issued its written cease and desist letter to Power" and "then imposed IP blocks in an effort to prevent Power's continued access." Op. 17. But Power "use[d] [Facebook's] computer anyway." *Brekka*, 581 F.3d at 1135; Op. 17. It "deliberately disregarded" Facebook's targeted direction to keep out, and "circumvented [Facebook's] IP barriers" by activating its "workaround solution 1." Op. 19; SER88. As the Electronic Frontier Foundation (EFF) itself admitted in its first amicus brief in this case (at 12): "If a particular technological restriction seeks to control access to or use of data from an entity unauthorized to obtain it, and the person has notice of that fact, then evasion of the technological restriction is likely" a violation.[2] That's just what Power did. Accordingly, it "accessed Facebook's computers 'without authorization' within the meaning of the CFAA." Op. 19. The panel's correct articulation of these settled principles, and application of them to Power's flagrant conduct, merits no further review.

B. Power nevertheless argues that "the panel decision is irreconcilable with this Court's *en banc* decision in *Nosal*." Pet. 5. According to Power, *Nosal I*

[2] EFF's newfound position—that the CFAA is limited to burglary-type "break[ing] into a computer," EFF Reh'g Br. 3—finds no support in the text of the statute or its objective of combatting computer *trespass*. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015) (reviewing the legislative history).

declared that no "written restriction" can give rise to a CFAA violation, so relying on Facebook's cease-and-desist letter contradicts *Nosal I*. Pet. 1, 6-7; *see also* EFF Reh'g Br. 8-9. But that isn't what *Nosal I* said. As the panel explained, "*Nosal I* was most concerned" with "terms of use" and the risk of creating "criminal liability for computer users who might be unaware that they were committing a crime." Op. 20; *see Nosal I*, 676 F.3d at 860 (emphasizing the "[s]ignificant notice problems [that] arise if … criminal liability [were] to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read"). By contrast, disregarding an "actual communication to the actor" prohibiting entry gives rise to trespass in a way that violating mere rules of conduct does not. Model Penal Code § 221.2(2)(a). That has been the rule in the physical world for centuries. *Id.* § 221.2(2)(a)-(c). And with good reason: There is no risk of stumbling into liability under a test that requires a notorious command to stay out, like a personalized letter or a targeted digital fence.[3]

That the cease-and-desist letter was motivated in part by Power's violation

[3] The panel was attentive to ensuring that Power indeed received proper notice, *e.g.*, Op. 20, for which Power accuses the panel of "confus[ing]" the CFAA's substantive element ("without authorization") with mens rea. Pet. 7-8. Power misreads the opinion. The panel construed "without authorization" to require that a party be informed that authority has been withdrawn before that party will be deemed to act "without authorization." The panel's focus on fair notice is cause for comfort, not criticism, and it follows directly from *Nosal I*. *See* Op. 20 (discussing 676 F.3d at 860).

of Facebook's policies is beside the point. *Cf.* Pet. 6-7; *see also* EFF Reh'g Br. 8-9. When a restaurant's rules say "no shirt, no shoes, no service," a patron does not commit trespass just by entering barefoot. But if, after being told to leave and not return, he sneaks back in through a window, he has trespassed, even if the reason he was banished is that he violated the proprietor's rules. The panel recognized that the same is true in the digital realm: "Violation of Facebook's terms of use, without more, would not be sufficient to impose liability" under *Nosal I*, but "deliberately disregard[ing]" a personalized demand to keep out *does* amount to access without authorization. Op. 17 n.2, 19.

Power is thus flatly wrong in asserting that "[t]his case involves the same scenario" of innocuous password sharing described in *Nosal I*. Pet. 5. *Nosal I* suggested that allowing "close friends and relatives to check their email or access their online accounts" would not be unauthorized access under the CFAA simply by virtue of violating a service provider's terms of use. Pet. 5 (quoting *Nosal I*, 676 F.3d at 861). As an initial matter, the panel opinion reaffirms rather than contradicts that holding: "[A] violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA." Op. 16, 17 n.2.

Moreover, the panel correctly held that this case involves much "more." Power "deliberately disregarded" a personalized demand to keep out. Op. 19. And Power "circumvented IP barriers" that Power knew had been put in place

specifically to keep it out. Op. 17-19; *see* ER21, 61-62; SER82, 87-88, 285, 292, 386-87; *see also* SER160 (Power's own executive likening Power's activity to "trespass to chattels").[4] That "circumvention of technological access barriers" was precisely the sort of access that *Nosal I* held impermissible. 676 F.3d at 863-64. The proper analogy, therefore, is not to mere innocuous password sharing—it is to someone who continues to use his friend's online account even *after* having been directly told by the provider to keep out of its systems entirely, and who does so by implementing a technical "workaround" to circumvent technological measures targeted at him specifically. That would be trespass, as it was here. Power ignores this aspect of the decision entirely.

C. Adopting Power's rule, in contrast, would create a conflict with settled authority. The upshot of Power's argument is that Facebook had *no right* to exclude Power from its system—even as Power used its illicit access to send over 60,000 junk emails—because, Power says, the permission it ostensibly received from its users gave it carte blanche to access Facebook. Pet. 9-11; EFF Reh'g Br.

[4] For this same reason, EFF is mistaken in contending (at 9-10) that the decision conflicts with *Nosal II*. In both cases, the defendants initially had permission to access a computer (express permission in *Nosal II*, and "implied authorization" in this case, Op. 21), but lost that permission when the computer owner rescinded it—and the defendants therefore violated the CFAA when they surreptitiously accessed the computer anyway. Far from conflicting with *Nosal II*, the panel opinion followed and relied upon it. *E.g.*, Op. 20 ("This case is closer to *Nosal II*, wherein liability attached after permission to access computers was expressly revoked, but then the defendant deliberately circumvented the rescission of authorization.").

7-9. That rule contradicts *Brekka* (as reaffirmed in *Nosal I*) and basic principles of property law.

*Brekka* establishes that the computer's *owner* has the "authority" to grant "permission" to access a "protected computer." There, it was the employer who owned "the company computer" that it had initially "permitted Brekka to use," before "rescind[ing] [his] permission." 581 F.3d at 1132-33, 1135; *see Nosal II*, 2016 WL 3608752, at *8-9 (relying on *Brekka*; holding that the party who may "grant or revoke … permission" is the party who "own[s] and control[s] access to its computers"). Accordingly, as the panel explained, a bank may eject a disruptive visitor notwithstanding that a bank customer had delegated authority to the visitor to access the customer's safe deposit box. Op. 18-19. The bank remains entitled to "control[] access to its premises." Op. 19. It may do so by ejecting the visitor directly; terminating the customer's account is not the only way to rescind authorization. *Contra* Pet. 3; EFF Reh'g Br. 7. Here as well, the permission Power received from users could not trump Facebook's right to exclude Power directly from connecting with its system. Op. 19.

## II. This Case Is A Poor Vehicle For Addressing Appellants' Many Hypotheticals.

Power faults the panel for failing to address various factual scenarios that are remote from this case. Pet. 8-9; *see also* EFF Reh'g Br. 12-14 (same). But the panel set out to write a judicial opinion, not a law review article. It properly

decided that the concrete facts before it gave rise to a CFAA violation, while leaving hypothetical questions to future courts. *E.g.*, Op. 16 n.1, 21 ("[W]e need not decide whether websites such as Facebook are presumptively open to all comers," because here Power "initially" had "implied" permission to access Facebook). Power similarly complains (at 8-9) that the panel did not opine whether any one aspect of Power's misconduct, standing alone, would have been dispositive. But this Court "need not decide whether any single fact would be enough to support [an outcome] because we are not called upon to review single facts in isolation." *United States v. Valdes-Vega*, 738 F.3d 1074, 1081 (9th Cir. 2013) (en banc).

And this certainly isn't the case for issuing broad guidance to "millions of Internet users." Pet. 9. It involves especially uncommon facts, as Power and its amici's own hypotheticals make clear. Power and EFF express concern about everyday activities like people "let[ting] close friends and relatives check their email or access their online accounts," Pet. 5, or asking a family member to "pay a bill" online, EFF Reh'g Br. 14. But, of course, in none of those hypotheticals are people personally ejected from a computer system through a communication that they unequivocally received and understood, and targeted with technical measures designed to prevent them from reentering, before employing multiple "workaround

solution[s]" to get back in surreptitiously.[5]

Finally, Power errs in suggesting that individual users "would presumably be guilty of violating the CFAA by aiding and abetting" an actor like Power. Pet. 14. On the contrary, aiding-and-abetting liability requires the "intent of facilitating the offense's commission." *Rosemond v. United States*, 134 S. Ct. 1240, 1245 (2014); *id.* at 1248-50. There is no reason to think that the individual users *knew* of measures Facebook took to keep Power out—or would have any idea of such measures in any future case—let alone that the users would intend to facilitate the deliberate circumvention of those measures by Power.

## CONCLUSION

The petition for rehearing and rehearing en banc should be denied.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

*/s/ Eric A. Shumsky*
Eric A. Shumsky
*Counsel for Appellee Facebook, Inc.*

September 15, 2016

[5] EFF also worries (at 16-17) about "account holders [who] use their accounts for research purposes" not permitted by a website owner. But violations of "restrictions on … *use*" fall outside the CFAA under *Nosal I*, 676 F.3d at 864, as the panel reaffirmed, Op. 16.

## CERTIFICATE OF COMPLIANCE

This response complies with the type-volume limitation of Ninth Circuit Rule 40-1(a) because this brief contains 3,600 words, excluding the parts of the response exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This response complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in Times New Roman 14-point font.

ORRICK, HERRINGTON & SUTCLIFFE LLP

*/s/ Eric A. Shumsky*
Eric A. Shumsky
*Counsel for Appellee Facebook, Inc.*

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on September 15, 2016.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

ORRICK, HERRINGTON & SUTCLIFFE LLP

*/s/ Eric A. Shumsky*
Eric A. Shumsky
*Counsel for Appellee Facebook, Inc.*