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, Honorable Lucy Koh

PETITION FOR PANEL REHEARING AND REHEARING EN BANC

Amy Sommer Anderson AROPLEX LAW 156 2nd Street San Francisco, CA 94105 (415) 866-4066 Marcia Hofmann ZEITGEIST LAW PC 25 Taylor Street San Francisco, CA 94102 (415) 830-6664 Orin S. Kerr LAW OFFICE OF ORIN S. KERR 2000 H Street, NW Washington, DC 20052 (202) 994-4775

Counsel for Defendant Appellant Power Ventures, Inc.

Steven Vachani 2425B Channing, #216 Berkeley, CA 94704 (917) 267-9923 *Pro Se* Appellant Case: 13-17154, 08/09/2016, ID: 10081753, DktEntry: 85-1, Page 2 of 18

CORPORATE DISCLOSURE STATEMENT

There is no parent corporation and no publicly held corporation that owns

10% or more of Power Ventures, Inc.'s stock.

TABLE OF CONTENTS

TABLE OF CONTENTS	iii
TABLE OF AUTHORITIES	iv
INTRODUCTION AND RULE 35(b) STATEMENT	5
FACTUAL AND PROCEDURAL BACKGROUND	6
REASONS FOR GRANTING REHEARING	9
I. The Panel Opinion Conflicts With This Court's <i>En Banc</i> Decision in <i>United States v. Nosal</i>	9
II. Rehearing is Necessary to Clarify When Internet Users Will Face Criminal and Civil Liability for Violating Written Restrictions Governing Access to Computers	12
III. Rehearing is Necessary to Ensure that Internet Users Can Delegate Access Rights to Their Agents	13
CONCLUSION	15
CERTIFICATE OF COMPLIANCE	17
CERTIFICATE OF SERVICE	18

(4 of 41)

Case: 13-17154, 08/09/2016, ID: 10081753, DktEntry: 85-1, Page 4 of 18

TABLE OF AUTHORITIES

CASE LAW

<i>Facebook, Inc. v. Power Ventures, Inc.</i> , 5:08-cv-05780-LHK (N.D. Cal. 2008)	4
<i>Facebook, Inc. v. Power Ventures, Inc.</i> , 844 F. Supp. 2d 1025 (N.D. Cal. 2012)	4
<i>LVRC Holdings LLC v. Brekka</i> , 581 F.3d 1127, 1134 (9th Cir. 2009)	*
United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)	1, 2, 5-8, 10, 11
<i>United States v. Nosal</i> , Nos. 14-10037 & 14-10025 (9th Cir. July 5, 2016) (" <i>Nosal II</i> ")	11,12

STATUTES

15 U.S.C. §7701 - Controlling the Assault of Non-Solicited	
Pornography And Marketing Act of 2003 ("CAN-SPAM Act")	3
18 U.S.C. § 2	10
18 U.S.C. § 1030 - Computer Fraud and Abuse Act ("CFAA")	1, 2, 4-6, 8- 11
California Penal Code § 502	2, 4, 5, 11

OTHER TEXTS

Restatement (Third) of Agency § 2.01 (Am. Law Inst. 2006)..... 10

INTRODUCTION AND RULE 35(b) STATEMENT

The scope of the Computer Fraud and Abuse Act ("CFAA"), codified at 18 U.S.C. § 1030, is important to every computer user in the United States. Although the CFAA includes a civil cause of action, it is primarily a criminal statute. The CFAA's line between authorized and unauthorized access to computers means the difference between lawful conduct and criminal liability for every American who uses the Internet.

In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*), this Court recognized the threat of broad readings of the CFAA. *Nosal* held that written restrictions on use of a computer, such as website terms of use or an employer's workplace policy, do not control whether access is authorized. *See id.* at 863-64. Under *Nosal*, a user is legally authorized to use his Facebook account even in the face of a written statement on Facebook's website that Facebook prohibits the use.

The panel opinion in this case conflicts with the *en banc* decision in *Nosal* and creates tremendous confusion about when using the Internet is a crime. The panel opinion holds that *Nosal* does not apply when Facebook users permit a third-party to access their accounts and Facebook issues a cease-and-desist letter indicating that the third-party use violates its terms of service. Slip op. at 19-20 (ECF No. 77-1). The panel's rationales for distinguishing *Nosal* were rejected in

Nosal itself, however, and they are premised on confusion between the act and mental state elements of the CFAA.

Rehearing is necessary to ensure that the panel opinion does not gut the *en banc* decision in *Nosal* and to avoid widespread confusion about when visiting a website is a crime. The Court already recognized the exceptional importance of the question when it granted the petition for rehearing in *Nosal*. The conflict between *Nosal* and the reasoning of the panel decision makes it necessary to grant rehearing once again to clarify the scope of the law.

Power Ventures and Steven Vachani (collectively "Power") ask this Court to grant panel rehearing or rehearing en banc with respect to liability under the CFAA. Because liability under the CFAA's state counterpart, California Penal Code § 502, was treated as a subsidiary question, Power also seeks review of liability under § 502. Power does not seek rehearing as to the remaining issues decided in the panel opinion.

FACTUAL AND PROCEDURAL BACKGROUND

In 2006, Power created a service for users of social networking sites such as Facebook and MySpace. Power's service allowed users to aggregate and manage their information and contacts from their accounts on multiple social networking sites at a single website hosted by Power at Power.com. SER 2 at ¶ 2. To utilize

Power's service, users would authorize Power to access their accounts and act on their behalves in executing activities specifically directed by the users.

Facebook objected to this practice and sent a cease-and-desist letter informing Power that Power's conduct "violated Facebook's Terms of Use." SER 298. The letter listed six different terms of use violations that Facebook believed Power had committed by operating as an agent of Facebook's users and acting on the users' behalves. SER 298-99. These violations included accessing another person's Facebook account without Facebook's permission and using Facebook for commercial purposes not expressly approved by Facebook. SER 298-99. The letter then informed Power of various legal causes of action that Facebook believed it "may" have against Power for Power's conduct. SER 299. The letter concluded by asking Power to confirm that in the future it would comply with Facebook's terms of use. SER 299.

After the letter was received, Facebook and Power entered into extensive negotiations about Power's service. Power Opening Brief at 15; 2-ER 173 at ¶ 11; 2-ER 96 at ¶ 6; 2-ER 103-108. When the negotiations were not satisfactorily resolved, Facebook eventually concluded that it did not want Power to access its website. Facebook did not suspend any Facebook user account or revoke any user credentials. Instead, Facebook sued Power, asserting the various causes of action it mentioned in the cease-and-desist letter, including violations of the CFAA, its state

counterpart, California Penal Code § 502, and the CAN-SPAM Act, 15 U.S.C. §7701. Compl., *Facebook, Inc. v. Power Ventures, Inc.*, 5:08-cv-05780-LHK (N.D. Cal. 2008) (ECF No. 1). The parties eventually stipulated to the dismissal of most of Facebook's claims, leaving only causes of action under the CFAA, Section 502, and the CAN-SPAM Act. (ECF No. 97).

In 2012, the district court granted summary judgment in favor of Facebook on all three claims, finding (*inter alia*) that Power violated the CFAA and Section 502 by taking steps to avoid Facebook's efforts to block IP addresses associated with Power. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1038-40 (N.D. Cal. 2012).

On July 12, 2016, the panel ruled for Power under CAN-SPAM, but ruled for Facebook on its claims brought under the CFAA and Section 502. Slip op. at 12. According to the panel, the cease-and-desist letter placed Power on notice that visiting Facebook's website was unauthorized under the CFAA. Because Power continued to visit Facebook "after receiving the cease and desist letter," Power "intentionally accessed Facebook's computers knowing that it was not authorized to do so [and was] liable under the CFAA." *Id.* at 20. The panel added that Power violated Section 502 for the same reason. *Id.* at 20-21.

REASONS FOR GRANTING REHEARING

I. The Panel Opinion Conflicts With This Court's *En Banc* Decision in *United States v. Nosal*.

This Court should grant rehearing because the panel decision is irreconcilable with this Court's *en banc* decision in *Nosal*. *Nosal* held that "violations of private computer use policies" governing access to websites "fail to meet the element of 'without authorization, or exceeds authorized access'" under the CFAA. 676 F.3d at 860, 863. Tellingly, *Nosal* used the hypothetical of a Facebook user permitting someone else to access his account in violation of Facebook's terms of use as example of an access that would be *authorized* under its decision:

Facebook makes it a violation of the terms of service to let anyone log into your account . . . Yet it's very common for people to let close friends and relatives check their email or access their online accounts.

Id. at 861.

This case involves the same scenario. Facebook users gave Power permission to access their Facebook accounts. That access was concededly in violation of Facebook's terms of use. But under *Nosal*, this violation of terms of use is irrelevant to CFAA liability. The Facebook users had legitimate Facebook accounts that they were authorized to access despite the terms of use violation, just like the errant employees in *Nosal*. And Power accessed the users' accounts with

their permission, acting as their agents, just as *Nosal* contemplated for "close friends and relatives" as authorized access. *Nosal*, 676 F.3d at 863. Yet according to the panel, access in one of these situations violates the CFAA while access in the other does not.

The panel offered three reasons why *Nosal* was "materially distinguishable" from this case. Slip op. at 19. The failure of these reasons to distinguish *Nosal* is at the heart of why rehearing is necessary: The panel's inability to explain why it treated like cases differently leaves the legal rule a mystery.

The panel's first argument for distinguishing *Nosal* is that *Nosal* involved a user who "arguably" exceeded authorized access while this case involve a user who accessed a computer "without authorization." *Id.* at 19-20. According to the panel, there is a critical distinction between a written restriction ordering a user to stay out entirely (which is binding, rendering access "without authorization") and a written restriction ordering a user to stay out only sometimes (which is not binding, as it is not exceeding authorized access under *Nosal*). *Id.*

This distinction is refuted by *Nosal* itself. *Nosal* held that violations of written restrictions do not "meet the element of *without authorization, or exceeds authorized access*" under the CFAA. 676 F.3d at 863 (emphasis added). Its rule covered both forms of unauthorized access. *Nosal* rejected the panel's idea that there is a significant difference between "access without authorization" and

Case: 13-17154, 08/09/2016, ID: 10081753, DktEntry: 85-1, Page 11 of 18

conduct that "exceeds authorized access," instead concluding that they are the same prohibition. The only distinction is that they simply cover slightly different kinds of trespassers—insiders versus outsiders. *Id.* at 858.

Second, the panel deemed *Nosal* distinguishable because Power was an outsider not subject to any contractual "terms and conditions" of the Facebook website. Slip op. at 20. To the extent this rationale does not just restate the panel's first argument, it fails because the basis of Facebook's case is that Power *was* subject to those terms and conditions. The crux of Facebook's cease-and-desist letter was that Power had violated Facebook's terms of use. SER 298-99. The letter listed the terms of use violations in detail, and it concluded by asking Power to comply with Facebook's terms of use. SER 298-99. Facebook's terms of use make clear that *anyone* who uses Facebook is subject to its terms and conditions. *See* Facebook's Terms of Use ("Statement of Rights and Responsibilities") at https://www.facebook.com/legal/terms. Its own language rejects the panel's attempted distinction.

Finally, the panel tried to distinguish *Nosal* based on the defendants' state of mind. *Nosal* was concerned with Internet users who were "unaware" of written restrictions, the panel explained, while Power "intentionally refused to comply" with Facebook's written language. Slip op. at 20. This attempted distinction is based on confusion between two different elements of the CFAA. To violate the

CFAA, a person must (1) access a computer without authorization or exceed authorized access, and (2) do so intentionally. 18 U.S.C. 1030(a)(2)(C). *Nosal* only interpreted the first element, whether the act of unauthorized access was satisfied. Power's state of mind only goes to the second element of whether the *mens rea* of intent was satisfied. As such, it cannot form a basis for distinguishing *Nosal*'s interpretation of unauthorized access.

II. Rehearing is Necessary to Clarify When Internet Users Will Face Criminal and Civil Liability for Violating Written Restrictions Governing Access to Computers.

Every Internet user regularly encounters written restrictions on using computers. *See Nosal*, 676 F.3d at 856-857. The panel's failure to identify a substantial basis to distinguish *Nosal* creates a great deal of confusion about the critical question the *en banc* court in *Nosal* tried to resolve: When is use of a computer in violation of a written restriction a federal crime? The combination of the panel decision and *Nosal* leaves the answer distressingly unclear.

For example, does liability depend on whether the written restriction forbids the user to access the website entirely or merely conditions when access occurs? *Nosal* indicates that the scope of the restriction makes no difference, but the panel suggests it may be decisive. *Compare Nosal*, 676 F.3d at 863 *with* slip op. at 19-20. Alternatively, does it matter whether the written restriction is found on the computer accessed, or whether it comes in the form of a letter? Does it matter if the letter merely repeats the terms of use of the website or whether it adds additional restrictions? Does it matter if the restrictions provide clear notice? At various points, the panel opinion suggests that these differences may or may not be critical. *See* slip op. at 17 n.2, 19-20.

By failing to identify the boundary between lawful and unlawful behavior, the panel decision leaves the law unclear for millions of Internet users. Although this case happens to involve a civil suit, any interpretation of the CFAA in a civil context is equally applicable in a criminal prosecution. *LVRC Holdings LLC v*. *Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009). *Brekka* stressed that the Court should be reluctant to interpret the CFAA "in surprising and novel ways that impose unexpected burdens" on criminal defendants. *Id*. Unfortunately, the panel decision does precisely that.

III. Rehearing is Necessary to Ensure that Internet Users Can Delegate Access Rights to Their Agents.

The panel also ruled that an Internet account holder cannot delegate rights to access his account on his behalf over the computer owner's objection. Slip op. at 18. The panel's holding that Internet users cannot delegate access rights to agents greatly expands criminal liability online and provides another reason to grant rehearing. Delegating computer access rights to agents is a routine part of using the Internet. As *Nosal* noted, "it's very common for people to let close friends and relatives check their email or access their online accounts." 676 F.3d at 861. Similarly, an employee might ask a co-worker to access her e-mail to check if a document arrived. An Internet user who wants to export his e-mail from one account to another might use a third-party program to do so. Indeed, using any Internet service is a sort of delegation: A person does not surf the web so much as have Internet-connected computers do so on his behalf.

Under the panel decision, all of these uses are criminal whenever the computer owner objects to the delegation. This conclusion flouts the traditional legal rule that an agent acting on a principal's behalf has the legal authority of the principal and acts as the principal. *See*, *e.g.*, Restatement (Third) of Agency § 2.01 (Am. Law Inst. 2006). The panel's sole support was a hypothetical about physical entry into a bank that itself cites no authority and is based on analogizing visiting a public website to entering a bank armed with a shotgun. Slip op. at 18-19.

Further, the panel's holding not only makes a criminal of the agent: It also likely makes a criminal out of the principal. The individual Facebook account holder would presumably be guilty of violating the CFAA by aiding and abetting the agent's conduct. *See* 18 U.S.C. § 2. This result is in direct conflict with *Nosal* and signals a dramatic expansion of criminal liability that the Court warned about in *Brekka*. See generally United States v. Nosal, Nos. 14-10037 & 14-10025 (9th Cir. July 5, 2016) ("*Nosal II*"), slip op. at 47 (Reinhardt, J., dissenting) (noting that interpreting the CFAA to prohibit password-sharing "loses sight of the anti-hacking purpose of the CFAA, and despite our warning, threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens.").

When Power accessed its customers' Facebook accounts with their permission, it was acting as its customers' agents. Because the customers were authorized to access their own accounts, Power was authorized as well. The Court should grant rehearing to ensure that the CFAA does not criminalize access by an agent in furtherance of the principal's wishes.

CONCLUSION

Power Ventures and Steven Vachani respectfully ask the Court to grant panel rehearing or rehearing en banc on whether they violated 18 U.S.C. § 1030. Because the panel's analysis of CFAA liability also determined its analysis of liability under California's state equivalent statute, Penal Code § 502, *see* slip op. at 20-21, they also respectfully ask the Court to grant panel rehearing or rehearing en banc on whether they violated California Penal Code § 502. To the extent that the Court sees common issues raised by this case and *Nosal II*, decided on July 5th, 2016, the Court may wish to grant rehearing in both cases. The petition for rehearing in *Nosal II* is currently due on August 18, 2016.

AROPLEX LAW

Dated: August 9, 2016

By <u>/s/ Amy Sommer Anderson</u>

<u>FILER'S ATTESTATION</u>: Pursuant to Circuit Rule 25-5(f), I attest under penalty of perjury that all other parties on whose behalf the filing is submitted concur in the filing's content.

Dated: August 9, 2016

/s/ Amy Sommer Anderson

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

I certify that this brief complies with the type-volume limitation set forth in

Rule 35(b)(2) of the Federal Rules of Appellate Procedure. This brief uses a

proportional typeface and 14-point font and contains 2,553 words.

Dated: August 9, 2016

/s/ Amy Sommer Anderson

CERTIFICATE OF SERVICE

I declare:

I am a citizen of the United States, employed in the City and County of San Francisco, over the age of eighteen years, and not a party to the within case. My business address is AROPLEX LAW, 156 2nd Street, San Francisco, California 94105. 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.

I declare under penalty of perjury that the foregoing is true and correct and that this declaration was executed on August 9, 2016, at San Francisco, California.

/s/ Amy Sommer Anderson

Case: 13-17154, 08/09/2016, ID: 10081753, DktEntry: 85-2, Page 1 of 23

FOR PUBLICATION

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

FACEBOOK, INC., a Delaware corporation, <i>Plaintiff-Appellee</i> , v.	No. 13-17102 D.C. No. 5:08-cv-05780-LHK
POWER VENTURES, INC., DBA Power.com, a California corporation; POWER VENTURES, INC., a Cayman Island corporation, <i>Defendants</i> ,	
and	
STEVEN SURAJ VACHANI, an individual, <i>Defendant-Appellant</i> .	

(19 of 41)

Case: 13-17154, 08/09/2016, ID: 10081753, DktEntry: 85-2, Page 2 of 23

2 FACEBOOK V. VACHANI	
	1
FACEBOOK, INC., a Delaware corporation,	No. 13-17154
Plaintiff-Appellee,	D.C. No. 5:08-cv-05780-LHK
V.	5.08-CV-05/80-LHK
POWER VENTURES, INC., DBA Power.com, a California corporation, <i>Defendant</i> ,	OPINION
and	
POWER VENTURES, INC., a Cayman Island corporation; and Steven Suraj Vachani, an individual, Defendants Appellants.	
Appeals from the United Sta	Ites District Court

Appeals from the United States District Court for the Northern District of California Lucy H. Koh, District Judge, Presiding

Argued and Submitted December 9, 2015 San Francisco, California

Filed July 12, 2016

Before: Susan P. Graber, Kim McLane Wardlaw, and Mary H. Murguia, Circuit Judges.

Opinion by Judge Graber

3

SUMMARY*

CAN-SPAM Act / Computer Fraud

The panel affirmed in part and reversed and vacated in part the district court's summary judgment in favor of Facebook, Inc., on its claims against Power Ventures, Inc., a social networking company that accessed Facebook users' data and initiated form e-mails and other electronic messages promoting its website.

Reversing in part, the panel held that Power's actions did not violate the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or CAN-SPAM Act, which grants a private right of action for a provider of Internet access service adversely affected by the transmission, to a protected computer, of a message that contains, or is accompanied by, header information that is materially false or materially misleading. The panel held that here, the transmitted messages were not materially misleading.

Reversing in part and affirming in part, the panel held that Power violated the Computer Fraud and Abuse Act of 1986, or CFAA, which prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use, and California Penal Code § 502, but only after it received a cease and desist letter from Facebook and nonetheless continued to access Facebook's computers without permission. With regard to authorization, the panel stated that a defendant can run afoul of the CFAA when he or she has no

^{*} This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

4

permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. The panel also stated that a violation of the terms of use of a website, without more, cannot be the basis for liability under the CFAA.

The panel vacated the district court's awards of injunctive relief and damages and remanded for consideration of appropriate remedies under the CFAA and § 502.

COUNSEL

Amy Sommer Anderson (argued), Aroplex Law, San Francisco, California; Steven Vachani (argued pro se), Berkeley, California, for Defendants-Appellants.

Eric A. Shumsky (argued), Orrick, Herrington & Sutcliffe LLP, Washington, D.C.; I. Neel Chatterjee, Monte Cooper, Brian P. Goldman, and Robert L. Uriarte, Orrick, Herrington & Sutcliffe LLP, Menlo Park, California, for Plaintiff-Appellee.

Jamie L. Williams (argued), Hanni M. Fakhoury, and Cindy A. Cohn, Electronic Frontier Foundation, San Francisco, California, as and for Amicus Curiae.

OPINION

GRABER, Circuit Judge:

One social networking company, Facebook, Inc., has sued another, Power Ventures, Inc., over a promotional campaign. Power accessed Facebook users' data and initiated form emails and other electronic messages promoting its website. Initially, Power had implied permission from Facebook. But Facebook sent Power a cease and desist letter and blocked Power's IP address; nevertheless Power continued its campaign. Facebook alleges that Power's actions violated the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), the Computer Fraud and Abuse Act of 1986 ("CFAA"), and California Penal Code section 502. We hold that Power did not violate the CAN-SPAM Act because the transmitted messages were not materially misleading. We also hold that Power violated the CFAA and California Penal Code section 502 only after it received Facebook's cease and desist letter and nonetheless continued to access Facebook's computers without permission. Accordingly, we affirm in part, reverse in part, and remand to the district court.

BACKGROUND

Defendant Power Ventures, a corporation founded and directed by CEO Steven Vachani, who also is a defendant here, operated a social networking website, Power.com. The concept was simple. Individuals who already used other social networking websites could log on to Power.com and create an account. Power.com would then aggregate the user's social networking information. The individual, a "Power user," could see all contacts from many social

5

6

networking sites on a single page. The Power user thus could keep track of a variety of social networking friends through a single program and could click through the central Power website to individual social networking sites. By 2008, the website had attracted a growing following.

Plaintiff Facebook also operates a social networking website, Facebook.com. Facebook users, who numbered more than 130 million during Power's promotional campaign, can create a personal profile—a web page within the site—and can connect with other users. Facebook requires each user to register before accessing the website and requires that each user assent to its terms of use. Once registered, a Facebook user can create and customize her profile by adding personal information, photographs, or other content. A user can establish connections with other Facebook users by "friending" them; the connected users are thus called "friends."

Facebook has tried to limit and control access to its website. A non-Facebook user generally may not use the website to send messages, post photographs, or otherwise contact Facebook users through their profiles. Instead, Facebook requires third-party developers or websites that wish to contact its users through its site to enroll in a program called Facebook Connect. It requires these third parties to register with Facebook and to agree to an additional Developer Terms of Use Agreement.

In December 2008, Power began a promotional campaign to attract more traffic to its website; it hoped that Facebook users would join its site. Power placed an icon on its website with a promotional message that read: "First 100 people who bring 100 new friends to Power.com win \$100." The icon

included various options for how a user could share Power with others. The user could "Share with friends through my photos," "Share with friends through events," or "Share with friends through status." A button on the icon included the words "Yes, I do!" If a user clicked the "Yes, I do!" button, Power would create an event, photo, or status on the user's Facebook profile.

In many instances, Power caused a message to be transmitted to the user's friends within the Facebook system. In other instances, depending on a Facebook user's settings, Facebook generated an e-mail message. If, for example, a Power user shared the promotion through an event, Facebook generated an e-mail message to an external e-mail account from the user to friends. The e-mail message gave the name and time of the event, listed Power as the host, and stated that the Power user was inviting the recipient to this event. The external e-mails were form e-mails, generated each time that a Facebook user invited others to an event. The "from" line in the e-mail stated that the message came from Facebook; the body was signed, "The Facebook Team."

On December 1, 2008, Facebook first became aware of Power's promotional campaign and, on that same date, Facebook sent a "cease and desist" letter to Power instructing Power to terminate its activities. Facebook tried to get Power to sign its Developer Terms of Use Agreement and enroll in Facebook Connect; Power resisted. Facebook instituted an Internet Protocol ("IP") block in an effort to prevent Power from accessing the Facebook website from Power's IP address. Power responded by switching IP addresses to circumvent the Facebook block. Through this period, Power continued its promotion even though it acknowledged that it

8

took, copied, or made use of data from Facebook.com without Facebook's permission.

Power's campaign lasted less than two months. On December 20, 2008, Facebook filed this action. Toward the end of January 2009, Power ended its campaign. In April 2011, Power ceased doing business altogether. In total, more than 60,000 external e-mails promoting Power were sent through the Facebook system. An unknown number of internal Facebook messages were also transmitted.

In this action, Facebook alleged violations of the CFAA, the CAN-SPAM Act, and California Penal Code section 502 and moved for summary judgment. The district court granted summary judgment to Facebook on all three claims. The district court awarded statutory damages of \$3,031,350, compensatory damages, and permanent injunctive relief, and it held that Vachani was personally liable for Power's actions. Discovery disputes persisted after the judgment; a magistrate judge ordered Power to pay \$39,796.73 in costs and fees for a renewed Federal Civil Procedure Rule 30(b)(6) deposition. Power filed a motion for reconsideration, which the district court denied. Defendants timely appeal both the judgment and the discovery sanctions.

STANDARD OF REVIEW

We review de novo a grant of summary judgment. *Johnson v. Poway Unified Sch. Dist.*, 658 F.3d 954, 960 (9th Cir. 2011). We may affirm the judgment on any ground supported by the record and presented to the district court. *Venetian Casino Resort L.L.C. v. Local Joint Exec. Bd.*, 257 F.3d 937, 941 (9th Cir. 2001).

9

DISCUSSION

A. CAN-SPAM Act

The CAN-SPAM Act grants a private right of action for a "provider of Internet access service adversely affected by a violation of section 7704(a)(1) of this title." 15 U.S.C. § 7706(g)(1). In relevant part, § 7704(a)(1) makes it unlawful for "any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading."

The CAN-SPAM Act "does not ban spam outright, but rather provides a code of conduct to regulate commercial email messaging practices." *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1047–48 (9th Cir. 2009). To prove a violation of the statute, Facebook cannot simply identify excessive electronic messages. Rather, assuming all facts in favor of the non-moving party, the offending messages must be "materially false" or "materially misleading." 15 U.S.C. § 7704(a)(1).

The statute provides that

the term "materially," when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to

10

identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

Id. § 7704(a)(6). A "from" line "that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading." *Id.* § 7704(a)(1)(B). And, further, "header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading." *Id.* § 7704(a)(1)(A).

Here, two types of messages might rise to the level of "materially misleading" under the CAN-SPAM Act: external e-mails sent when Power caused a Facebook event to be created and internal Facebook messages authored by Power that Power users transmitted to their Facebook friends.

We first consider the external e-mails. Facebook generated these e-mails whenever a Power user created a Facebook event, promoting Power. The "from" line of the e-mails identified "Facebook" as the sender. The body was signed "Thanks, The Facebook Team." The header stated that a friend of the recipient invited her to an event entitled "Bring 100 friends and win 100 bucks!"

Because the statute provides that a "from" line that accurately identifies a person who initiated the message is not misleading, it is relevant whether Facebook, identified in the

11

The statute defines from line, initiated the messages. "initiate" as "to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message." Id. § 7702(9). It provides that "more than one person may be considered to have initiated a message." A Power user gave Power permission to share a Id. promotion, Power then accessed that user's Facebook data, and Facebook crafted and caused form e-mails to be sent to recipients. These actions all go beyond the routine conveyance of a message. All the actions require some affirmative consent (clicking the "Yes, I do!" button) or some creative license (designing the form e-mails). Because more than one person may be considered to have initiated the message, we hold that, within the meaning of the statute, Power's users, Power, and Facebook all initiated the messages at issue.

Because Facebook (among others) initiated the messages, the "from" line accurately identified a person who initiated the messages. Accordingly, the "from" line is not misleading within the meaning of the statute. Similar reasoning also leads us to conclude that the header is technically accurate. Because a Power user consented to share Power's promotion through an event invitation, a header line that stated that a recipient's friend "invited" the recipient to the event does not conceal or misstate a creator of the e-mail.

It is true that the CAN-SPAM Act includes as materially misleading a technically accurate header that includes information accessed through false or fraudulent pretenses or representations. *Id.* § 7704(a)(1)(A). But Power users consented to Power's access to their Facebook data. In clicking "Yes, I do!," users gave Power permission to share

its promotion through event invitations. On this record, Power did not use false pretenses or fraudulent representations to obtain users' consent. Therefore, the external messages were not materially misleading within the meaning of the CAN-SPAM Act.

We next consider internal messages sent within the Facebook system. We can find these messages misleading only if they impaired the ability of the recipient to "respond to a person who initiated the electronic mail message" or the ability of Facebook to locate the initiator of the messages. *Id.* § 7704(a)(6). Two factors convince us that the messages are not misleading under this standard. First, the body of the messages included both Power's name and a link to the Power website. A reasonable recipient could understand that Power had drafted the message or had some part in its construction. Second, Facebook users who were identified as the senders did authorize the sending of these messages. It was not misleading for such users to be identified in internal messages sent through the Facebook system.

Because neither e-mails nor internal messages sent through Power's promotional campaign were materially misleading, Power did not violate the CAN-SPAM Act. We reverse the district court on this claim and remand for entry of judgment in favor of Defendants.

B. CFAA

12

The CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use. It creates criminal and civil liability for whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . .

information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). "The statute thus provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio v. United States*, 136 S. Ct. 709, 713 (2016). The CFAA provides a private right of action for "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g).

First, we hold that Facebook suffered a loss within the meaning of the CFAA. The statute permits a private right of action when a party has suffered a loss of at least \$5,000 during a one-year period. *Id.* § 1030(c)(4)(A)(i)(I). The statute defines "loss" to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). It is undisputed that Facebook employees spent many hours, totaling more than \$5,000 in costs, analyzing, investigating, and responding to Power's actions. Accordingly, Facebook suffered a loss under the CFAA.

We next consider whether Power accessed Facebook's computers knowing that it was not authorized to do so. We have previously considered whether a defendant has accessed a computer "without authorization" or in a manner that "exceeds authorized access" under the CFAA in three separate opinions.

Most recently, in United States v. Nosal, No. 14-10037, slip op. at 1 (9th Cir. July 5, 2016) ("Nosal II"), we considered the definition of "without authorization." In that case, an employee, David Nosal, had worked at an executive search firm, Korn/Ferry, until he decided to leave and start his own competing business. Id. at 8. Though Korn/Ferry explicitly revoked Nosal's computer access credentials, Nosal enlisted the support of his former executive assistant, who remained authorized to access the company computers. He used her password to continue accessing company computers and privileged information. Id. at 9-10. After Nosal was prosecuted and convicted under the CFAA, on appeal, we were "asked to decide whether the 'without authorization' prohibition of the CFAA extends to a former employee whose computer access credentials have been rescinded but who, disregarding the revocation, accesses the computer by other means." Id. at 6. We concluded that it did. We held that

> "without authorization" is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission. This definition has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party.

Id. at 4.

14

The holding in *Nosal II* clarified our two earlier cases on the CFAA. In *LVRC Holdings LCC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), an employee logged onto his employer's

15

computer, accessed confidential information, and sent e-mails from the computer to himself and his wife with the intention of starting a competing business. We held that a person is "without authorization" under the CFAA "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." Id. at 1135. Because the employee had sent e-mails while he still had authorized access to the company's computers, his actions did not constitute unauthorized use and did not run afoul of the CFAA. Id. That fact was key; had the employee accessed company computers without express permission, he would have violated the CFAA. "[I]f [the employee had] accessed LVRC's information on the LOAD website after he left the company in September 2003, [the employee] would have accessed a protected computer 'without authorization' for purposes of the CFAA." Id. at 1136.

In United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc) ("Nosal I"), an earlier case stemming from the same events that led to Nosal II, we considered whether a group of employees who logged on to a work computer, downloaded information from a confidential database, and transferred it to a competing business "exceed[ed] authorized access." *Id.* at 856. Wary of creating a sweeping Internet-policy mandate, we applied the rule of lenity to the CFAA and reversed liability for the defendant. *Id.* at 863. The decision broadly described the application of the CFAA to websites' terms of service. "Not only are the terms of service vague and generally unknown . . . but website owners retain the right to change the terms at any time and without notice." *Id.* at 862. As a result, imposing criminal liability for violations of the

16

terms of use of a website could criminalize many daily activities. Accordingly, "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly." *Id.* at 863.

From those cases, we distill two general rules in analyzing authorization under the CFAA. First, a defendant 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. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. Second, a violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA.

Here, initially, Power users arguably gave Power permission to use Facebook's computers to disseminate messages. Power reasonably could have thought that consent from *Facebook users* to share the promotion was permission for Power to access *Facebook's* computers.¹ In clicking the "Yes, I do!" button, Power users took action akin to allowing a friend to use a computer or to log on to an e-mail account. Because Power had at least arguable permission to access Facebook's computers, it did not initially access Facebook's result.

¹ Because, initially, Power users gave Power permission to use Facebook's computers to disseminate messages, we need not decide whether websites such as Facebook are presumptively open to all comers, unless and until permission is revoked expressly. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1163 (2016) (asserting that "websites are the cyber-equivalent of an open public square in the physical world").

computers "without authorization" within the meaning of the CFAA.

But Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power on December 1, 2008. Facebook's cease and desist letter informed Power that it had violated Facebook's terms of use and demanded that Power stop soliciting Facebook users' information, using Facebook content, or otherwise interacting with Facebook through automated scripts.² Facebook then imposed IP blocks in an effort to prevent Power's continued access.

The record shows unequivocally that Power knew that it no longer had authorization to access Facebook's computers, but continued to do so anyway. In requests for admission propounded during the course of this litigation, Power admitted that, after receiving notice that its use of or access to Facebook was forbidden by Facebook, it "took, copied, or made use of data from the Facebook website *without Facebook's permission* to do so." (Emphasis added; capitalization omitted.) Contemporaneously, too, soon after receiving the cease and desist letter, Power's CEO sent an email stating: "[W]e need to be prepared for Facebook to try to block us and the [sic] turn this into a national battle that gets us huge attention." On December 4, 2008, a Power executive sent an e-mail agreeing that Power engaged in four

² The mention of the terms of use in the cease and desist letter is not dispositive. Violation of Facebook's terms of use, without more, would not be sufficient to impose liability. *Nosal I*, 676 F.3d at 862–63. But, in addition to asserting a violation of Facebook's terms of use, the cease and desist letter warned Power that it may have violated federal and state law and plainly put Power on notice that it was no longer authorized to access Facebook's computers.

18

"prohibited activities"³; acknowledging that Power may have "intentionally and without authorization interfered with [Facebook's] possessory interest in the computer system," while arguing that the "*unauthorized use*" did not cause damage to Facebook; and noting additional federal and state statutes that Power "may also be accused of violating," beyond those listed in Facebook's cease and desist letter. Emails sent later in December 2008 discussed the IP blocks that Facebook had imposed and the measures that Power took to evade them. Nevertheless, Power continued to access Facebook's data and computers without Facebook's permission.

The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission. An analogy from the physical world may help to illustrate why this is so. Suppose that a person wants to borrow a friend's jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank's property while armed. In other words, to access the safe deposit box, the person needs permission both from his friend (who controls access to the safe) and from the bank

³ The activities were: "- Using a person's Facebook account without Facebook's authorization; - Using automated scripts to collect information from their site; - Incorporating Facebook's site in another database[; and] - Using Facebook's site for commercial purposes[.]"

(which controls access to its premises). Similarly, for Power to continue its campaign using Facebook's computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers). Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter.

In sum, as it admitted, Power deliberately disregarded the cease and desist letter and accessed Facebook's computers without authorization to do so. It circumvented IP barriers that further demonstrated that Facebook had rescinded permission for Power to access Facebook's computers.⁴ We therefore hold that, after receiving written notification from Facebook on December 1, 2008, Power accessed Facebook's computers "without authorization" within the meaning of the CFAA and is liable under that statute.

Nosal I is materially distinguishable. First, *Nosal I* involved employees of a company who arguably exceeded the limits of their authorization. 676 F.3d at 856. Here, by contrast, Facebook explicitly revoked authorization for *any* access, and this case does not present the more nuanced question of exceeding authorization. *Nosal I* involved a defendant who "exceeded authorization," while this case involves a defendant who accessed a computer "without

⁴ Simply bypassing an IP address, without more, would not constitute unauthorized use. Because a blocked user does not receive notice that he has been blocked, he may never realize that the block was imposed and that authorization was revoked. Or, even if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user's roommate or co-worker.

authorization." Second, although Nosal I makes clear that violation of the terms of use of a website cannot itself constitute access without authorization, this case does not involve non-compliance with terms and conditions of service. Facebook and Power had no direct relationship, and it does not appear that Power was subject to any contractual terms that it could have breached. Finally, Nosal I was most concerned with transforming "otherwise innocuous behavior into federal crimes simply because a computer is involved." Id. at 860. It aimed to prevent criminal liability for computer users who might be unaware that they were committing a crime. But, in this case, Facebook clearly notified Power of the revocation of access, and Power intentionally refused to comply. Nosal I's concerns about overreaching or an absence of culpable intent simply do not apply here. 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.

Accordingly, we hold that, after receiving the cease and desist letter from Facebook, Power intentionally accessed Facebook's computers knowing that it was not authorized to do so, making Power liable under the CFAA. We therefore affirm in part the holding of the district court with respect to the CFAA.

C. Section 502

20

California Penal Code section 502 imposes liability on a person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing

internal or external to a computer, computer system, or computer network." *Id.* § 502(c)(2). This statute, we have held, is "different" than the CFAA. *United States v. Christensen*, 801 F.3d 970, 994 (2015). "[T]he California statute does not require *unauthorized* access. It merely requires *knowing* access." *Id.*

But despite differences in wording, the analysis under both statutes is similar in the present case. Because Power had implied authorization to access Facebook's computers, it did not, at first, violate the statute. But when Facebook sent the cease and desist letter, Power, as it conceded, knew that it no longer had permission to access Facebook's computers at all. Power, therefore, knowingly accessed and without permission took, copied, and made use of Facebook's data. Accordingly, we affirm in part the district court's holding that Power violated section 502.

D. Personal Liability

We affirm the district court's holding that Vachani is personally liable for Power's actions. A "corporate officer or director is, in general, personally liable for all torts which he authorizes or directs or in which he participates, notwithstanding that he acted as an agent of the corporation and not on his own behalf." *Comm. for Idaho's High Desert, Inc. v. Yost*, 92 F.3d 814, 823 (9th Cir. 1996) (internal quotation marks omitted). Cases finding "personal liability on the part of corporate officers have typically involved instances where the defendant was the 'guiding spirit' behind the wrongful conduct, or the 'central figure' in the challenged corporate activity." *Davis v. Metro Prods., Inc.*, 885 F.2d 515, 523 n.10 (9th Cir. 1989) (internal quotation marks and ellipsis omitted).

Vachani was the central figure in Power's promotional scheme. First, Vachani admitted that, during the promotion, he controlled and directed Power's actions. Second, Vachani admitted that the promotion was his idea. It is undisputed, therefore, that Vachani was the guiding spirit and central figure in Power's challenged actions. Accordingly, we affirm the district court's holding on Vachani's personal liability for Power's actions.

E. Discovery Sanctions

22

We affirm the discovery sanctions imposed against Power for non-compliance during a Rule 30(b)(6) deposition. Defendants failed to object to discovery sanctions in the district court. Failure to object forfeits Defendants' right to raise the issue on appeal. *Simpson v. Lear Astronics Corp.*, 77 F.3d 1170, 1174 (9th Cir. 1996).

Even assuming the issue was not waived, we "review the district court's rulings concerning discovery, including the imposition of discovery sanctions, for abuse of discretion." *Goodman v. Staples Office Superstore, LLC*, 644 F.3d 817, 822 (9th Cir. 2011). The magistrate judge's findings that Vachani was unprepared, unresponsive, and argumentative and that Power Ventures had failed to produce many e-mails responsive to Facebook's requests prior to discovery are supported by the record. Accordingly, we hold that the discovery sanctions imposed were not an abuse of discretion.

F. Remedies

Because we reverse in significant part, we also vacate the injunction and the award of damages. We remand the case to the district court to reconsider appropriate remedies under the

CFAA and section 502, including any injunctive relief. With respect to damages, the district court shall calculate damages only for the period after Power received the cease and desist letter, when Power continued to access data contained in Facebook's servers and memory banks.

REVERSED in part, **VACATED** in part, **AFFIRMED** in part, and **REMANDED**. The parties shall bear their own costs on appeal.