2016 WL 3741956
United States Court of Appeals,
Ninth Circuit.

Facebook, Inc., a Delaware corporation, Plaintiff–Appellee,
v.
Power Ventures, Inc., dba Power.com, a California corporation; Power Ventures, Inc., a Cayman Island corporation, Defendants,
and
Steven Suraj Vachani, an individual, Defendant–Appellant.
Facebook, Inc., a Delaware corporation, Plaintiff–Appellee,
v.
Power Ventures, Inc., dba Power.com, a California corporation, Defendant,
and
Power Ventures, Inc., a Cayman Island corporation; and Steven Suraj Vachani, an individual, Defendants Appellants.

No. 13-17102, No. 13-17154
|
Argued and Submitted December 9, 2015
|
Filed July 12, 2016

Synopsis

Background: Plaintiff social networking website brought action against defendant social networking website and its chief executive officer (CEO), alleging defendant website and CEO violated Controlling the Assault of Non–Solicited Pornography and Marketing Act (CAN–SPAM), Computer Fraud and Abuse Act (CFAA), and California law by unlawfully accessing plaintiff website to send unsolicited and misleading commercial e-mails to its users. The United States District Court for the Northern District of California, James Ware, Chief Judge, 844 F.Supp.2d 1025, entered summary judgment for plaintiff website. Defendant website and CEO appealed.

Holdings: The Court of Appeals, Graber, Circuit Judge, held that:

[1] actions of defendant website and CEO were not "materially misleading" under CAN–SPAM Act;

[2] plaintiff website suffered losses of more than $5,000 in costs, as required to bring claim alleging violation of CFAA;

[3] defendant website accessed plaintiff website's computers "without authorization" after plaintiff website issued it a written cease and desist letter, as required for liability under CFAA and California law; and

[4] CEO was personally liable for defendant website's violations of CFAA and California statute.

Ordered accordingly.

West Headnotes (16)

[1] Federal Courts
Theory and Grounds of Decision of Lower Court

Federal Courts
Summary judgment

The Court of Appeals reviews de novo a grant of summary judgment, and may affirm the judgment on any ground supported by the record and presented to the district court. Fed. R. Civ. P. 56.

Cases that cite this headnote

[2] Telecommunications
Unsolicited e-mail

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN–SPAM Act) does not ban "spam" messages outright, but rather, provides a code of conduct to regulate commercial e-mail messaging practices. 15 U.S.C.A. §§ 7704(a)(1), 7706(g)(1).

Cases that cite this headnote

[3] Telecommunications

Unsolicited e-mail

Header information in e-mails sent when defendant social networking website caused an "event" to be created on plaintiff's social networking website, promoting defendant website, was not "materially misleading" under Controlling the Assault of Non–Solicited Pornography and Marketing Act (CAN–SPAM); a user of defendant website gave defendant website permission to share a promotion, defendant website then accessed that user's data from plaintiff website, plaintiff website crafted and caused form e-mails to be sent to recipients, and, as a result, both websites and their users initiated the messages at issue. 15 U.S.C.A. §§ 7704(a)(1), 7704(a)(6).

Cases that cite this headnote

[4] Telecommunications

Unsolicited e-mail

Messages authored by defendant social networking website, which users of such website transmitted to their "friends" on plaintiff social networking website, were not "materially misleading" under Controlling the Assault of Non–Solicited Pornography and Marketing Act (CAN–SPAM); body of messages included defendant website's name and link to its website, such that reasonable recipient could understand that defendant website had drafted the message or had some part in its construction, and users of plaintiff website who were identified as senders authorized sending of the messages. 15 U.S.C.A. §§ 7704(a)(1), 7704(a)(6).

Cases that cite this headnote

[5] Telecommunications

Offenses and Prosecutions

The Computer Fraud and Abuse Act (CFAA) 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. 18 U.S.C.A. §§ 1030(a)(2)(C), 1030(g).

1 Cases that cite this headnote

[6] Telecommunications

Fraud;unauthorized access or transmission

Plaintiff social networking website suffered losses of more than $5,000 in costs analyzing, investigating and responding to unsolicited and misleading commercial e-mails defendant social networking website caused to be sent to users of plaintiff website, as required for plaintiff website to bring claim against defendant website alleging violation of Computer Fraud and Abuse Act (CFAA). 18 U.S.C.A. § 1030(c)(4)(A)(i)(I), (e)(11), (g).

Cases that cite this headnote

[7] Telecommunications

Fraud;unauthorized access or transmission

A defendant can run afoul of the Computer Fraud and Abuse Act (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. 18 U.S.C.A. §§ 1030(a)(2)(C), 1030(g).

2 Cases that cite this headnote

[8] Telecommunications

Fraud;unauthorized access or transmission

A violation of the terms of use of a website —without more—cannot be the basis for liability under the Computer Fraud and Abuse Act (CFAA). 18 U.S.C.A. §§ 1030(a)(2)(C), 1030(g).

1 Cases that cite this headnote

[9] Telecommunications

Fraud;unauthorized access or transmission

Although defendant social networking website did not initially access computers of plaintiff social networking website "without authorization" within meaning of Computer Fraud and Abuse Act (CFAA), it did access plaintiff website's computers "without authorization" after plaintiff website issued it a written cease and desist letter, as required for liability under CFAA; defendant website had at least arguable permission from plaintiff website's users, but permission was rescinded after issuance of letter, plaintiff website then imposed internet protocol (IP) blocks in effort to prevent defendant website's continued access, and defendant website knew it no longer had authorization to access plaintiff website's computers but continued to do so. 18 U.S.C.A. § 1030(c)(4)(A)(i)(l), (e)(11), (g).

1 Cases that cite this headnote

[10] Telecommunications
Offenses and Prosecutions

California statute prohibiting knowing access and unauthorized taking, copying, or making use of any data from computer, computer system, or computer network does not require unauthorized access, but merely requires knowing access. Cal. Penal Code § 502.

Cases that cite this headnote

[11] Telecommunications
Fraud;unauthorized access or transmission

Although defendant social networking website did not initially access computers of plaintiff social networking website "without permission" within meaning of California statute prohibiting knowing access and unauthorized taking, copying, or making use of any data from computer, computer system, or computer network, it did access plaintiff website's computers "without permission," in violation of California statute, after plaintiff website issued it a written cease and desist letter; defendant website had at least arguable permission from plaintiff website's users, but permission was rescinded after issuance of letter, plaintiff website then imposed internet protocol (IP) blocks in effort to prevent defendant website's continued access, and defendant website knew it no longer had authorization to access plaintiff website's computers but continued to do so. Cal. Penal Code § 502.

1 Cases that cite this headnote

[12] Corporations and Business Organizations
Tortious acts in general

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; such cases typically involve instances where officer or director was "guiding spirit" behind wrongful conduct, or "central figure" in challenged corporate activity.

Cases that cite this headnote

[13] Corporations and Business Organizations
Tortious acts in general

Corporations and Business Organizations
Fraud

Chief executive officer (CEO) of defendant social networking website was personally liable for defendant website's violations of Computer Fraud and Abuse Act (CFAA) and California statute prohibiting knowing access and unauthorized taking, copying, or making use of any data from computer, computer system, or computer network, caused by unlawfully accessing plaintiff social networking website to send unsolicited and misleading commercial e-mails to users of plaintiff website; CEO admitted that he controlled and directed defendant website's actions, and he admitted scheme was his idea. 18 U.S.C.A. § 1030; Cal. Penal Code § 502.

Cases that cite this headnote

[14] Federal Courts
Preliminary proceedings;depositions and discovery

A defendant's failure to object to discovery sanctions in district court forfeits the defendant's right to raise the issue on appeal.

Cases that cite this headnote

[15] Federal Civil Procedure
Failure to Appear or Testify;Sanctions

In action brought by plaintiff social networking website against defendant social networking website and its chief executive officer (CEO), alleging defendant website and CEO violated Controlling the Assault of Non–Solicited Pornography and Marketing Act (CAN–SPAM), Computer Fraud and Abuse Act (CFAA), and California law by unlawfully accessing its website to send unsolicited and misleading commercial e-mails to users of plaintiff website, District Court did not abuse its discretion by imposing discovery sanctions against defendant website for non-compliance during its deposition; CEO was unprepared, unresponsive and argumentative, and defendant website failed to produce many e-mails responsive to plaintiff website's requests prior to discovery. 15 U.S.C.A. §§ 7704(a)(1), 7706(g)(1); 18 U.S.C.A. § 1030; Cal. Penal Code § 502.

Cases that cite this headnote

[16] Federal Courts
Discovery sanctions

The Court of Appeals reviews a district court's rulings concerning discovery, including the imposition of discovery sanctions, for abuse of discretion.

Cases that cite this headnote

Appeals from the United States District Court for the Northern District of California, Lucy H. Koh, District Judge, Presiding. D.C. No. 5:08–cv–05780–LHK

Attorneys and Law Firms

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.

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

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 e-mails 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

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

***3** 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

[1] 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).

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."

[2] The CAN–SPAM Act "does not ban spam outright, but rather provides a code of conduct to regulate commercial e-mail 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 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).

***4** 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.

[3] 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 from line, initiated the messages. The statute defines "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." *Id.* A Power user gave Power permission to share a 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.

[4] 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.

***5** 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*

[5] 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*, —— U.S. ——, 136 S.Ct. 709, 713, 193 L.Ed.2d 639 (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).

[6] 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*, —— F.3d ——, ——, 2016 WL 3608752 (9th Cir.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 ——.

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 —— – ——. 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 ——. 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.

***6** *Id.* at ——.

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 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 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.

[7] **[8]** 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.

[9] 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 computers "without authorization" within the meaning of the CFAA.

***7** 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 e-mail 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 "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. E-mails 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 (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.

***8** 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 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*

[10] 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.*

[11] 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*

***9** **[12]** 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).

[13] 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*

[14] 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).

[15] **[16]** 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.

All Citations

--- F.3d ----, 2016 WL 3741956, 16 Cal. Daily Op. Serv. 7428, 2016 Daily Journal D.A.R. 7051

Footnotes

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").

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.

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[.]"

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.