Ninth Circuit Says You're Going to Jail for Visiting That Website without Permission

David Smyth
July 28, 2016

Zounds, right? But that is arguably what the U.S. Court of Appeals for the Ninth Circuit said about the Computer Fraud and Abuse Act in *Facebook v. Power Ventures, Inc.* on July 12th. Let's get to it.

Facts

Power Ventures and its CEO Steven Vachani operated a social network called Power.com. The concept was simple. People using other social networking sites could create a Power account to aggregate the user's social networking information. The users could keep track of a variety of social networking friends through a single program and click through the central Power website to individual sites. By 2008, the website had attracted a growing following. Maybe it was even a good idea! I don't know.

Facebook also runs a social networking website. You may have heard of it. Facebook requires each user to register and assent to its terms of use. Registered users can then create and customize profiles by adding photos, funny GIFs, completely engrossing and persuasive political rants, etc. A user can establish connections with other Facebook users and make them "friends." Some of those are real friends; others are your racist uncles.

Non-Facebook users may not use the site to send messages, post photographs, or otherwise contact Facebook users through their profiles. Instead, Facebook requires third-party developers or websites that want 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 Dec. 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 site 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. If a user clicked the "Yes, I do!" button on the icon, Power would create an event, photo, or status on the user's Facebook profile.

In many instances in this campaign, Power caused messages to be transmitted to the user's friends within the Facebook system. At other times, 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 said the Power user was

BLOG ARCHIVE

TOPICS

About This Blog
Access to Court Dockets
Access to Courtrooms
Access to Search Warrants
Anti-SLAPP Statutes
Contact
Cyberattack
Data Breach
Data Security
Defamation
Digital Media and Data Privacy Law
Disclaimer
Drone Law
Fair Report Privilege
FCC Matters
First Amendment
First Amendment Retaliation
FOIA
HIPAA
Indecency
Internet
Intrusion
Miscellaneous
Mobile Privacy
Newsroom Search Warrants
Newsroom Subpoenas
Political Advertising
Prior Restraints
Privacy
Privacy Policies
Public Records

inviting the recipient to this event. The external e-mails were form e-mails, generated each time 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."

As it turns out, Facebook did not like this! On Dec. 1, 2008, Facebook first learned of Power's campaign and sent a cease-and-desist letter 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 installed an Internet Protocol ("IP") block to prevent Power from accessing the Facebook website. Power circumvented the Facebook block by switching IP addresses. Through this period, Power continued its promotion and acknowledged that it took, copied, or made use of data from Facebook.com without Facebook's permission.

On Dec. 20, 2008, Facebook sued under the Computer Fraud and Abuse Act, among other causes of actions, and toward the end of Jan. 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.

The CFAA in the Ninth Circuit

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 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).

More critically, did Power access Facebook's computers knowing it wasn't authorized to do so? In a very recent case discussed here (*Nosal II*), a Ninth Circuit panel was "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." The court said yes, and held that "without authorization" is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." Also, "[t]his 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."

Several years ago in another case (see here: *Nosal I*), the full Ninth Circuit 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." Wary of creating a sweeping Internet-policy mandate, the court applied the rule of lenity to the CFAA and reversed liability for the defendant. The decision broadly described the application of the CFAA to websites' terms of service. Because those terms of service are often vague and generally unknown, website owners frequently can change the terms at any time and without notice. So imposing criminal liability for violations of the terms of use of a website could criminalize many daily activities, and the court didn't do so in *Nosal I*.

But the Ninth Circuit did distill two general rules in analyzing authorization under the CFAA. First, a defendant can violate the CFAA when he has no permission to access a computer or when that permission has been explicitly revoked. Second, violating a website's terms of use – without more – cannot be the basis for liability under the CFAA.

Discussion

Here, initially, Power users arguably gave Power permission to use Facebook's computers to disseminate messages. Power could reasonably have thought that consent from Facebook users to share the promotion was permission for

Reporters Privilege
Services
Shield Laws
Wiretapping

LINKS

International Association of Privacy Professionals
National Association of Broadcasters
North Carolina Cable Telecommunications Association
North Carolina Press Association
North Carolina Association of Broadcasters
Radio-Television News Directors Association of the Carolinas
Media Law Resource Center
The Reporters Committee for Freedom of the Press
Society of Professional Journalists
The Journalist's Toolbox - American Press Institute
Law Blog - WSJ.com
Legal Blog Watch
North Carolina Business Litigation Report

Power to access Facebook's computers. But Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power on Dec. 1, 2008.

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." It circumvented IP barriers that further demonstrated that Facebook had rescinded permission for Power to access Facebook's computers.

Was *Nosal I* distinguishable? In that case, remember, the court reversed a conviction when the indictment merely charged violations of Korn-Ferry's general policies. The court said Power was in a different bucket for three reasons. First, *Nosal I* involved employees of a company who arguably exceeded the limits of their authorization. Here, by contrast, Facebook explicitly revoked authorization for *any* access, and this case does not present the more nuanced question of exceeding authorization. Second, though *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 it could have breached. Finally, the court said, *Nosal I* was most concerned with transforming "otherwise innocuous behavior into federal crimes simply because a computer is involved." It aimed to prevent criminal liability for computer users who might be unaware they were committing crimes. But Facebook clearly notified Power of the revocation of access, and Power intentionally refused to comply. The court closed by saying "*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."

Is that right?

Um, not everybody thinks so! Here's what Orin Kerr, who knows a lot more about computer crime than you or me, says:

> This is an important case. This was a civil dispute, but the CFAA is also criminal statute. If read broadly, the case seems to say that if you want to make it a crime for someone to visit your website, you just need to give them notice that you don't want them to visit. I gather that as long as you phrase the notice as a command to cease and desist, rather than as just general terms of use, it becomes legally binding.

The implications could be staggering. It seems entirely possible that the Ninth Circuit could grant a petition for rehearing *en banc*. We'll see.