

Three Steps That Allow Companies to Use the Computer Fraud and Abuse Act for Misuse of Computers and Information – Even in the Ninth Circuit

Key Takeaway: Companies that follow these 3 steps can use the Computer Fraud and Abuse Act as a tool to combat the misuse of their computers (and information) by (1) actively monitoring for misuses, (2) taking reasonable steps to actively resist and prevent such misuses, and (3) clearly and conspicuously notifying the transgressor that his authorization has been terminated.

In the last couple of years the Ninth Circuit has done more work than any other circuit on refining its “narrow” or “access means access” approach to determining whether an access “exceeds authorized access” or is “without authorization” for purposes of the [Computer Fraud and Abuse Act](#). The district courts in the Ninth Circuit are now taking those principles and applying them at the trial court level. Over the last few weeks we have seen two of those cases that, when compared to each other, do a really nice job of plotting the points for how this “narrow” approach really works.

The cases are [Craigslist Inc. v. 3Taps Inc.](#), 2013 WL 447520 (ND Ca. Aug. 16, 2013) and [Spam Arrest, LLC v. Replacements, Ltd.](#), 2013 WL 4675919 (W.D. Wa. Aug. 29, 2013). A brief summary of both cases can be found on the [CFAA digest](#) (my latest project). Here are the key points:

Access. The plaintiffs in both cases provided unrestricted access to their computers. Craigslist provided a website that was accessible to anyone in the world; Spam Arrest provided an email server that was accessible to anyone in the world who wanted to send emails to its customers.

Contractual Use Restrictions. The plaintiffs in both cases had contractual use restrictions that prohibited the defendants from doing what they ultimately did with the computers. Craigslist’s has a Terms of Use that prohibits the collection of data from its site; Spam Arrest’s agreement required the defendant to promise not to use the computer to send spam.

Prohibited Use. The defendants in both cases used those computers for purposes that were prohibited by the contractual restrictions. In [Craigslist](#), the defendant used a program to scrape the plaintiff’s website and basically rip off all of its content; in [Spam Arrest](#), the defendant used the email server to send spam email to the plaintiff’s customers — the plaintiff sold anti-spam services and, quite understandably so, was not pleased.

Ninth Circuit Law. “[T]he phrase ‘exceeds authorized access’ in the CFAA does not extend to violations of use restrictions. . . . Therefore, we hold that ‘exceeds authorized access’ in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use.” *United States v.*

Nosal (Nosal II), 676 F.3d 854, 863 (9th Cir. 2012).

Same Outcome? At this point, it seems like both cases should have the same outcome, correct? Yes, they should, based on the information I have provided so far — based on this information it sounds like both plaintiffs’ claims under the Computer Fraud and Abuse Act should fail. The there is more ...

Active Resistance. Spam Alert simply sat back and relied on its contractual use restrictions as its only efforts to prevent the misuse of its computer; Craigslist did more. After learning about 3 Taps’ activities, Craigslist took two important steps:

(1) it sent a cease-and-desist letter to 3Taps informing it that “[t]his letter notifies you that you and your agents, employees, affiliates, and/or anyone acting on your behalf are no longer authorized to access, and/or prohibited from accessing Craigslist’s website or services for any reason”;

(2) Craigslist configured its website to block access from IP addresses associated with 3Taps.

Because Craigslist took these steps to actively resist the misuse of its website, the court framed the issue as whether a plaintiff, who had made its website publicly available and authorized the world to access it, could revoke that permission on a case-by-case basis through its cease-and-desist letter and IP blocking measures. **The court held that “authorization” turns on the decision of the “authority” that grants or prohibits access and Craigslist, as owner of the website, rescinded that permission for 3Taps; further access by 3Taps after that rescission was “without authorization.”**

What these two cases show is that, even in the Ninth Circuit (and Fourth), a company can use the Computer Fraud and Abuse Act as a tool to combat the misuse of its computers, and the information available thereon, if it actively monitors for such misuses and, upon discovering them, takes reasonable steps to actively resist and prevent such misuses by terminating the transgressor’s ability to access the computers and clearly and conspicuously notifying him that such authorization has been terminated.

If you would like to discuss how your company can be better prepared to take advantage of the remedies available through the Computer Fraud and Abuse Act please feel free to give me a call (469.635.1335) or email me (stuma@brittontuma.com).

–Shawn Tuma