LOS ANGELES
Daily Journal
www.dailyjournal.com
MONDAY, OCTOBER 5, 2015

PERSPECTIVE

Scope of computer crime law upturned

By Jonathan H. Blavin

In *United States v. Christensen*, 08-50531 (Aug. 25, 2015), the 9th U.S. Circuit Court of Appeals upturned what was previously seen as established precedent regarding the contours of California computer crime law. By holding that California's Comprehensive Computer Data Access and Fraud Act (Penal Code Section 502(c)) does not require a showing of unauthorized "access" into a computer system, via the circumvention of technological barriers or otherwise, but simply the unauthorized "taking" or "use" of data, the 9th Circuit drew a sharp distinction between the boundaries of Section 502(c) and its federal corollary, the Computer Fraud and Abuse Act. The decision significantly expands the scope of California computer crime law and portends a new wave of Section 502(c) criminal and civil litigation.

The federal CFAA provides, as an element of the offense, that a defendant have "knowingly ... access[ed] a protected computer without authorization or exceeding authorized access." 18 U.S.C. Section 1030(a)(4). In *United States v. Nosal*, 676 F.3d 854, 859 (2012), the 9th Circuit expressed concerned that interpreting the "without authorization" or "exceeding authorized access" language to mean in violation of computer use, as opposed to access, restrictions would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." As the court humorously noted, "[m]inds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes." The court discussed a litany of examples of use restriction violations that could be federal crimes under this interpretation of the CFAA, such as a minor using a website that "forbade minors from using its services," letting someone else log into your Facebook account, or "describing yourself" on a dating website as 'tall, dark and handsome,' when you're actually short and homely."

Following *Nosal*, district courts in the 9th Circuit have dismissed CFAA claims on the basis that the plaintiffs have only alleged the unauthorized "use" of a computer system or data, and not unauthorized "access" to a system. See *Incorp Servs. Inc. v. Incsmart.Biz Inc.*, 11-4660 (N.D. Cal. Aug. 24, 2012) (dismissing CFAA claim where there are "no direct or clear allegations of 'hacking' ... being, broadly, 'the circumvention of technological access barriers,' not violation of 'use restrictions'"). Courts have indicated, though, that allegations of technological "hacking" may not be necessary, and simply unauthorized "access" will suffice. See *Loop AI Labs Inc v. Gatti*, 15-798 (N.D. Cal. Sept. 2, 2015) (though "*Nosal* did not limit the CFAA's application to instances of hacking — i.e., the circumvention of technological access barriers" it "is not a violation of the CFAA to access a computer with permission, but with the intent to use the information gained thereby in violation of a use agreement.").

Section 502(c)(2) subjects a defendant to liability who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." Prior to *Christensen*, several district courts within the 9th Circuit had interpreted the "without permission" language as requiring, similar to the CFAA, that a defendant gain unauthorized access to a computer network and specifically "in a manner that circumvents technical or code based barriers in place to restrict or bar a user's access." *In re Google Android Consumer Privacy Litig.*, 11-2264 (N.D. Cal. Mar. 26, 2013); see also *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012) (citing authorities and stating that "individuals may only be subjected to liability for acting 'without permission' under § 502 if they 'access[ ] or us[e] a computer, computer network, or website in a manner that overcomes technical or code-based barriers'"). Indeed, courts had even described the "requirements of both statutes" as "functionally identical." *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 968 (N.D. Cal. 2013); see also *Multiven Inc. v. Cisco Sys. Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) ("the necessary elements of § 502 do not differ materially from the necessary elements of the CFAA for purposes of this action").

In *Christensen*, however, the 9th Circuit upended this body of law. There, Anthony Pellicano and employees of his investigation firm were charged with multiple crimes relating to, amongst other acts, access to police and telephone company databases using valid passwords and credentials obtained by bribing law enforcement officials and telephone company employees. The court considered whether such acts could violate the CFAA and Section 502(c). As to the CFAA, the court vacated the defendants' convictions, as the jury instruction "contrary to *Nosal* ... allowed the jury to convict for unauthorized use of information rather than only for unauthorized *access*." But with respect to Section 502(c), the court held that "[i]n contrast to the CFAA," Section 502(c)(2) "does not require *unauthorized* access," and that a "plain reading of the statute demonstrates that its focus is on unauthorized taking or use of information." The court concluded that the "term 'access'" in Section 502(c)(2) "includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly," and that to hold otherwise, the "words 'without permission' would be redundant, since by definition hackers lack permission to access a database." The court held that there was sufficient evidence of defendants' underlying intent to violate Section 502(c)(2).

Relying exclusively upon the plain language of Section 502(c), *Christensen* did not engage in the searching policy analysis that animated *Nosal*'s interpretation of the CFAA. But apart from the philosophical question of whether those who lie about their looks on a dating profile should be subject to criminal or civil liability, the decision's import for litigators is clear: *Christensen* dramatically expands the scope of Section 502(c) liability and gives prosecutors and plaintiffs a powerful tool to challenge the unauthorized taking or use of data, even if that data was obtained through authorized access to a computer system.

Jonathan H. Blavin *is a partner at Munger, Tolles & Olson LLP. You can reach him at Jonathan.Blavin@mto.com.*

JONATHAN BLAVIN
Munger, Tolles & Olson