

Wentworth-Douglass v. Young & Novis 10-CV-120-SM 6/29/12
UNITED STATES DISTRICT COURT

DISTRICT OF NEW HAMPSHIRE

Wentworth-Douglass Hospital,
Plaintiff

v.

Case No. 10-cv-120-SM
Opinion No. 2012 DNH 112

Young & Novis Professional
Association d/b/a Piscataqua
Pathology Associates; Cheryl C.
Moore, M.D.; Glenn H. Littell,
M.D.; and Thomas Moore, M.D.,
Defendants

O R D E R

Defendants move the court to reconsider its earlier order denying the parties' cross-motions for summary judgment on plaintiff's claims under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"). See Order of March 30, 2012 (document no. 138). The motion is granted in part and denied in part. And, for the reasons discussed, judgment as a matter of law shall be entered in favor of defendants Cheryl Moore and Glenn Littell on count one of the hospital's amended complaint. In all other respects, defendants' motion for reconsideration is denied.

Background

That portion of the CFAA currently at issue provides as follows: "Whoever intentionally accesses a computer without

authorization or exceeds authorized access, and thereby obtains information from any protected computer" shall be exposed to both criminal penalties and civil liability. 18 U.S.C. § 1030(a)(2)(C) (emphasis supplied). See also 18 U.S.C. § 1030(g). In their motion for reconsideration, defendants ask the court to resolve a legal question previously identified, but not fully briefed: Whether violating an employer's computer use policy - as opposed to circumventing its computer access restrictions - gives rise to liability under that provision of the CFAA. Defendants urge a narrow construction of the statutory language that would impose liability only when one circumvents computer access restrictions.

Defendants' argument invokes the Ninth Circuit's recent en banc decision in United States v. Nosal, 676 F.3d 854 (9th Cir. 2012), in which the court held that, "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." Id. at 863. Rather, the court concluded that "the plain language of the CFAA targets the unauthorized procurement or alteration of information, not its misuse or misappropriation." Id. (citation and internal punctuation omitted). See also Orbit One Communications, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information.

It does not prohibit misuse or misappropriation. . . . [T]he statute as a whole indicates Congress's intent to prohibit access of a computer without authorization, not an employee's misuse of information that he or she was entitled to access or obtain.").

In other words, the Court of Appeals for the Ninth Circuit concluded that the CFAA does not address the situation in which someone "has unrestricted physical access to a computer, but is limited in the use to which he can put the information." Nosal, 676 F.3d at 857. And, one "exceeds authorized access" under the CFAA if he or she is "authorized to access only certain data or files but accesses unauthorized data or files - what is colloquially known as 'hacking.'" Id.¹

Defendants say they are entitled to summary judgment on the hospital's CFAA claims because they allege only a violation of the hospital's computer "use policy," rather than any circumvention of its computer "access restrictions." The hospital objects, arguing that Nosal was wrongly decided, is not binding precedent in this district, and is inconsistent with

¹ As an example, the court posited the situation in which an employee is authorized to access computer-based customer lists in order to perform his job, but he is prohibited from sharing that information with a competitor. While providing such information to a competing business might contravene the employer's policy, it would not expose the employee to either civil or criminal liability under the CFAA.

existing First Circuit precedent. Moreover, says the hospital, its CFAA claim in count one is based (at least in part) on alleged violations of "access restrictions," not simply "use restrictions."

Discussion

Initially, it is worth noting that defendants take the position that "In order to sustain a claim under the CFAA, [the hospital] must show that the Defendants exceeded their authorized access. . . . Each count fails because the Defendants were entitled to access all of the files copied, taken, and deleted." Defendants' Memorandum (document no. 139-1) at 4. That is not entirely correct. Count two of the amended complaint alleges that defendants violated 18 U.S.C. § 1030(a)(5)(A), by intentionally causing damage, without authorization, to a hospital computer. Contrary to defendants' suggestion, that count does not contain an "exceeds authorized access" element. See, e.g., Grant Mfg. & Alloying, Inc. v. McIlvain, 2011 WL 4467767, 8 (E.D.Pa. 2011) ("Unlike the other CFAA provisions [plaintiff] invokes, § 1030(a)(5)(A) does not require access of a protected computer without authorization or in excess of authorized access."); Farmers Bank & Trust, N.A. v. Witthuhn, 2011 WL 4857926, 6 (D.Kan. 2011) ("Unlike subsection (a)(5)(C), this section creates liability for knowingly causing transmission

of something that causes damage without authorization, as compared to damage that is the result of access without authorization."). And, count three of the amended complaint simply alleges that the three individually named defendants conspired to violate sections (a)(2) and (a)(5)(A). See 18 U.S.C. § 1030(b). Only count one of the amended complaint requires the hospital to prove that defendants accessed a hospital computer "without authorization" or that they "exceed[ed] authorized access." Accordingly, the court will restrict its analysis to that particular count.

Mirroring the language of the CFAA, count one of the amended complaint alleges that "Defendants intentionally accessed computers without authorization or exceeded authorized access, and thereby obtained information from a protected computer." Amended Complaint (document no. 68) at para. 82. But, in elaborating on that claim, the hospital says:

Count I [of the amended complaint] alleges the Defendants violated [18 U.S.C. § 1030(a)(2)(C)] because, without the prior authorization and approval of the WDH Information Systems Department and in violation of the IM-09, they connected removable storage devices or external hardware to hospital computers and obtained or altered information from WDH computers owned by WDH that they were not entitled to obtain or alter.

Plaintiff's Motion for Summary Judgment (document no. 81-1) at 13 (emphasis supplied). Additionally, the amended complaint alleges that Dr. Thomas Moore circumvented access restrictions on two hospital computers (known as "PY001" and the "HP Laptop") by using his wife's password to view, copy, and delete data he was not authorized to access. Amended Complaint at paras. 49, 58, and 60.

With respect to Dr. Cheryl Moore and Dr. Littell, the issue presented is whether they can be liable under section 1030(a)(2)(C) for having violated the hospital's computer use policy when they allegedly connected removable storage devices to hospital computers and then downloaded and/or copied data that they were otherwise authorized to access. In support of its view that such violations of an employer's computer use restrictions can give rise to liability under the CFAA, the hospital cites two opinions from the Court of Appeals for the First Circuit: EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) ("EF Cultural I") and EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003) ("EF Cultural II").

To be sure, dicta in the EF Cultural opinions can be read to support the hospital's expansive view of the CFAA's reach. But

the holdings in those cases are more narrow than the hospital suggests. As then Chief Judge Boudin explained:

The panel [in EF Cultural I] held that the use of the scraper tool exceeded the defendants' authorized access to EF's website because (according to the district court's findings for the preliminary injunction) access was facilitated by use of confidential information obtained in violation of the broad confidentiality agreement signed by EF's former employees.

EF Cultural II, 318 F.3d at 61 (emphasis supplied). See also EF Cultural I, 274 F.3d at 583, n.14 (noting that defendants provided their agent with "extremely confidential" information, which would allow the agent to "log into [plaintiff's] website as a tour leader"). Consequently, those decisions are better understood, in this context, as focusing less on whether defendants violated a website's "use restrictions," and more on whether, by employing improperly obtained confidential information, defendants gained unauthorized access by circumventing "access restrictions" to the website's data.

Having considered the parties legal memoranda (and the cases cited therein), and in light of the court of appeals' limited holdings in its EF Cultural opinions, the court agrees that the better (and more reasonable) interpretation of the phrase "exceeds authorized access" in the CFAA is a narrow one. See, e.g., Nucor Steel Marion, Inc. v. Mauer, 2010 WL 5092774, 2010

DNH 207 (D.N.H. Dec. 7, 2010) (granting defendant's motion to dismiss claims under 18 U.S.C. § 1030(a)(2) because "the complaint nowhere alleges that [defendant] used his authorized access to obtain information from [plaintiff's] computer beyond that which he was entitled to obtain."). Accordingly, under § 1030(a)(2)(C), an employee's unauthorized use, disclosure, or misappropriation of data which he or she has obtained through authorized access is not conduct governed by the CFAA.

Parenthetically, the court notes that the CFAA is somewhat atypical in that it is a criminal statute that also provides a civil cause of action. 18 U.S.C. § 1030(g). Consequently, great care must be taken when construing the statute's scope. As the Court of Appeals for the Ninth Circuit observed:

Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law. Significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read.

* * *

Basing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.

Nosal, 676 F.3d at 860. So, for example, suppose an employer's policy authorizes employees to access their work computers exclusively for business purposes. Under the hospital's proposed construction of the CFAA, an employee would be exposed to criminal prosecution if he or she accessed the computer for a decidedly non-business purpose - say to obtain a list of hospital employees to use in preparing invitations to a private function. As the Nosal court noted, "The employer should be able to fire the employee, but that's quite different from having him arrested as a federal criminal." Id. at 860, n.7.

Turning to the facts alleged in the hospital's amended complaint, it is plain that the conduct in which Dr. Thomas Moore allegedly engaged does fall squarely within the scope of section 1030(a)(2)(C)'s proscribed conduct. The hospital alleges that he was not authorized to access certain data on the hospital's servers; his hospital-issued password did not allow such access; and he circumvented the hospital's access restrictions to that data when he allegedly used his wife's password to gain unauthorized access. If those allegations are true, Dr. Thomas Moore violated the CFAA by exceeding his authorized access to, and thereby obtaining information from, the hospital's computers. Consequently, he is not entitled to judgment as a matter of law on count one of the amended complaint.

Dr. Cheryl Moore and Dr. Littell, however, were authorized to access the hospital's computers and the data at issue. They are accused of having used that access for an impermissible purpose - that is, to move data belonging to the hospital onto portable storage devices. If the allegations are true, that conduct may well be otherwise redressable. But, for the reasons discussed, it does not expose them to liability under 18 U.S.C. § 1030(a)(2)(C), since violations of an employer's computer use policy, as opposed to its computer access restrictions, are not actionable under the CFAA.

The hospital, not surprisingly, takes issue with the court's characterization of both its computer use policy and the conduct of Moore and Littell, saying:

[E]ven applying the reasoning of Nosal, the Defendants' actions fall within the scope of the CFAA because their access was unauthorized. IM-09 states that "All employees/affiliates are to access only information necessary for completing job responsibilities and to ensure the integrity of the information in their work areas." This policy specifically limits access and not just use. Defendants' last act on their way out the door was to access the information in order to download and delete data in violation of hospital policy and not for the purpose of completing job responsibilities. The access was, therefore, unauthorized.

Plaintiff's Memorandum (document no. 140-1) at 14-15 (emphasis in original). The court disagrees. Of course, the distinction between an employer-imposed "use restriction" and an "access

restriction" may sometimes be difficult to discern, since both emanate from policy decisions made by the employer - decisions about who should have what degree of access to the employer's computers and stored data, and, once given such access, the varying uses to which each employee may legitimately put those computers and the data stored on them. But, simply denominating limitations as "access restrictions" does not convert what is otherwise a use policy into an access restriction. Here, the hospital's policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an "access" restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access. An employee who is given access to hospital data need not "hack" the hospital's computers or circumvent any technological access barriers in order to impermissibly copy that data onto an external storage device. The offending conduct in such a case is misuse of data the employee was authorized to access, not an unauthorized access of protected computers and data.

Dr. Cheryl Moore and Dr. Littell were provided with access to the hospital's computers when they were given passwords that allowed them to create, view, edit, save, and delete various files on the hospital's servers. Hospital policy - in the form

of the IM-09 - then defined the legitimate uses to which they might put that information. The provision cited by the hospital is, then, akin to a policy that prohibits employees from sharing confidential information (which they have been authorized to access) with competitors, or e-mailing such information to other computers - conduct that is not proscribed by the CFAA.²

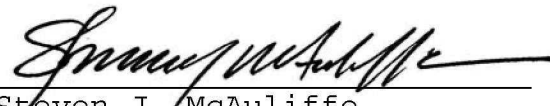
Defendants Cheryl Moore and Glenn Littell are, then, entitled to judgment as a matter of law on count one of the amended complaint.

Conclusion

For the foregoing reasons, defendants' motion to reconsider (document no. [139](#)) is granted in part, and denied in part. It is granted to the extent that defendants Cheryl Moore and Glenn Littell are entitled to judgment as a matter of law on count one of the hospital's amended complaint. In all other respects, however, that motion is denied and the court's order of March 30, 2012, stands.

² Of course, such conduct may be unlawful in other ways. It may, for example, constitute a breach of contract, theft of trade secrets, or common law conversion - the latter being one of the claims the hospital advances against the defendants.

SO ORDERED.


Steven J. McAuliffe
United States District Judge

June 29, 2012

cc: Conrad W. P. Cascadden, Esq.
Dustin M. Lee, Esq.
William E. Christie, Esq.
Charles W. Grau, Esq.