

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

----oo0oo----

ATPAC, INC., a California Corporation,

NO. CIV. 2:10-294 WBS KJM

Plaintiff,

v.

MEMORANDUM AND ORDER RE:
MOTION TO DISMISS, MOTION FOR
JUDGMENT ON THE PLEADINGS, AND
MOTION TO STRIKE

APTITUDE SOLUTIONS, INC., a Florida Corporation, COUNTY OF NEVADA, a California County, and GREGORY J. DIAZ, an individual,

Defendants.

_____ /

----oo0oo----

Plaintiff AtPac, Inc. ("AtPac") filed this action against defendants Aptitude Solutions, Inc. ("Aptitude"), County of Nevada, and Gregory J. Diaz alleging breach of contract, misappropriation of trade secrets, copyright infringement, and violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 et seq. Defendants move to dismiss and move for judgment on the pleadings on plaintiff's fourth cause of action pursuant

1 to Federal Rules of Civil Procedure 12(b)(6) and 12(c) for
2 failure to state a claim upon which relief can be granted, and to
3 strike plaintiff's prayer for statutory damages for its third
4 cause of action for copyright infringement pursuant to Rule 12(f)
5 because plaintiff is not entitled to statutory damages as a
6 matter of law.

7 I. Factual and Procedural Background

8 AtPac provides software and consulting services related
9 to county clerk-recorder information imaging systems. (Compl. ¶
10 3.) These systems are computer-based and designed to, inter
11 alia, electronically receive, store, and organize information
12 that is within the purview of a county clerk-recorder and store
13 images of relevant documents associated with this information.
14 (Id.) AtPac's clerk-recorder imaging information software is
15 distributed under the mark "CRiis." (Id.) In 1999, AtPac
16 allegedly entered into a License Agreement with County of Nevada
17 for the CRiis software and related services to help County of
18 Nevada electronically maintain and organize public information.
19 (Id. ¶ 12.) The License Agreement was allegedly amended between
20 2001 and 2006, the most recent of which extended the term of the
21 License Agreement until June 30, 2010. (Id. ¶ 13.)

22 The License Agreement allegedly provides, inter alia,
23 that AtPac retains title to the software, that the software is
24 trade secrets and that County of Nevada will not release or
25 disclose the information to third parties (Id. ¶ 14), that County
26 of Nevada will notify AtPac immediately of any known or suspected
27 unauthorized use or access of the CRiis software (Id. ¶ 16), and
28 that all documents provided to County of Nevada may not be

1 reproduced by County of Nevada (Id. ¶ 17). California law
2 governs the License Agreement. (Id. ¶ 22.)

3 In November 2008, Diaz, the Clerk-Recorder of County of
4 Nevada, allegedly notified AtPac that County of Nevada intended
5 to terminate the License Agreement and obtain the services of
6 Aptitude, one of AtPac's competitors. (Id. ¶ 23.) Diaz
7 allegedly rejected AtPac's offer to help County of Nevada extract
8 the data from AtPac's files and convert it to a form usable by
9 Aptitude. (Id.) Diaz allegedly represented in a January 8, 2008
10 letter that County of Nevada would extract the data from the
11 AtPac files on its own, and that County of Nevada would not
12 provide AtPac's trade secret information to Aptitude or save the
13 trade secret and proprietary information. (Id. ¶¶ 24-25.) On
14 January 13, 2009, County of Nevada allegedly ratified an
15 indemnification agreement between Aptitude and County of Nevada,
16 indemnifying Aptitude for claims related to "extraction and
17 migration of County data for the system conversion." (Id. ¶ 26.)

18 AtPac alleges that County of Nevada did not perform the
19 data extraction itself, and that it instead provided Aptitude
20 with AtPac's trade secret and copyright-protected information.
21 (Id. ¶¶ 28-30.) Specifically, AtPac alleges that Diaz and County
22 of Nevada copied and provided this information through e-mail
23 communications and through a public, non-secure file transfer
24 protocol ("FTP") site entitled "Aptitude FTP" without AtPac's
25 authorization. (Id. ¶¶ 29-33.) Diaz and County of Nevada
26 allegedly provided Aptitude with "full and unfettered access" to
27 the server located in County of Nevada's offices on which AtPac
28 trade secret information and the CRIis source code are stored

1 without AtPac's authorization. (Id. ¶ 34.)

2 Plaintiff filed its Complaint on February 3, 2010,
3 (Docket No. 1) and Aptitude and Diaz filed their Answer on March
4 19, 2010. (Docket No. 10.) Presently before the court are
5 County of Nevada's motion to dismiss plaintiff's fourth cause of
6 action for violation of the CFAA (Docket No. 13) and Aptitude and
7 Diaz's motion for judgment on the pleadings on plaintiff's fourth
8 cause of action for violation of the CFAA, as well as each
9 defendant's motion to strike plaintiff's prayer for statutory
10 damages.

11 II. Discussion

12 On a motion to dismiss, the court must accept the
13 allegations in the complaint as true and draw all reasonable
14 inferences in favor of the plaintiff. Scheuer v. Rhodes, 416
15 U.S. 232, 236 (1974), overruled on other grounds by Davis v.
16 Scherer, 468 U.S. 183 (1984); Cruz v. Beto, 405 U.S. 319, 322
17 (1972). To survive a motion to dismiss, a plaintiff needs to
18 plead "only enough facts to state a claim to relief that is
19 plausible on its face." Bell Atl. Corp. v. Twombly, 127 S. Ct.
20 1955, 1974 (2007). This "plausibility standard," however, "asks
21 for more than a sheer possibility that a defendant has acted
22 unlawfully," and where a complaint pleads facts that are "merely
23 consistent with" a defendant's liability, it "stops short of the
24 line between possibility and plausibility." Ashcroft v. Iqbal,
25 129 S. Ct. 1937, 1949 (2009) (quoting Twombly, 550 U.S. at
26 556-57).

27 Judgment on the pleadings is appropriate after the
28 pleadings have closed when, on the face of those pleadings,

1 accepting the allegations of the non-moving party as true, no
2 material issue of fact remains to be resolved. See Fed. R. Civ.
3 P. 12(c); Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc.,
4 896 F.2d 1542, 1550 (9th Cir. 1990). Under such circumstances,
5 the moving party can obtain judgment as a matter of law. Hal
6 Roach Studios, 896 F.2d at 1550. "Generally, district courts
7 have been unwilling to grant a Rule 12(c) dismissal 'unless the
8 movant clearly establishes that no material issue of fact remains
9 to be resolved and that he is entitled to judgment as a matter of
10 law.'" Doleman v. Meiji Mut. Life Ins. Co., 727 F.2d 1480, 1482
11 (9th Cir. 1984) (quoting 5A C. Wright & A. Miller, Federal
12 Practice and Procedure: Civil, § 1368 at 690 (1969)).

13 On a motion for judgment on the pleadings, the factual
14 allegations of the non-moving party are taken as true. Doleman,
15 727 F.2d at 1482 (citing Austad v. United States, 386 F.2d 147,
16 149 (9th Cir. 1967)). A Rule 12(c) motion is therefore
17 essentially equivalent to a Rule 12(b)(6) motion to dismiss and
18 consequently, a district court may "dispos[e] of the motion by
19 dismissal rather than judgment."¹ Sprint Telephony PCS, L.P. v.
20 County of San Diego, 311 F. Supp. 2d 898, 902-03 (S.D. Cal.

21
22 ¹ The motions differ in only two respects:

23 (1) the timing (a motion for judgment on the pleadings is
24 usually brought after an answer has been filed, whereas
25 a motion to dismiss is typically brought before an answer
26 is filed) . . . and (2) the party bringing the motion (a
27 motion to dismiss may be brought only by the party
against whom the claim for relief is made, usually the
defendant, whereas a motion for judgment on the pleadings
may be brought by any party).

28 Sprint Telephony PCS, L.P. v. County of San Diego, 311 F. Supp. 2d
898, 902-03 (S.D. Cal. 2004).

1 2004). "[D]ismissal can be based on either the lack of a
2 cognizable legal theory or the absence of sufficient facts
3 alleged under a cognizable legal theory." Sprint Telephony, 311
4 F. Supp. 2d at 902-03; see also Balistreri v. Pacifica Police
5 Dep't, 901 F.2d 696, 699 (9th Cir. 1988). The court will
6 therefore evaluate defendants' motions together.

7 In general a court may not consider items outside the
8 pleadings upon deciding a motion to dismiss or motion for
9 judgment on the pleadings, but may consider items of which it can
10 take judicial notice. Heliotrope Gen., Inc. v. Ford Motor Co.,
11 189 F.3d 971, 981 n.18 (9th Cir. 1999) (internal citations
12 omitted); Barron v. Reich, 13 F.3d 1370, 1377 (9th Cir. 1994). A
13 court may take judicial notice of facts "not subject to
14 reasonable dispute" because they are either "(1) generally known
15 within the territorial jurisdiction of the trial court or (2)
16 capable of accurate and ready determination by resort to sources
17 whose accuracy cannot reasonably be questioned." Fed. R. Evid.
18 201. County of Nevada has submitted a Request for Judicial
19 Notice ("RJN") (Docket No. 15) that contains a copy of the U.S.
20 Copyright Office's web page showing that AtPac registered its
21 CRiis software for copyright on January 26, 2010. (RJN Ex. A.)
22 The court will take judicial notice of this exhibit because the
23 record is generated by an official government website such that
24 its accuracy is not reasonably in dispute. See, e.g., Edejer v.
25 DHI Mortg. Co., No. 09-1302, 2009 WL 1684714, at *4 (N.D. Cal.
26 June 12, 2009); Piazza v. EMPI, Inc., No. 07-954, 2009 WL 590494,
27 at *4 (E.D. Cal. Feb. 29, 2008); see also Denius v. Dunlap, 330
28 F.3d 919, 926-27 (7th Cir. 2003) (taking judicial notice of

1 information on official government website).

2 A. Motions to Dismiss Plaintiff's Fourth Cause of Action
3 for Violation of the CFAA

4 As a preliminary matter the court notes that the
5 motions are substantively identical, and will therefore only
6 refer to and cite County of Nevada's motion to dismiss when
7 discussing the motions.

8 The CFAA prohibits any person from "intentionally
9 access[ing] a computer without authorization or exceed[ing]
10 authorized access, and thereby obtain[] . . . information from
11 any protected computer" 18 U.S.C. § 1030(a)(2)(C). It
12 also prohibits any person from "knowingly, and with intent to
13 defraud, access[ing] a protected computer without authorization,
14 or exceed[ing] authorized access, and by means of such conduct
15 further[ing] the intended fraud and obtain[ing] anything of value
16" Id. § 1030(a)(4). The CFAA also prohibits any person
17 from "intentionally access[ing] a protected computer without
18 authorization, and as a result of such conduct recklessly
19 caus[ing] damage; or [] intentionally access[ing] a protected
20 computer without authorization, and as a result of such conduct,
21 caus[ing] damage and loss." Id. § 1030(a)(5)(B)-(C). The CFAA
22 does not define "authorization" or "authorized access," but does
23 define "[e]xceeds authorized access" as "to access a computer
24 with authorization and to use such access to obtain or alter
25 information in the computer that the accesser is not entitled to
26 so obtain or alter." Id. § 1030(e)(6); see also LVRC Holdings
27 LLC v. Brekka, 581 F.3d 1127, 1132-33 (9th Cir. 2009) (discussing
28 "authorization" under the CFAA). The CFAA is a criminal statute

1 that also allows "any person who suffers damage or loss" under
2 the statute to bring a civil action. Id. § 1030(g); see
3 generally LVRC Holdings, 581 F.3d at 1130-33.

4 Plaintiff's fourth cause of action alleges that
5 Aptitude, County of Nevada, and Diaz all violated these sections
6 of the CFAA by accessing "the computer network (including
7 computers and servers)" on which AtPac's trade secret and
8 copyright-protected information reside without authorization or
9 in excess of any authorization granted to them by AtPac. (FAC ¶
10 73.) Plaintiff alleges that these computers and servers are
11 located in County of Nevada's offices. (Id. ¶ 34.)

12 1. County of Nevada and Diaz's Liability

13 With respect to County of Nevada and Diaz, plaintiff
14 fails to allege that they lacked any authority or authorization
15 to use the computers. See LVRC Holdings, 581 F.3d at 1132-33
16 (explaining the distinction between the terms "without
17 authorization" and "exceeds authorized access"). Plaintiff does
18 not allege that plaintiffs were absolutely prohibited from using
19 them. To the contrary, it is clear from the License Agreement
20 that plaintiff granted those defendants the right to use
21 plaintiff's software in conjunction with County of Nevada's
22 computer system. (Compl. ¶ 12.) Counsel for plaintiff also
23 conceded at oral argument that County of Nevada was authorized to
24 use the computer at issue for at least some purposes. For this
25 reason alone defendant's motion to dismiss should be granted with
26 respect to County of Nevada and Diaz for the alleged §
27 1030(a)(5)(B)-(C) violations, as it only provides for liability
28 for "intentionally access[ing] a protected computer without

1 authorization" and does not provide for liability for exceeding
2 authorized access.

3 Plaintiff instead argues in its Opposition that County
4 of Nevada and Diaz exceeded their authorization to access the
5 computers by accessing the CRIis software source code in
6 violation of the License Agreement. (Opp'n at 7, 9.) While the
7 Complaint excerpts provisions of the alleged License Agreement
8 that cover disclosures to third parties, copies, notification of
9 unauthorized use, periodic audits, and reproduction of the
10 software, it fails to contain any allegation that the License
11 Agreement prohibited the County of Nevada from accessing,
12 obtaining, or altering plaintiff's software or source code.
13 Indeed, the complaint fails to allege any facts that would
14 indicate what constitutes an unauthorized access of the software
15 by County of Nevada; the complaint merely states there were
16 limits on how County of Nevada could use it by making copies of
17 it or disclosing it to third parties. (See Compl. ¶¶ 14-15.)
18 Rather, plaintiff's fourth cause of action makes only the
19 conclusory allegation that defendants violated the CFAA. (Compl.
20 ¶¶ 73-75.) Such conclusory allegations are "mere labels and
21 conclusions" that are prohibited by Federal Rule of Civil
22 Procedure 8(a)(2). Twombly, 550 U.S. at 555.

23 To the extent that plaintiff alleges that County of
24 Nevada or Diaz are liable under the CFAA for providing Aptitude
25 access to plaintiff's software, State Analysis, Inc. v. American
26 Financial Services Assoc., 621 F. Supp. 2d 309 (E.D. Va. 2009),
27 is instructive. In State Analysis, the court confronted a
28 similar factual situation where a licensee defendant provided a

1 third party with the means to access the plaintiff's protected
2 materials. That court noted that the licensee was not guilty of
3 unauthorized access or access exceeding authorization under the
4 CFAA, but guilty only of unauthorized use or misappropriation of
5 its access under the license agreement. 621 F. Supp. 2d at 317
6 ("[R]ather, the allegation is that [licensee defendant] used the
7 information in an inappropriate way.") As the court has
8 explained above, plaintiff's Complaint is devoid of any
9 allegations that County of Nevada or Diaz exceeded their
10 authorized access or accessed, obtained, or altered prohibited
11 materials. Accordingly, the court will dismiss plaintiff's
12 fourth cause of action as against County of Nevada and Diaz.

13 2. Aptitude's Liability

14 Courts have differed as to how broadly or narrowly to
15 construe 18 U.S.C. § 1030(a)(2) and the concepts of
16 "authorization" and "authorized access." Several cases exploring
17 the potential liability of employees or former employees, for
18 example, have determined that employees may go beyond their
19 authorized access when they act as agents for others or act
20 contrary to their employer's interest. See, e.g., LVRC Holdings,
21 581 F.3d at 1133 (clarifying that employee's "authorization" to
22 use a computer does not cease when employee uses computer in
23 violation of employer's limitations, but rather that employee has
24 merely "exceeded authorized access"); EF Cultural Travel BV v.
25 Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (former employee
26 exceeded authorized access when he passed along information to a
27 third party in violation of a broad confidentiality agreement);
28 Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.,

1 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (plaintiff's employees
2 were defendant's agents when they had accepted job offers with
3 defendant and used work computers to send trade secrets to
4 defendant; employees therefore lacked authorization to access
5 work computers). The Ninth Circuit has clarified that a
6 plaintiff can bring a cause of action under the CFAA for
7 unauthorized access to information stored on a third party's
8 computer. Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir.
9 2004) (no ownership or control of computer required for CFAA
10 action alleging harm by unauthorized access).

11 Two cases from the United States District Court for the
12 Eastern District of Virginia address the specific question of
13 whether third-party defendants can be liable under the CFAA where
14 their access to plaintiff's software is made possible by another
15 party violating its license agreement with the plaintiff. While
16 of course neither case is binding authority, the court finds
17 their juxtaposition instructive. In SecureInfo Corp. v. Telos
18 Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005), SecureInfo granted a
19 software license to defendant Berman, a consultant for one of
20 SecureInfo's competitors, which allowed him narrowly restricted
21 access to the SecureInfo's materials. Berman--who was not sued
22 under the CFAA--then allowed the other defendants access to
23 SecureInfo's materials and his server on which they were located,
24 in violation of the license agreement. Id. at 608. The court
25 explained that Berman gave the other defendants "permission and
26 authorization to use the [] server and view what was contained
27 therein" and that "[e]ven if Mr. Berman allowed the defendants
28 access to the [] server and SecureInfo's materials in violation

1 of the license agreements, under his grant of authority to the
2 defendants, they were entitled to obtain the information on the
3 server." Id. at 609.

4 In contrast, the District Court for the Eastern
5 District of Virginia four years later in State Analysis rejected
6 SecureInfo's seemingly absolute ban on third-party defendant CFAA
7 liability where one party gives the third-party defendant access
8 to software in violation of a license agreement with the
9 plaintiff. The State Analysis court held that defendant and
10 prior client Kimbell Sherman Ellis ("KSE") acted "without
11 authorization" when it accessed plaintiff's website and obtained
12 proprietary material with the user names and passwords given to
13 it by one of plaintiff's clients. That court found that the
14 defendant "may not hide behind purported 'authorization' granted
15 to it" by the client that violated the terms of use of its
16 contract with plaintiff, particularly given that KSE was
17 plaintiff's formal client and presumably knew the terms of
18 plaintiff's license agreement. Id. at 316.

19 Naturally, plaintiff relies on State Analysis and
20 argues not only that Aptitude cannot hide behind County of
21 Nevada's "authorization" because it knew it violated the license
22 agreement, but that the authorization was void ab initio because
23 County of Nevada contracted away its right to authorize third-
24 party access. In contrast, defendants rely on SecureInfo for the
25 proposition that Aptitude did not exceed the "unfettered" access
26 granted it by County of Nevada and Diaz. Plaintiff notes that
27 SecureInfo distinguished its fact pattern from that in EF
28 Cultural Travel, stating in dicta that had the plaintiff sued

1 licensee Berman rather than the third parties, the rule in EF
2 Cultural Travel "may have applied." 387 F. Supp. 2d at 609. All
3 this means, however, is that the licensee may have exceeded his
4 authorization and been subject to CFAA liability had he been
5 sued, not that the third party defendants would become liable
6 solely due to the presence of an additional defendant.

7 While the cases described above make clear that certain
8 "insiders" can exceed their authorized access or even in some
9 circumstances lose their authorization to access computers and
10 computer networks, State Analysis does not establish--and the
11 court is not willing to so rule--that third parties can
12 ordinarily be liable under the CFAA for exploiting a licensee's
13 violation of its license agreement. Rather, State Analysis is
14 perhaps best applied in situations where the third-party
15 defendant uses subterfuge--like using user names and passwords
16 that do not belong to it--to gain access to plaintiff's protected
17 materials on plaintiff's own website, computers, or servers.

18 This is consistent with the Ninth Circuit's decision in
19 Theofel, which, in dicta referencing its prior analysis under the
20 Stored Communications Act, 18 U.S.C. § 2701 et seq., implied that
21 defendants who had issued a patently overbroad and illegal
22 subpoena to Netgate for plaintiff's e-mails and subsequently
23 viewed those e-mails on Netgate's website were not "authorized"
24 under the CFAA by Netgate to view those e-mails. See 359 F.3d at
25 1072-74, 1078 (stating that the Stored Communications Act--and
26 presumably also the CFAA--"provides no refuge for a defendant who
27 procures consent by exploiting a known mistake that relates to
28 the essential nature of his access."). While Theofel is silent

1 with respect to the instant issue of whether a licensee can
2 consent to give access to the licensed information to another,
3 this court adopts the basic premise that a defendant's deceitful
4 conduct can vitiate consent or authorization by a licensee. The
5 door remains open for third-parties to be liable under the CFAA
6 for accessing software programs held on a licensee's computers or
7 servers where the defendant engages in the kind of fraudulent
8 conduct that was present in State Analysis.

9 This case is more similar to SecureInfo where the
10 licensee gives the third-party access to its own servers to
11 access the protected information. Plaintiff does not allege that
12 Aptitude accessed plaintiff's computers or servers, or that such
13 access would require an access code or password that County of
14 Nevada wrongfully provided Aptitude. Plaintiff instead alleges
15 that County of Nevada gave Aptitude access to the servers located
16 in its offices, and sent information by e-mail and via a public
17 FTP site. (Compl. ¶¶ 28-34.) This does not allege the sort of
18 subterfuge this court believes is necessary to find a defendant
19 not party to a license agreement civilly liable under the CFAA
20 where the licensee grants it authority to access information in
21 violation of the license agreement.

22 B. Motions to Strike Plaintiff's Prayer for Statutory
23 Damages

24 In their respective motions, the defendants each move
25 to strike plaintiff's prayer for relief for statutory damages
26 under the Copyright Act pursuant to Federal Rule of Civil
27 Procedure 12(f). Section 412 of the Copyright Act prohibits an
28 award of statutory damages unless a plaintiff has first

1 registered its work prior to the "commencement of the
2 infringement." 17 U.S.C. § 412. "[T]he first act of
3 infringement in a series of ongoing infringements of the same
4 kind marks the commencement of one continuing infringement under
5 § 412." Derek Andrew, Inc. v. Poof Apparel Corp., 528 F.3d 696,
6 701 (9th Cir. 2008) (emphasis in original). According to County
7 of Nevada's Request for Judicial Notice, plaintiff registered its
8 copyright on January 26, 2010 (RJN Ex. A.), a mere eight days
9 before filing its Complaint in this action. (See Docket No. 1.)

10 While the face of plaintiff's Complaint does not allege
11 any legally different kind of copyright infringement occurred
12 between January 26, 2010 and February 3, 2010, it does allege
13 that County of Nevada and Diaz copied and disclosed plaintiff's
14 protected information to Aptitude in January 2009 (Compl. ¶¶ 23-
15 33), and that Nevada County continues to maintain copies of
16 plaintiff's protected information to this day. (Id. ¶¶ 35-37.)
17 The discovery process will properly determine if or in what ways
18 defendants have continued to violate plaintiff's copyright, and
19 after discovery defendants can renew their motion or raise the
20 issue on summary judgment.


21 IT IS THEREFORE ORDERED that County of Nevada's motion
22 to dismiss plaintiff's fourth cause of action be, and the same
23 hereby is, GRANTED.

24 IT IS FURTHER ORDERED that Aptitude and Diaz's motion
25 for judgment on the pleadings on plaintiff's fourth cause of
26 action be, and the same hereby is, GRANTED.

27 IT IS FURTHER ORDERED that defendants' motions to
28 strike be, and the same hereby are, DENIED.

1 Plaintiff is given twenty days from the date of this
2 Order to file an amended complaint consistent with this Order.

3 DATED: April 28, 2010

4 

5 WILLIAM B. SHUBB

6 UNITED STATES DISTRICT JUDGE

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28