United States District Court
For the Northern District of California

1

2

3

4

5   UNITED STATES DISTRICT COURT

6   NORTHERN DISTRICT OF CALIFORNIA

7

8   UNITED STATES OF AMERICA,   No. CR-08-0237 EMC

9   Plaintiff,

10   v.   **ORDER DENYING DEFENDANT'S
                                                     MOTION TO DISMISS**
11   DAVID NOSAL,   **(Docket Nos. 274, 276)**

12   Defendant.
                                         /
13

14

15   I.   **INTRODUCTION**

16   Pending before the Court is Defendant's motion to dismiss three counts of violating the

17   Computer Fraud and Abuse Act ("CFAA"). Docket No. 274, 276.[1] The superseding indictment in

18   this case included eight counts for violations of the CFAA related to unauthorized access of a

19   computerized database of his former employer, Korn/Ferry. The indictment also included several

20   counts for misappropriation, theft of trade secrets, and conspiracy that are not the subject of this

21   motion. Judge Patel previously dismissed five of the counts for violations of the CFAA. Docket

22   No. 135. The government appealed the dismissal to the Ninth Circuit. A panel of three judges

23   reversed the dismissal, but upon en banc review, the Ninth Circuit affirmed Judge Patel's opinion.

24   Defendant now argues that the Ninth Circuit's en banc opinion clarified the application of the CFAA

25   in a way that now requires dismissal of the remaining CFAA counts, which were not addressed on

26

27   _____

28   [1] Docket No. 274 is the original version of the motion; Docket No. 276 is an amended
     motion.

1   the appeal. Since the hearing on this motion, the government has secured a second superseding

2   indictment adding additional factual detail to two of the CFAA counts.[2]

3   ## II.   FACTUAL & PROCEDURAL BACKGROUND

4   The original indictment in this case was filed on April 10, 2008. Docket No. 1. The first

5   superseding indictment was filed on June 28, 2008. Docket No. 42. The superseding indictment

6   brings various charges against Defendant, including eight charges of violating the Computer Fraud

7   and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a), for aiding and abetting his co-conspirators in

8   securing unauthorized access to a protected computer with intent to defraud and obtain something of

9   value. *Id.* ¶ 21 (counts 2-9). The following facts are taken from the first superseding indictment.

10 Defendant is a former employee of Korn/Ferry, an executive search firm headquartered in

11 Los Angeles with offices in San Francisco and Redwood City, California. Superseding Indictment

12 ("SI") ¶¶ 1-2. The company is a leading provider of executive recruitment services, assisting

13 companies to fill executive and other high level positions. SI ¶ 1. Defendant worked for Korn/Ferry

14 from approximately April 1996 until October 2004. SI ¶ 2. When he ceased his employment with

15 the firm, he entered into Separation and General Release Agreement, and an Independent Contractor

16 Agreement with Korn/Ferry. SI ¶ 2. In these agreements, he agreed to serve as an independent

17 contractor to Korn/Ferry from November 1, 2004 through October 15, 2005. SI ¶ 2. He also agreed

18 not to perform executive search or related services for any other entity during the term of his

19 contract. SI ¶ 2. In return, he received compensation in the amount of $25,000 per month. SI ¶ 2.

20 Despite these agreements, Defendant began to set up his own rival executive search firm with the

21 assistance of three other current or former Korn/Ferry employees, Becky Christian, J.F., and M.J. SI

22 ¶¶ 3-5. J.F. was Defendant's assistant while he was a Korn/Ferry employee, and continued to be

23 employed by Korn/Ferry after Defendant's departure. SI ¶ 4. M.J. was a Korn/Ferry employee until

24 approximately March of 2005. SI ¶ 5.

25

26 _____

27 [2] The second superseding indictment also renumbers the counts. The counts at issue in this motion, which had been numbers three, eight, and nine, are now counts two, three, and four,
28 respectively. Since this motion pertains to the first superseding indictment, it will refer to the counts as numbered therein.

1 Christian, who is also named as a defendant in the superseding indictment, was employed by

2 Korn/Ferry from approximately September 1999 to approximately January 2005. SI ¶ 3. After

3 leaving Korn/Ferry, she set up an executive search firm known as Christian & Associates, though

4 she was in fact working with Defendant to set up his executive search firm. SI ¶ 3. Christian

5 generally retained 20% of the revenues from the searches the two conducted, while Defendant

6 retained 80%. SI ¶ 3.

7 Korn/Ferry maintained the "Searcher" database, a proprietary database of executives and

8 companies. SI ¶ 6. Using the "Custom Report" feature of the database, Korn/Ferry employees were

9 able to created targeted reports on executives, companies, and prior search engagements Korn/Ferry

10 had conducted for clients. SI ¶ 6. The database was also capable of producing "source lists," or

11 candidate lists, which were provided to client companies with regards to a particular position they

12 were trying to fill. SI ¶ 8. Korn/Ferry had built up the information contained in the Searcher

13 database over many years, and considered it to be one of the most comprehensive databases of its

14 kind in the world. SI ¶ 7.

15 Korn/Ferry took a number of steps to preserve the confidential nature of the Searcher

16 database, including controlling electronic access to the database, and controlling physical access to

17 the servers on which it was stored. SI ¶ 9. Korn/Ferry employees received unique user names and

18 passwords that allowed them to access the company's computer systems, including the Searcher

19 Database. SI ¶ 9. These passwords were intended for use by employees only. SI ¶ 9. All

20 Korn/Ferry employees, including Defendant, entered into agreements explaining the proprietary

21 nature of the Searcher database, and restricting the use of the database and related information to

22 legitimate company business. SI ¶ 10. Defendant executed such an agreement on or about April 26,

23 1996. SI ¶ 10.

24 Korn/Ferry also explicitly noted the confidential and proprietary nature of the information

25 from the Searcher database on reports and in the computer logon process. SI ¶ 11. All custom

26 reports generated from the database had the phrase "Korn/Ferry Proprietary and Confidential"

27 written across the top. SI ¶ 11. When an individual logged on to the Korn/Ferry computer system,

28 the following notification was displayed

1   This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution. . . .

SI ¶ 11.

     The superseding indictment alleges that Defendant, along with co-conspirator Christian and others, "did steal, and without authorization knowingly take by fraud, artifice, and deception, trade secrets from Korn/Ferry's computer system, including source lists." SI ¶ 15. The indictment alleges that individual co-conspirators and others obtained these source lists and other trade secrets prior by using their own Korn/Ferry usernames and passwords prior to and upon termination, and that they did so without authorization and in excess of authorization. SI ¶ 16. Defendant and co-conspirators also obtained trade secrets from Korn/Ferry's computer system by using, either directly or through J.F., J.F.'s Korn/Ferry username and password, and that this was done without authorization and in excess of authorization. SE ¶ 17. The specific factual allegations related to the various CFAA counts in the first superseding indictment are as follows:

A.   Count 2

     During the fourth quarter of 2004, just prior to the end of her employment with Korn/Ferry, Christian downloaded custom reports from the Searcher database containing over 3000 records. SI ¶ 19j. She took copies of these reports with her when she left the firm. SI ¶ 19j.

B.   Count 3

     On or about April 11, 2005, Christian sent an email to J.F. that stated in part, "It is to [sic] difficult to explain the searcher run I would need to log in as you." SI ¶ 19a. The next day, Christian emailed Defendant three Korn/Ferry source lists of Chief Financial Officers ("CFOs") that had been downloaded from the Searcher database earlier that day using J.F.'s username and password. SI ¶ 19b. These source lists were marked as proprietary and confidential. SI ¶ 19b. Defendant and Christian later used individuals on this source list in performing a Chief Financial Officer ("CFO") search for Company B. SI ¶ 19e.

     The second superseding indictment specifies that it was Christian who downloaded the source lists after J.F. provided Christian with her password. Second Superseding Indictment ("SSI")

United States District Court
For the Northern District of California

1 ¶ 19a. Christian did not have authorization from Korn/Ferry to access its computer system at that

2 time. *Id.*

3 C.   Count 4

4   Also in April 2005, Company C retained Defendant to conduct a search for a senior vice

5 president of human resources. SI ¶ 19h. The CEO of Company C emailed Defendant on April 25,

6 2005, asking Defendant to draft a job description for the position, and requesting that Defendant

7 "make sure that the payment terms are the aggressive ones you quoted." SI ¶ 19h. On April 29,

8 Christian emailed the CEO of Company C a position description, copying Defendant, and signing

9 the email "David & Becky." SI ¶ 19i. This position description was largely identical to a position

10 specification recently obtained from Korn/Ferry's computer system by J.F. SI ¶ 19i.

11 D.   Count 5

12   On or about May 26, 2005, M.J. contacted J.F., requesting that J.F. obtain information from

13 the Searcher database on 17 individuals, and on a specific prior Korn/Ferry search engagement. SI ¶

14 19l. M.J. had obtained the names of at least some of the individuals from Defendant. SI ¶ 19l. J.F.

15 obtained the requested information from the Searcher database, and copied the files containing the

16 information onto a C.D., which J.F. then provided to M.J. SI ¶ 19l. Defendant later used at least

17 some of this information in a meeting with a prospective client. SI ¶ 19l.

18 E.   Count 6

19   On or about June 3, 2005, J.F. performed a query within the Searcher database for human

20 resources managers at M.J.'s request. SI ¶ 19m. This query yielded a list of approximately 366

21 executives, which J.F. then exported to a spreadsheet titled "Choc Chip Cookie Recipes," and

22 burned to a C.D. titled "ChocChip Cookies." SI ¶ 19m. J.F. later provided this C.D. to M.J. for use

23 in the search for Company C. SI ¶ 19m.

24 F.   Count 7

25   On or about June 23, 2005, J.F. used the Searcher database to create a custom report for

26 senior vice president supply chain managers working at various companies. SI ¶ 19n. This report

27 listed approximately 1,205 executives. SI ¶ 19n. J.F. later provided the custom report to Christian,

28 who used it in an executive search. SI ¶ 19n.

G.   Count 8

On or about July 12, 2005, an individual used a computer at Defendant's San Francisco offices to remotely log into Korn/Ferry's computer network using J.F.'s username and password. SI ¶ 19f. A co-conspirator then ran queries for information on two of the individuals who were being considered for Company B's CFO position. SI ¶ 19f. The following month, Company B announced that it had hired one of these two individuals. SI ¶ 19f.

The second superseding indictment does not identify who logged onto the computer, but does specify that Christian was the one who ran the queries, and that she additionally downloaded two source lists from the Korn/Ferry system. SSI ¶ 19f.

H.   Count 9

On or about July 29, 2005, J.F. used M.J.'s computer in Defendant's offices to remotely log into the Korn/Ferry computer network with her username and password. SI ¶ 19o. She then turned the computer over to M.J., who used the Searcher database to download information from the database to the computer, including 25 source lists. SI ¶ 19o.

I.   Relevant Procedural History

On January 12, 2009, Defendant filed a motion to dismiss various counts in the superseding indictment, including the CFAA counts. Docket No. 84. Defendant argued that the CFAA does not cover misuse or misappropriation of information obtained by employees with authorization to access the information, and that the counts should thus be dismissed because the indictment alleges nothing more. *Id.* at 3-7. Judge Patel denied Defendant's motion to dismiss the CFAA counts, holding that the statute covered the situations alleged in the complaint. Docket No. 105.

In September 2009, the Ninth Circuit decided *LVRC Holdings LLC v. Brekka*, which interpreted the CFAA's prohibition on accessing computers "without authorization" or "exceeding authorized access." 581 F.3d 1127, 1133-35 (9th Cir. 2009). In light of *Brekka*, Defendant filed a renewed motion to dismiss on October 5, 2009. Docket No. 122. Judge Patel granted Defendant's motion as to counts two, and four through seven, those counts which were predicated on allegations that Christian, J.F., or M.J. accessed Korn/Ferry's computers while they were still employed by Korn/Ferry, and thus still permitted to access the Searcher database. Docket No. 135 at 9.

1   The government appealed these dismissals to the Ninth Circuit. A three judge panel of the

2 Ninth Circuit reversed, but Defendant successfully sought en banc review, and the en banc panel of

3 the Ninth Circuit upheld the dismissals. *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

4 Though counts three, eight, and nine were not considered on appeal, Defendant now argues that the

5 Ninth Circuit's decision in *Nosal* requires that those claims be dismissed as well.

III.   DISCUSSION

7   Under Rule 12 of the Federal Rules of Criminal Procedure, a Defendant may make a motion

8 to dismiss before trial raising "any defense, objection, or request that the court can determine

9 without a trial of the general issue." Fed. R. Crim. P. 12(2). In analyzing a motion to dismiss an

10 indictment, the court must accept the truth of the facts alleged in the indictment. *United States v.*

11 *Boren*, 278 F.3d 911, 914 (9th Cir. 2002). "An indictment will withstand a motion to dismiss 'if it

12 contains the elements of the charged offense in sufficient detail (1) to enable the defendant to

13 prepare his defense; (2) to ensure him that he is being prosecuted on the basis of the facts presented

14 to the grand jury; (3) to enable him to plead double jeopardy; and (4) to inform the court of the

15 alleged facts so that it can determine the sufficiency of the charge.'" *United States v. Rosi*, 27 F.3d

16 409, 414 (9th Cir. 1994) (quoting *United States v. Bernhardt*, 840 F.2d 1441, 1445 (9th Cir. 1988)).

17   An indictment will be found defective and dismissed if it fails to recite an essential element

18 of the charged offence. *United States v. Gondinez-Rabadan*, 289 F.3d 630, 632 (9th Cir. 2002). The

19 Supreme Court has held that "[i]t is generally sufficient that an indictment set forth the offense in the

20 words of the statute itself, as long as those words of themselves fully, directly, and expressly,

21 without any uncertainty or ambiguity, set forth all the elements necessary to constitute the offence

22 intended to be punished." *Hamling v. United States*, 418 U.S. 87, 117, 94 (1974) (internal citations

23 and quotation marks omitted). The Ninth Circuit has noted, however, that "implied, necessary

24 elements, not present in the statutory language, must be included in an indictment." *United States v.*

25 *Jackson*, 72 F.3d 1370, 1380 (9th Cir. 1995). On the other hand, indictments are not required to

26 incorporate judicial decisions that have interpreted the statutory language. *United States v. Renteria*,

27 557 F.3d 1003, 1006-07 (9th Cir. 2009).

United States District Court
For the Northern District of California

A.   CFAA Statutory Language

The CFAA provides criminal penalties for an individual who:

> knowingly and with intent to defraud, accesses a protected computer
> without authorization, or exceeds authorized access, and by means of
> such conduct furthers the intended fraud and obtains anything of
> value, unless the object of the fraud and the thing obtained consists
> only of the use of the computer and the value of such use is not more
> than $5,000 in any 1-year period

18 U.S.C. § 1030(a)(4). In order to establish a violation of this provision, the government must show that Defendant "(1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value." *Brekka*, 581 F.3d at 1132. The statute does not define the term "authorization," but does define the phrase "exceeds authorized access" as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6).

Judge Patel initially denied Defendant's motion to dismiss the CFAA counts under this provision. Docket No. 105. Judge Patel recognized that the Ninth Circuit had not yet addressed whether the CFAA applied to a user who was otherwise authorized to access a computer but who did so with the intent to misuse or misappropriate information. *Id.* at 6. Surveying cases from other circuits, however, she concluded that "A CFAA violation under section 1030(a)(4) occurs when a person accesses a protected computer knowingly and with the intent to defraud – which renders the access unauthorized or in excess of authorization – and then, by means of such conduct, the person furthers the intended fraud." *Id.* at 8. As Defendant and his co-conspirators had accessed the Searcher database with the intent to make unauthorized use of the information therein, Judge Patel found that they were thus acting without authorization or in excess of authorized access. *Id.* at 9-10.

B.   *LVRC Holdings v. Brekka*

Shortly thereafter, the Ninth Circuit considered the interpretation of the term "without authorization" under the CFAA in *Brekka*. 581 F.3d at 1133-35. In that case, which arose under the provision of the CFAA that allows a private right of action for anyone who suffers damage from violations of one of the criminal provisions of that Act, an employer sued a former employee who

United States District Court
For the Northern District of California

1 had allegedly acted without authorization in emailing certain work files to his personal computer.

2 *Id.* at 1129-30. At the time the defendant emailed himself the files, he was an employee with

3 authorization to access the files in question in the course of performing his duties. *Id.* The employer

4 argued, however, that he had violated the CFAA because he accessed and transmitted the files not

5 for the purposes of executing his duties, but to further his own personal interests. *Id.* at 1132.

6   The court rejected this argument, and held that whether an employee using an employer's

7 computer is acting with authorization depends not on the user's intent, but on the employer's actions

8 to grant or deny permission to use the computer or relevant content. *Id.* at 1135. The court held that

9 the prohibition on accessing a computer "without authorization" referred to one who "accesses a

10 computer without any permission at all, while a person who 'exceeds authorized access,' has

11 permission to access the computer, but accesses information on the computer that the person is not

12 entitled to access." *Id.* at 1133. Based on this interpretation of the statute, the court concluded that

13 the defendant had not acted either without authorization or in excess of his authorization because he

14 had possessed authorization to access the relevant files at the time that he emailed them, and his

15 motivation for doing so did not render his access "without authorization." *Id.* at 1135.

16   Following *Brekka*, Judge Patel reconsidered the earlier ruling denying Defendant's motion to

17 dismiss the CFAA claims. Docket No. 135. In her January 6, 2010 order, she noted that reading

18 *Brekka* together with the statutory definition of "exceeds authorized access" makes clear that, "an

19 individual's intent in accessing a computer, be it to defraud or otherwise, is irrelevant in determining

20 whether an individual has permission or is authorized to access the computer." *Id.* at 8. As counts

21 two and four through seven were based on allegations that Christian and J.F. had accessed the

22 Searcher database during their employment with Korn/Ferry, and thus during a period where they

23 were authorized to access the database, Judge Patel found that they had not acted without

24 authorization or in excess of authorization. *Id.* at 11. Accordingly, those claims were dismissed. *Id.*

25   Considering the remaining counts under the CFAA, Judge Patel noted that on its face, the

26 indictment did not explicitly specify who accessed the Searcher database in the incidents that are the

27 basis for counts three and eight. *Id.* at 12; *see* SI ¶¶ 19b, 19f, 21. At the December 16, 2009 hearing

28 on the motion to reconsider, the government indicated that at trial it intends to introduce evidence

1   that it was Christian who accessed the database on those occasions. Docket No. 135 at 12; Def.'s

2   Opp. at 3. In light of this disclosure, Judge Patel declined to dismiss those counts. Docket No. 135.

3   at 12. As noted above, the second superseding indictment amends these counts to include

4   allegations that Christian accessed the database on those occasions. SSI ¶ 19. As to count nine,

5   Judge Patel noted that the indictment specifically alleged that J.F. had logged onto the database and

6   then turned over access to M.J., who was then no longer a Korn/Ferry employee. *Id.* at 12-13; SI ¶¶

7   19o, 21. As this count specifically alleged database access by an individual without authorization,

8   Judge Patel denied the motion to dismiss this count. Docket No. 135 at 13.

9   C.   The Ninth Circuit's Decision in *Nosal*

10   The government appealed the dismissal of counts two and four through seven. On appeal,

11   the Ninth Circuit sitting en banc rejected the government's argument that this case is distinguishable

12   from *Brekka* because Korn/Ferry had an explicit policy forbidding use of the contents of the

13   Searcher database for purposes other than performing one's duties as a Korn/Ferry employee. 676

14   F.3d at 857-58. The court held "that 'exceeds authorized access' in the CFAA is limited to

15   violations of restrictions on *access* to information, and not restrictions on its *use*." *Id.* at 863-64. In

16   so holding, the court expressed concern that interpreting the CFAA to create criminal penalties for

17   violations of use agreements "would transform the CFAA from an anti-hacking statute into an

18   expansive misappropriation statute." *Id.* at 857. The court thus rejected the argument that an

19   individual could be liable for accessing a computer in excess of authorization when they had

20   permission to access the information on a computer, but did so for a purpose not condoned by the

21   relevant use agreement. *Id.*

22   The court noted that a related provision of the CFAA provided criminal penalties for

23   exceeding authorized access of a computer even without any culpable intent. *Id.* at 859. Allowing a

24   definition of "exceeds authorized access" that includes actions that violate use agreements (as

25   opposed to access restrictions) would create sweeping criminal liability for users of the numerous

26   websites and computer systems that have lengthy use agreements that often go unread by users. *Id.*

27   at 860-62. Since the court found that the plain language of the CFAA did not clearly create liability

28   for violations of use agreements, the rule of lenity precluded interpreting the law in such a way that

1 would create such sweeping liability. *Id.* at 863. Rather, a violation of the CFAA requires

2 unauthorized access (or access that exceeds authorization), not misuse of information after obtaining

3 authorized access. The court noted that the narrower interpretation of the phrase "exceeds

4 authorized access" is more consistent with the text of the statute, the legislative history, and the

5 purpose of the CFAA. *Id.* at 863-64.

6 D.   Application to Remaining CFAA Counts

7   1.   Defendant's Definition of Hacking

8   Defendant now argues that the Ninth Circuit's opinion in *Nosal* limits the applicability of the

9 CFAA to not just unauthorized access but to hacking crimes where the defendant circumvented

10 technological barriers to access a computer. Thus, Defendant argues, the remaining CFAA claims

11 must be dismissed because they do not include allegations that Defendant or his co-conspirators

12 circumvented any technological access barriers.

13   The Ninth Circuit acknowledged that the CFAA was passed "primarily to address the

14 growing problem of computer hacking." *Id.* at 858. The court further rejected the government's

15 argument that accessing a computer "without authorization" was intended to refer to hackers, while

16 accessing a computer in a way that "exceeds authorized access" necessarily refers to authorized

17 users who access a computer for an unauthorized purpose.

18   it is possible to read both prohibitions as applying to hackers:
"[W]ithout authorization" would apply to *outside* hackers (individuals

19   who have no authorized access to the computer at all) and "exceeds
authorized access" would apply to *inside* hackers (individuals whose

20   initial access to a computer is authorized but who access unauthorized
information or files). This is a perfectly plausible construction of the

21   statutory language that maintains the CFAA's focus on hacking rather
than turning it into a sweeping Internet-policing mandate.

22

23 *Id.* at 858 (emphasis in original). The court noted that the Defendant's "narrower interpretation [of

24 the CFAA] is also a more sensible reading of the text and legislative history of a statute whose

25 general purpose is to punish hacking – the circumvention of technological access barriers – not

26 misappropriation of trade secrets – a subject Congress has dealt with elsewhere." *Id.* at 863.

27   The court did not, however, explicitly hold that the CFAA is limited to hacking crimes, or

28 discuss the implications of so limiting the statute. For example, the court did not revisit the elements

1   of crimes under § 1030(a)(4) as articulated in *Brekka*, where it held the elements of a violation of

2   that provision were: (1) accessing a protected computer; (2) without authorization or exceeding such

3   authorization that was granted; (3) knowingly and with intent to defraud; and thereby (4) furthering

4   the intended fraud and obtaining anything of value. *Brekka*, 581 F.3d at 1132. Nowhere does the

5   court's opinion in *Nosal* hold that the government is additionally required to allege that a defendant

6   circumvented technological access barriers in bringing charges under § 1030(a)(4). Instead, *Nosal*

7   holds only that it is not a violation of the CFAA to access a computer with permission, but with the

8   intent to use the information gained thereby in violation of a use agreement. 676 F.3d at 863-64.

9   The court did not address limits on liability under the CFAA based on the *manner* in which access is

10   limited, whether by technological barrier or otherwise. *Id.* Thus, Defendant's interpretation is not a

11   fair reading of *Nosal* on this front is simply incorrect. Hacking was only a shorthand term used as

12   common parlance by the court to describe the general purpose of the CFAA, and its use of the phase

13   "circumvention of technological access barriers" was an aside that does not appear to have been

14   intended as having some precise definitional force.

15   Even if *Nosal* added a "circumventing technological access barriers" element to crimes under

16   § 1030(a)(4), the indictment sufficiently alleges such circumvention. As the government points out

17   "password protection is one of the most obvious technological access barriers that a business could

18   adopt." Gov.'s Opp. at 1. Faced with this reality, Defendant acknowledges that the Ninth Circuit

19   did not offer a definition of hacking, and urges this Court to look to the definition in the Digital

20   Millenium Copyright Act, which provides that to "'circumvent a technological measure' means to

21   descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove,

22   deactivate, or impair a technological measure, without the authority of the copyright owner." 17

23   U.S.C. § 1201(a)(3)(A). However, there is no legal basis to incorporate into the CFAA the Digital

24   Millenium Copyright Act which was passed 14 years after the CFAA and which concerned matters

25   separate and distinct from the CFAA.[3] Moreover, it is noteworthy that neither the CFAA nor the

26

27   [3] The CFAA is aimed at addressing various forms of computer-related crime, such as
     hacking. *See Nosal*, 676 F.3d at 858. The Digital Millenium Copyright Act creates various criminal

28   and civil penalties for circumventing copyright protection systems, including the circumvention of
     technological measures intended to protect copyrighted materials. 17 U.S.C. § 1201-1204.

United States District Court
For the Northern District of California

1 Digital Millenium Copyright Act employs the term "hacking." In any event, even if the Digital

2 Millenium Copyright Act's definition of "circumvent a technological measure" were to inform the

3 scope of the CFAA, as noted above, the actions alleged in the indictment fall within it. Use of

4 another's password "avoids" and "bypasses" the technological measure of password protection.

5   Defendant argues that the remaining CFAA claims fail because they do not allege "J.F.'s

6 password was obtained illegally or without her consent." Def.'s Mot. at 5. Defendant's argument is

7 premised in part on the notion that because J.F. allowed Defendant's co-conspirators to use her

8 credentials to access the Korn/Ferry system, the co-conspirators cannot be said to be acting "without

9 authorization" in accessing the Searcher database. In *Brekka*, however, the Ninth Circuit made clear

10 that it is the actions of the employer who maintains the computer system that determine whether or

11 not a person is acting with authorization. *Brekka*, 581 F.3d at 1135 ("The plain language of the

12 statute therefore indicates that 'authorization' depends on actions taken by the employer."). Further,

13 the CFAA appears to contemplate that one using the password of another may be accessing a

14 computer without authorization, as it elsewhere provides penalties for anyone who "knowingly and

15 with intent to defraud traffics in any password or similar information through which a computer may

16 be accessed without authorization." 18 U.S.C. § 1030(a)(6).[4]

17   Additionally, Defendant argues that the CFAA does not cover situations where an employee

18 voluntarily provides her password to another by analogizing to the law of trespass with regards to

19 physical property: "Just as consensual use of an employee's key to gain physical access is not

20 trespass, consensual use of an employee's computer password is not hacking." Def.'s Mot. at 6.

21 Defendant argues that the court in *Nosal* held that "the CFAA was based on principles of trespass."

22

23   [4] In support of his argument that there is no criminal liability under the CFAA because J.F.
willingly provided her access credentials, Defendant cites to an example given by the court in *Nosal*,
24 where the court, discussing the variety of terms to be found in use restrictions, notes that Facebook's
user agreement makes it a violation of terms to allow another person to log into your account.
25 *Nosal*, 676 F3d at 861. Besides constituting a mere example cited in dicta, that situation is
distinguishable from the circumstances here. First, in the case of Facebook, what is at issue is a use
26 restriction that restricts a user from giving their password to another person. Furthermore, allowing
such person to use one's password permits them to access the user's Facebook account containing
27 the user's personal account and information; it does not allow access to any Facebook trade secrets.
In the case at bar, what is being accessed by circumventing the password protection is Korn/Ferry's
28 trade secrets.

1 *Id.* This is a mischaracterization of the opinion in *Nosal*, which merely noted that the CFAA was

2 passed to address the growing problem of hacking, and quoted a Senate report that stated "[i]n

3 intentionally trespassing into someone else's computer files, the offender obtains at the very least

4 information as to how to break into that computer system." *Nosal*, 676 F.3d at 858 (quoting S.Rep.

5 No. 99–432, at 9 (1986), 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.)). Aside from these passing

6 comments positing an analogy, Defendant points to nothing in the wording of the CFAA or

7 interpretive case law to support its construction. If the CFAA were not to apply where an authorized

8 employee gave or even sold his or her password to another unauthorized individual, the CFAA could

9 be rendered toothless. Surely, Congress could not have intended such a result.

10   2.   "Access"

11   The factual scenario presented in count nine, does, however, raises the question of how to

12 interpret the term "access" in the CFAA. Defendant argues that J.F. was the individual "accessing"

13 the Korn/Ferry system when she logged in using her password, and that M.J.'s use of the system

14 *after* the login does not constitute unauthorized "access" within the meaning of the statute. The

15 government, on the other hand, argues that "access" encompasses ongoing use, including M.J.'s

16 unauthorized use of the system after J.F. logged in.

17   In support of its argument, the government cites to two Senate Reports from the CFAA's

18 legislative history. The first, from the 1996 amendments to the CFAA, notes that "the term

19 'obtaining information' includes merely reading it." Sen. Rep. No. 104-357, at 7 (1996). The

20 government argues that just as "obtaining information" may include merely reading, so too may

21 access be as simple as reading the materials in question.[5] The second Senate Report, associated with

22

23   [5] The full context for the quote is:

24   "Information" as used in this subsection includes information stored in
        intangible form. Moreover, the term ''obtaining information'' includes

25   merely reading it. There is no requirement that the information be
        copied or transported. This is critically important because, in an

26   electronic environment, information can be "stolen" without
        asportation, and the original usually remains intact. This interpretation

27   of "obtaining information" is consistent with congressional intent
        expressed as follows in connection with 1986 amendments to the

28   Computer Fraud and Abuse statute:

the 1986 version of the CFAA, notes the intention to criminalize "knowingly trafficking in other

people's computer passwords." Sen. Rep. No. 99-432, at 3 (1986). This comment, however, seems

to be in reference to § 1030(a)(6) of the CFAA, which criminalizes trafficking in passwords, and is

not at issue in the current case. *See id.* at 13.

The Court need not opine on whether § 1030(a)(4) should be read so broadly as to

encompass the situation where an unauthorized person looks over the shoulder of the authorized user

to view password protected information or files. The allegation in Count Nine is that J.F. logged on

to the computer using her credentials, then handed over the computer terminal to M.J., who ran his

own searches through the Korn/Ferry database and then downloaded files therefrom.

Functionally and logically, this is no different than if J.F. gave M.J. the password, and M.J.

typed in the password himself. The only distinction differentiating the two scenarios is one based on

a constrained and hypertechnical definition of "access" in which access focuses solely on the

moment of entry and nothing else. Not only would such a definition produce a non-sensical result; it

is not supported by the language of the statute. The crime under § 1030(a)(4) is "accessing" a

protected computer, or not "entering" or "logging on to" a protected computer. 18 U.S.C. §

1030(a)(4). Nothing in the CFAA suggests anything other than a common definition of the term

"access," applies. The Oxford English Dictionary defines "access" as, *inter alia*, "[t]he opportunity,

means, or permission to gain entrance to *or use* a system, network, file, etc." *See* Oxford English

Dictionary, www.oed.com (emphasis added); *see also* Black's Law Dictionary (defining access as,

inter alia, "[a]n opportunity or ability to enter, approach, pass to and from, or communicate with").

The common definition of the word "access" encompasses not only the moment of entry, but also

the ongoing use of a computer system. Under the facts alleged in the indictment, M.J. "proceeded to

---

Because the premise of this subsection is privacy
protection, the Committee wishes to make clear that
'obtaining information' in this context includes mere
observation of the data. Actual asportation, in the sense
of physically removing the date from its original
location or transcribing the data, need not be proved in
order to establish a violation of this subsection.

Sen. Rep. No. 104-357, at 7 (1996) (quoting Sen. Report No. 99–432, at 6–7 (1986)).

1 query Korn/Ferry's Searcher database and download information, after obtaining initial access." SI

2 ¶ 19o. That J.F. entered the password for him rather than having M.J. type it himself does not alter

3 the fact that in common parlance and in the words of the CFAA, M.J. accessed the protected

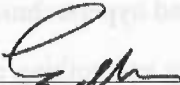4 computer system, and he did not have authorization to do so.[6]

IV.   CONCLUSION

6 For the foregoing reasons, Defendant's motion to dismiss the third, eighth, and ninth counts

7 of the first superseding indictment is **DENIED**.[7]

8 This order disposes of Docket Nos. 274 and 276.

10 IT IS SO ORDERED.

12 Dated: March 12, 2013

13

14 EDWARD M. CHEN
   United States District Judge

---

23 [6] In his motion, Defendant also argued that the third and eighth counts must be dismissed because the first superseding indictment did not specify who used the Searcher database to download information. The second superseding indictment, however, has remedied this problem by alleging that Christian was the person who accessed the database on both occasions, and that she did so without authorization. SSI ¶ 19. Though the second superseding indictment does not allege who logged into the Korn/Ferry system with respect to count eight, it does allege that it was Christian who ran the queries in the database. For the reasons discussed above with respect to count nine, this is sufficient to allege that Christian accessed the database without authorization, and thus to state a violation of the CFAA.

[7] As noted above, the third, eighth, and ninth counts of the first superseding indictment correspond to the third, fourth, and fifth counts of the second superseding indictment.

United States District Court
For the Northern District of California