

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
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

KONINKLIJKE PHILIPS N.V., et al.,

Plaintiffs,

v.

ELEC-TECH INTERNATIONAL CO.,
LTD., et al.,

Defendants.

Case No. [14-cv-02737-BLF](#)

ORDER ON MOTIONS TO DISMISS

[Re: ECF 34, 35, 36]

Plaintiffs Koninklijke Philips N.V. (“Philips”) and Philips Lumileds Lighting Company LLC (“Lumileds”) bring suit against eleven Defendants, including a Chinese-based competitor, Elec-Tech International Co. (“ETI”), seven of ETI’s subsidiaries, two corporate directors (Mr. Donglei Wang and Ms. Eva Chan), and a former Lumileds employee, Dr. Gangyi Chen, currently employed by ETI.

This case involves the global market for Light Emitting Diode (“LED”) technology. In general terms, Plaintiffs’ suit alleges that Dr. Chen, while still an employee at Lumileds, downloaded thousands of files “containing Philips Lumileds’ trade secrets and confidential business information onto a portable storage device.” Complaint, ECF 1 ¶ 5. Dr. Chen then began working for ETI in China. Plaintiffs allege that only six months after Dr. Chen began at ETI, the company announced two new high-energy LED lighting products, an amount of time Plaintiffs claim is “unprecedented” in the lighting industry. *See, e.g.*, Compl. ¶ 62. Plaintiffs allege ten causes of action, nine of which arise out of state law. Plaintiffs also plead a single federal cause of action, based on a purported violation of the Computer Fraud and Abuse Act (“CFAA”).

Defendants move to dismiss on a number of grounds: most salient for purposes of this order is Defendants’ contention that Plaintiffs have failed to state a claim under the CFAA, and

1 that the Court should dismiss this CFAA claim and decline to exercise supplemental jurisdiction
2 over Plaintiffs' pendent state law claims. The Court ultimately agrees with Defendants, and for the
3 reasons stated below DISMISSES this case, with prejudice.

4 **I. BACKGROUND**

5 **A. Procedural History and the Motions to Dismiss**

6 Plaintiffs filed their Complaint on June 12, 2014. Defendants then filed three motions to
7 dismiss under Federal Rule of Civil Procedure 12(b), pursuant to a stipulation between the parties:
8 a motion to dismiss for lack of subject matter jurisdiction, based on a lack of diversity between the
9 parties as well as a failure to adequately plead a federal claim; a partial motion to dismiss, on
10 behalf of seven of the eleven Defendants, for lack of personal jurisdiction; and a partial motion to
11 dismiss nine of the ten causes of action for failure to state a claim upon which relief can be
12 granted.¹ Plaintiffs opposed all three motions, but withdrew their assertion of diversity
13 jurisdiction. *See* ECF 84-6 at 8-9 ("Plaintiffs have chosen to withdraw their reliance on diversity
14 as a basis for federal jurisdiction."). Plaintiffs argued that the Court nonetheless had subject matter
15 jurisdiction over this case because the Complaint stated a claim under the CFAA, and that the
16 Court could exercise supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28
17 U.S.C. § 1367.

18 At the outset, the Court must decide the appropriate order in which to adjudicate
19 Defendants' arguments presented in the Rule 12 motions. Though Defendants filed three motions,
20 Plaintiffs' withdrawal of their diversity jurisdiction argument really leaves the Court with two: a
21 partial Rule 12(b)(6) motion, which if granted as to the CFAA claim then requires the Court to
22 determine whether it will decline to exercise its discretion to retain Plaintiffs state law claims; and
23 a Rule 12(b)(2) motion for lack of personal jurisdiction as to seven of the Defendants.

24 In the normal course, the Court would determine personal jurisdiction before reaching the
25 Rule 12(b)(6) motion. In this circuit, however, the Court may "assume the existence of personal
26 jurisdiction and adjudicate the merits in favor of the defendant without making a definitive ruling
27

28 ¹ Defendants did not move to dismiss the fifth cause of action, for breach of contract.

1 on jurisdiction.” *See Lee v. City of Beaumont*, 12 F.3d 933, 937 (9th Cir. 1993) *overruled on other*
2 *grounds by Calif. Dep’t of Water Resources v. Powerex Corp.*, 533 F.3d 1087 (9th Cir. 2008). In
3 *Lee*, the Ninth Circuit found that the district court could assume personal jurisdiction in order to
4 reach the question of whether to dismiss the federal claims asserted against the defendant. 12 F.3d
5 at 937-38. In this case, because the Court determines below that Plaintiffs have not—and cannot—
6 plead a CFAA claim, the Court assumes without deciding that it has personal jurisdiction over all
7 eleven Defendants. *See Sameena, Inc. v. U.S. Air Force*, 147 F.3d 1148, 1152 n.1 (9th Cir. 1998).

8 **B. Factual Background**

9 The facts below are pled in the Complaint, and are presumed true for purposes of
10 adjudicating the Rule 12(b)(6) motion to dismiss.

11 Dr. Chen worked as a principal development engineer at Lumileds’ headquarters in San
12 Jose, California, from 2005 through 2012. In 2011, he began discussions with Mr. Wang about
13 joining ETI. On June 22, 2012, he terminated his employment with Lumileds and, thereafter,
14 began working at ETI. Compl. ¶¶ 5, 58. Between June 15 and June 22, 2012, Dr. Chen used a
15 computer at Lumileds’ offices “to copy several thousand files from its secure networks[,]”
16 contain[ing] information about Philips Lumileds’ proprietary epitaxy technology used in
17 developing its LEDs, as well as other confidential business information.” Compl. ¶ 55. Dr. Chen
18 traveled to China, began working for ETI, and disclosed trade secret information regarding
19 Lumileds’ proprietary epitaxy technology to Defendants. Compl. ¶ 59.

20 In the Complaint, Plaintiffs asserted their CFAA claim against five Defendants: ETI, ETI
21 International (H.K.) Co., Ltd. (“ETI-HK”), Mr. Wang, Ms. Chan, and Dr. Chen. In their
22 opposition to the motion to dismiss, and again at oral argument, Plaintiffs conceded their CFAA
23 claim against Dr. Chen. *See, e.g.*, ECF 84-6 at 7 (“ETI, ETI HK, Wang, and Chan *themselves* were
24 not authorized to access Lumileds’ network, and Plaintiffs are not tying their liability under the
25 statute to Chen’s.”) (emphasis in original). Plaintiffs allege that ETI, ETI-HK, Mr. Wang, and Ms.
26 Chan violated the CFAA by accessing Lumileds’ network “through their agent, defendant Chen,”
27 because they themselves were not permitted to access Lumileds’ network. Compl. ¶¶ 145, 147,
28 149. They argue that this “indirect access interpretation [of the CFAA] does not implicate current

1 employees otherwise permitted to access their employer’s computer (in this case Chen).” ECF 84-
2 6 at 7.

3 Essentially, Plaintiffs argue that, though Dr. Chen himself was authorized to access
4 Lumileds’ network, and did not exceed his authorized access while downloading information prior
5 to his resignation, the other four Defendants implicated in the CFAA claim should be held liable
6 based on their indirect, unauthorized access of the Lumileds’ network *through* Dr. Chen’s actions.

7 **II. LEGAL STANDARD**

8 A motion to dismiss under Rule 12(b)(6) concerns what facts a plaintiff must plead on the
9 face of its claim. Under Rule 8(a)(2) of the Federal Rules of Civil Procedure, a complaint must
10 include “a short and plain statement of the claim showing that the pleader is entitled to relief.”
11 Any complaint that does not meet this requirement can be dismissed pursuant to Rule 12(b)(6). In
12 interpreting Rule 8(a)'s “short and plain statement” requirement, the Supreme Court has held that a
13 plaintiff must plead “enough facts to state a claim to relief that is plausible on its face,” *Bell Atl.*
14 *Corp. v. Twombly*, 550 U.S. 544, 570 (2007), which requires that “the plaintiff plead factual
15 content that allows the court to draw the reasonable inference that the defendant is liable for the
16 misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). This standard does not ask a
17 plaintiff to plead facts that suggest it will probably prevail, but rather “it asks for more than a sheer
18 possibility that a defendant has acted unlawfully.” *Id.* (internal quotation marks omitted).

19 **III. DISCUSSION**

20 Though Plaintiffs present a number of claims against the various Defendants, the Court’s
21 task here is a fairly limited one: it must determine whether Plaintiffs have stated a claim against
22 any Defendant under the CFAA, and if not, whether Plaintiffs could amend to state a claim under
23 this circuit’s interpretation of the CFAA.

24 The CFAA was enacted in 1984 as a criminal statute, designed to prohibit various
25 computer crimes related to accessing computers without authorization in order to obtain
26 information or data. In 1994, Congress amended the statute to add a civil provision, exposing
27 violators of the statute to both civil and criminal liability. *See* 18 U.S.C. § 1030(c)(4)(A). Plaintiffs
28 allege violations of three provisions of the Act: Sections (a)(2)(C) and (a)(4), which prohibit

1 individuals from “exceed[ing] authorized access” to a computer, or otherwise “access[ing] . . .
 2 without authorization” a computer; and Section (a)(5), which similarly prohibits a person from
 3 “intentionally access[ing] a protected computer without authorization.” The statute itself defines
 4 “exceeds authorized access” to mean “to access a computer with authorization and to use such
 5 access to obtain or alter information in the computer that the accesser is not entitled so to obtain or
 6 alter.” 18 U.S.C. § 1030(e)(6). Courts interpreting the CFAA describe the Act as “an anti-hacking
 7 statute.” *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (“The government agrees that
 8 the CFAA was concerned with hacking, which is why it also prohibits accessing a computer
 9 ‘without authorization.’”); *see also Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D.
 10 Ariz. 2008) (“The general purpose of the CFAA was to create a cause of action against computer
 11 hackers.”); *see also WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012).

12 Two Ninth Circuit cases, *United States v. Nosal* and *LVRC Holdings LLC v. Brekka*, define
 13 narrowly the phrases “exceeds authorized access” and “without authorization.” *Brekka*, a civil
 14 case, outlines what it calls “a sensible interpretation of §§ 1030(a)(2) and (4)”:

15 [A] person who “intentionally accesses a computer without
 16 authorization,” §§ 1030(a)(2) and (4), accesses a computer without
 17 any permission at all, while a person who “exceeds authorized
 18 access,” *id.*, has permission to access the computer, but accesses
 19 information on the computer that the person is not entitled to access.

20 *Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).

21 The Ninth Circuit further explicated this interpretation of the language of the CFAA in
 22 *Nosal*, an en banc decision from 2012. The facts of *Nosal*, a criminal case, are relatively
 23 straightforward. David Nosal worked at Korn/Ferry, an executive search firm. He left Korn/Ferry
 24 to start a competing business, and, after leaving, convinced several current Korn/Ferry employees
 25 to access Korn/Ferry’s computers and “download source lists, names and contact information from
 26 a confidential database . . . then transfer[] the information to Nosal.” *Nosal*, 676 F.3d at 856. The
 27 employees who were accused of accessing the information were authorized to access the database
 28 in question. *See id.* Mr. Nosal was criminally charged under § 1030(a)(4)—one of the three
 provisions at issue in this suit—for aiding and abetting the Korn/Ferry employees in “exceeding
 their authorized access with intent to defraud.” *Id.*

1 The government asked the Ninth Circuit to broadly read the CFAA to include not only a
2 person who accesses information without authorization, but also a person authorized to access the
3 information but who “is limited in the use to which he can put that information.” *Nosal* at 857.
4 Engaging in detailed statutory interpretation, the Ninth Circuit expressly rejected such a reading,
5 stating that “[t]he government’s interpretation would transform the CFAA from an anti-hacking
6 statute into an expansive misappropriation statute.” *Id.* at 857; *see also id.* at 859 (“The
7 government’s construction of the statute would expand its scope far beyond computer hacking to
8 criminalize *any unauthorized use of information obtained from a computer.*”) (emphasis added).
9 Ultimately, it determined that “the plain language of the CFAA targets the unauthorized
10 procurement or alternation of information, not its misuse or misappropriation.” *Id.* at 863.

11 Here, it is undisputed that Dr. Chen was authorized to access the information he allegedly
12 stole from Lumileds. Plaintiffs therefore cannot plead a cause of action under the CFAA unless at
13 least one of ETI, ETI-HK, Mr. Wang, or Ms. Chen (hereinafter the “CFAA Defendants”)
14 themselves violated the CFAA. Plaintiffs argue that the CFAA Defendants “accessed” Lumileds’
15 information through Dr. Chen *as their agent* – essentially that Dr. Chen, though himself
16 authorized to access the data, was a conduit by which the CFAA Defendants engaged in their own
17 unauthorized access. *See, e.g.*, ECF 84-6 at 7-8 (arguing that ETI should be liable under the CFAA
18 “when [it] unlawfully induce[s] an ‘insider’ to give [it] access to a secure computer network”).

19 This indirect access theory of CFAA liability suffers from several problems. First,
20 Plaintiffs have provided no factual pleading regarding agency, instead making a cursory allegation
21 that Dr. Chen “act[ed] as an agent of ETI, ETI HK, Wang, and Chan.” Compl. ¶ 55. Second, even
22 a well-pled agency allegation would leave the Plaintiffs no closer to stating a claim under the
23 CFAA with regard to any of these four Defendants, because *Nosal* forecloses this form of indirect
24 access liability under the CFAA. *Nosal* explicitly cautions that the CFAA was designed to target
25 hacking, not misappropriation. *See, e.g.*, 676 F.3d at 857. The only reasonable reading of this
26 statutory interpretation is that CFAA violations require a person to engage in the hacking, not
27 merely benefit from its results.

28 *Dresser-Rand Co. v. Jones*, a case from the Middle District of Pennsylvania which adopted

1 the Ninth Circuit’s reasoning in *Nosal*, is instructive. 957 F. Supp. 2d 610 (E.D. Pa. 2013). In
2 *Dresser-Rand*, an company brought suit against three individuals for violations of the CFAA: two
3 former employees, King and Jones, and the president of a competitor, Wadsworth. King and Jones
4 were alleged to have accessed information via their Dresser-Rand laptops – information they were
5 both authorized to access. *See id.* at 621. They downloaded files and sent them to Wadsworth, who
6 “viewed and edited [the] documents on his own computer.” *Id.* at 615. Though Wadsworth himself
7 was not authorized to access the documents, he did not run afoul of the CFAA because “he never
8 accessed Dresser-Rand computers, as required under the CFAA.” *Id.* The district court found that
9 “Dresser-Rand provide[d] no legal basis in the CFAA or otherwise to justify imputing liability
10 from the individuals who access a computer without authorization to those who may eventually
11 benefit from their actions.” *Id.*

12 Plaintiffs here make no allegation that either Mr. Wang or Ms. Chan was given Dr. Chen’s
13 password and then ran searches, nor do they allege that either individual Defendant in any way
14 accessed or downloaded information from Lumileds’ network. By the Complaint’s own
15 allegations, none of the CFAA Defendants accessed Lumileds’ information—Dr. Chen did, at a
16 time when he was authorized to download this information. Even if he misappropriated the
17 information, and gave it to the CFAA Defendants, *Nosal* forecloses a claim against those
18 Defendants under the CFAA because they themselves did not hack Lumileds’ system. Plaintiffs’
19 argument that Dr. Chen and the CFAA Defendants were essentially “acting as one” for purposes
20 of accessing the files does not save Plaintiffs’ CFAA claim. Rather, it shows that this case is
21 factually quite similar to *Nosal*: it is alleged that outsiders convinced an insider to access
22 information the insider was authorized to access, then hand that information over to the outsiders.
23 While such allegations could possibly state a claim for misappropriation, they cannot state a claim
24 under the CFAA after *Nosal*. Reading the CFAA in its context as an anti-hacking statute, “access”
25 means something more than persuading someone to procure information you desire. Instead, as
26 described by the district court in *Nosal II*, “[t]he common definition of the word ‘access’
27 encompasses not only the moment of entry, but also the ongoing use of a computer system.” *Nosal*
28 *II*, 930 F. Supp. 2d 1051, 1063 (N.D. Cal. 2013). None of the CFAA Defendants entered or used

1 Lumileds’ network. At most, they encouraged Dr. Chen to do so, and stood to benefit from the
2 alleged misappropriation. This action may give rise to a number of claims, but it does not support
3 a theory of liability under the CFAA.²

4 Plaintiffs also argue that *Nosal II*, decided on remand after *Nosal*, compels the Court to
5 reach a different result because the district court there “denied a motion to dismiss where the
6 government alleged that defendant, after leaving Korn/Ferry, accessed a Korn/Ferry computer
7 through a current Korn/Ferry employee who logged in and gave him access.” ECF 77 at 10. In
8 *Nosal II*, however, the facts were quite different than they are here: an employee who was
9 authorized to access Korn/Ferry’s network logged into the company’s computer system and then
10 “turned the computer over” to another individual who was not authorized to access the system.
11 That unauthorized user then “proceeded to query Korn/Ferry’s Searcher database and download
12 information.” 930 F. Supp. 2d 1051, 1056, 1063. Thus, in *Nosal II*, the unauthorized user did not
13 merely view information given to him by the authorized user, he himself *physically engaged in the*
14 *hacking*. Here, Plaintiffs make no allegation that Mr. Wang or Ms. Chan physically accessed the
15 computer, only that Dr. Chen did so as their agent. *Nosal II* expressly declined to extend its
16 holding to the situation where “an unauthorized person looks over the shoulder of the authorized
17 user to view password protected information,” *id.* at 1062, and did not in any way hold that an
18 agency theory of liability, such as the one Plaintiffs proffer here, was viable under the CFAA.

19 At oral argument, Plaintiffs contended that they could amend in order to plead several facts
20 that they believed would permit them to state a CFAA claim – namely, that at the time Dr. Chen
21 accessed the Lumileds data he had been paid a substantial monetary bonus by ETI and was
22 effectively already working for that company. Plaintiffs argue that this situation is analogous to
23 ETI sending its own employee into Lumileds, unauthorized, to access the network. For the sake of
24

25 ² Similarly, Plaintiffs argue that *Nosal* was only charged with aiding and abetting liability under
26 the CFAA, and that the Ninth Circuit has therefore “not addressed the indirect access
27 interpretation” of the CFAA. *See* ECF 77 at 9 n.3. The Ninth Circuit, however, makes clear in
28 *Nosal* that there is a crucial distinction between one who accesses unauthorized information and
one who ultimately receives the information so accessed – the accesser can be held liable under
the CFAA, while the beneficiary cannot if he did not himself access the computer. *Nosal* at 863.
Nosal is fairly read to cover Plaintiffs’ indirect access interpretation, and this Court holds that
Plaintiffs’ argument is inconsistent with both the plain language and purpose of the CFAA.

1 determining whether Plaintiffs could feasibly state a claim under the CFAA if given the chance to
2 amend, the Court considers whether these facts bring Plaintiffs any closer to stating a viable claim.
3 They do not, for two reasons. First, if Dr. Chen signed a contract to later begin employment with
4 ETI, and even if he had already been partially compensated to join the company, it would not have
5 rendered his access of Lumileds' confidential information "unauthorized." Employees regularly
6 leave their companies after signing a new employment contract with their soon-to-be employers.
7 That new contract, even if money exchanges hands prior to the employee's ultimate resignation
8 from his or her current company, does not terminate the existing employer-employee relationship.
9 If Dr. Chen had been stripped of his badge and password, then snuck into Lumileds to download
10 information he was no longer authorized to access, Plaintiffs could state a claim against him under
11 the CFAA. That situation is not present here. Second, even if Dr. Chen was working on ETI's
12 behalf, the liability of ETI, ETI-HK, Mr. Wang, and Ms. Chan relies on Plaintiffs' agency theory.
13 Even if this theory were sufficiently pled, the Court has, for the reasons stated above, found it
14 foreclosed in this circuit after *Nosal*.³

15 If the Court accepted Plaintiffs' argument here, that the mere pleading of an agency
16 relationship between the insider and an outsider could render the outsider subject to liability under
17 the CFAA, it would effectively federalize all trade secret misappropriation cases where parties use
18 a computer to download sensitive or confidential trade secret information – which would be nearly
19 every trade secret case nowadays, when companies maintain their files electronically rather than in
20

21 ³ Plaintiffs point to two cases from the Middle District of Pennsylvania, *Binary Semantics Ltd. v.*
22 *Minitab, Inc.*, 2008 WL 763575 (M.D. Pa. Mar. 20, 2008) and *Advanced Fluid Systems, Inc. v.*
23 *Huber*, 28 F. Supp. 3d 306, 327 (M.D. Pa. 2014), and argue that these cases compel the Court to
24 reach a different result. Though these out-of-district cases are not binding on this Court, nor are
25 they even persuasive given the clear direction from the Ninth Circuit in *Nosal*, at least one is
26 distinguishable: in *Huber*, the Complaint alleged that the defendant "continued to unlawfully
27 access [plaintiff's] information through his company-issued laptop *subsequent to leaving his*
28 *employment.*" *Huber* at 329 (emphasis added). Thus, *Huber* contained allegations that the
defendant exceeded his authorized access which are not present here. In *Binary Semantics*, it is
unclear whether the plaintiff pled that the individual who accessed the files was unauthorized to do
so, thus the Court cannot ascertain whether it is factually distinct from this case. *See Binary*
Semantics at *2 ("Plaintiff further alleges that Menon took confidential and proprietary
information from Binary at Minitab's direction and gave it to Minitab."). Though the Third Circuit
is silent on this question, at least one other district court in Pennsylvania has adopted *Nosal*'s
narrow reading of the CFAA. *See Dresser-Rand*, 957 F. Supp. 2d at 619-21.


1 physical cabinets. Plaintiffs are really making a policy argument better directed to Congress
2 instead of this Court, which must follow the clear direction from the Ninth Circuit as to who can
3 and cannot be held liable under the CFAA. *See Nosal* at 863 (“If Congress wants to incorporate
4 misappropriation liability into the CFAA, it must speak more clearly.”).⁴

5 The Court therefore DISMISSES Plaintiffs’ CFAA claim against Defendants Dr. Chen,
6 ETI, ETI-HK, Mr. Wang, and Ms. Chan. Because the Court finds, for the reasons proffered above,
7 that Plaintiffs’ proposed amendments would not cure the CFAA claim’s deficiencies, this
8 dismissal is with prejudice. *See Lopez v. Smith*, 203 F.3d 1122, 1128 (9th Cir. 2000) (declining to
9 grant leave to amend when such amendment would be futile). In light of the Court’s dismissal of
10 the CFAA claim, Plaintiffs’ Complaint lacks a federal cause of action. “When the single federal-
11 law claim in the action was eliminated at an early stage of the litigation, the District Court had a
12 powerful reason to choose not to continue to exercise jurisdiction.” *Carnegie-Mellon Univ. v.*
13 *Cohill*, 484 U.S. 614, 619 (1988). For reasons of comity and efficiency, *see id.*, the Court declines
14 to exercise supplemental jurisdiction over Plaintiffs’ state law claims under 28 U.S.C. § 1367.⁵

15 **IV. ORDER**

16 For the foregoing reasons, this action is DISMISSED, with prejudice.

17 Dated: March 20, 2015

18 
19 BETH LABSON FREEMAN
20 United States District Judge

21
22
23
24

25 ⁴ The Court recognizes that the various circuits are split on this question: while the Ninth and
26 Fourth Circuits read the CFAA narrowly, the Fifth, Seventh, and Eleventh adopt, in varying
degrees, a broader view of the CFAA’s ambit. *See Nosal* at 862 (compiling cases).

27 ⁵ This Court leaves the personal jurisdiction determination to the state court that will fully
28 adjudicate these claims. Thus, no decision on Defendants’ motion to dismiss for lack of personal
jurisdiction is rendered here, and that motion is terminated. ECF 36.