IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge William J. Martínez

Civil Action No. 15-cv-0485-WJM-KLM

CLOUDPATH NETWORKS, INC., a Colorado corporation,

Plaintiff,

v.

SECUREW2 B.V., a Dutch corporation,
SECUREW2, INC., a Washington corporation,
JEFFREY GRIMM,
ROGER “LYNN” HANEY,
BHARAT RAM “BERT” KASHYAP, and
BASZ UNIVERSAL, LLC, a Washington limited liability company,

Defendants.

ORDER DENYING SECUREW2 B.V.’S RULE 12(b)(2) MOTION TO DISMISS AMENDED COMPLAINT, AND GRANTING IN PART AND DENYING IN PART ALL DEFENDANTS’ RULE 12(b)(6) MOTION TO DISMISS AMENDED COMPLAINT

Plaintiff Cloudpath Networks, Inc. (“Cloudpath”) sues various parties (collectively, “Defendants”) for numerous causes of action related to alleged theft and misuse of Cloudpath’s trade secrets. (*See* ECF No. 37 (First Amended Complaint) (“FAC”).) Currently before the Court is Defendant SecureW2 B.V.’s Motion to Dismiss Amended Complaint, arguing that this Court lacks personal jurisdiction over it (“Rule 12(b)(2) Motion”). (ECF No. 58.) Also before the Court is the remaining Defendants’ Motion to Dismiss Amended Complaint, arguing that Cloudpath has failed to state a claim against them (“Rule 12(b)(6) Motion”). (ECF No. 40.) SecureW2 B.V. joins this motion to the extent its Rule 12(b)(2) Motion fails. (ECF No. 58 at 15.)[1]

For the reasons explained below, the Court denies SecureW2 B.V.'s Rule 12(b)(2) Motion, finding that factual questions preclude a personal jurisdiction determination at this stage. The Court grants in part and denies in part the Rule 12(b)(6) Motion, dismissing with prejudice Cloudpath's claims under the Electronic Communications Privacy Act and Stored Communications Act, and dismissing with prejudice in part Cloudpath's claims under the Computer Fraud and Abuse Act.

I. FACTS

Unless otherwise noted, the Court assumes the following allegations to be true for present purposes.

Cloudpath is a Colorado company that develops software permitting "users with mobile computing devices to connect seamlessly to secure networks via Wi-Fi or wired connections." (ECF No. 37 ¶¶ 6, 21–22.) In essence, Cloudpath is in the business of assisting organizations to enable secure network access on devices brought from outside the organization (such as an employee's smartphone or a student's laptop).

Beginning in October 2008, Defendant Kashyap and/or his wholly owned LLC, Defendant Basz Universal (collectively, "Kashyap"), became an independent sales representative for Cloudpath (*i.e.*, a non-employee sales agent). (*Id.* ¶ 36.) In exchange for contractual agreements to maintain the confidential and proprietary nature of Cloudpath's trade secrets and to work exclusively on Cloudpath's behalf when it comes to selling and marketing software of the kind Cloudpath creates, Cloudpath

[1] All ECF page citations are to the page number in the ECF header, which does not always match the document's internal pagination.

granted Kashyap access to its trade secrets, including through login credentials to Cloudpath's secure servers. (*Id.* ¶¶ 37–40, 54.)

Kashyap was also an independent sales representative for SecureW2 B.V. ("SecureW2"), a Dutch company that did not, at that time, have a competing product. (*Id.* ¶¶ 7, 51–52.) SecureW2 was, rather, "a co-marketing and co-sales partner" with Cloudpath, and had executed a non-disclosure agreement, agreeing to protect Cloudpath's confidential information. (*Id.* ¶ 49.)

As discussed further in Part II.B.1, below, the parties dispute the scope of this non-disclosure agreement. In any event, as early as January 2012, Kashyap and SecureW2 allegedly began conspiring to steal Cloudpath's trade secrets and thereby develop a competing product. (*Id.* ¶¶ 53, 56.) SecureW2 indeed launched a competing product in June 2012. (*Id.* ¶ 61.) Kashyap then notified Cloudpath that he was no longer associated with SecureW2, but he surreptitiously continued the conspiracy, including through allowing SecureW2 to use his Cloudpath login credentials to access Cloudpath's proprietary information. (*Id.* ¶¶ 54–63.) Kashyap also began promoting SecureW2's product when approached by potential customers interested in Cloudpath's product. (*Id.* ¶¶ 64–66.)

Kashyap ended his relationship with Cloudpath in March 2013. (*Id.* ¶ 67.) Just before his departure, he tried to erase his Cloudpath e-mail account, although he was only partially successful. (*Id.*) In May 2014, Kashyap caused the incorporation of Defendant SecureW2, Inc. ("SecureW2-USA"), a Washington corporation and a wholly-owned subsidiary of SecureW2. (*Id.* ¶¶ 3, 50, 71.)

Also in 2014, Kashyap and the SecureW2 entities managed to convince two Cloudpath employees, Defendants Grimm and Haney, to assist SecureW2 in its efforts to compete with Cloudpath. (*Id.* ¶ 73.) In September 2014 or thereabouts, Grimm began preparing to leave Cloudpath for SecureW2-USA. (*Id.* ¶ 75.) As part of his preparations, he downloaded substantial amounts of proprietary information and software code, deleted and corrupted sales leads and customer information, and deleted his Cloudpath e-mail account. (*Id.* ¶¶ 77–78, 80–81.) He resigned abruptly on January 5, 2015, explaining that "he was starting employment at an oil and gas software company" the next day. (*Id.* ¶ 82.) Instead, he began working for SecureW2-USA the next day (January 6), but continued to use his Cloudpath login credentials to access Cloudpath proprietary information on January 6 and 7. (*Id.* ¶¶ 84–86.)

Haney was pursuing a similar course at this time. According to the FAC, he intentionally sabotaged Cloudpath's software bug reporting system and "launched a software program within the Cloudpath computer system for the express purpose of creating an unauthorized rogue wireless network that would allow surreptitious and unauthorized access." (*Id.* ¶¶ 87–91.) He also gathered "all of Cloudpath's customer account information" from which he could "generate contact lists." (*Id.* ¶ 92.) Like Grimm, Haney resigned on January 5, 2015, and then went to work for SecureW2-USA. (*Id.* ¶¶ 87, 97.)

Cloudpath has lost at least twenty-six customers to SecureW2 or its affiliates on account of Defendants' conduct. (*Id.* ¶ 161.) It has also incurred expenses "to investigate the activities of Grimm and Haney prior to their resignation[s], and to analyze their computer systems revealing the activities [described] above." (*Id.* ¶ 101.)

II. RULE 12(b)(2) ANALYSIS

A. Legal Standard

The purpose of a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(2) is to test whether the Court has personal jurisdiction over the named parties. The Tenth Circuit has established a two-part test for personal jurisdiction: "First, we ask whether any applicable statute authorizes service of process on defendants. Second, we examine whether the exercise of statutory jurisdiction comports with constitutional due process demands." *Dudnikov v. Chalk & Vermillion Fine Arts, Inc.*, 514 F.3d 1063, 1070 (10th Cir. 2008). "In a federal question case . . . [where] the federal statute at issue does not authorize nationwide service, personal jurisdiction is determined according to the law of the forum state." *Impact Prods., Inc. v. Impact Prods., LLC*, 341 F. Supp. 2d 1186, 1189 (D. Colo. 2004).

Colorado's long-arm statute "confers the maximum jurisdiction permissible consistent with the Due Process Clause." *Archangel Diamond Corp. v. Lukoil*, 123 P.3d 1187, 1193 (Colo. 2005) (citing Colo. Rev. Stat. § 13-1-124). Thus, the Court need only address the constitutional question of whether the exercise of personal jurisdiction over the relevant defendant comports with due process. *Dudnikov*, 514 F.3d at 1070 (noting that the inquiry into whether any statute authorizes service of process "effectively collapses into the second, constitutional, analysis" in Colorado).

The plaintiff bears the burden of establishing personal jurisdiction over a defendant. *Behagen v. Amateur Basketball Ass'n*, 744 F.2d 731, 733 (10th Cir. 1984).

When the district court does not hold an evidentiary hearing before ruling on jurisdiction, "the plaintiff need only make a *prima facie* showing" of personal jurisdiction to defeat a motion to dismiss. *Id.* A *prima facie* showing is made where the plaintiff has demonstrated facts that, if true, would support jurisdiction over the defendant. *OMI Holdings, Inc. v. Royal Ins. Co. of Can.*, 149 F.3d 1086, 1091 (10th Cir. 1998). To defeat the plaintiff's *prima facie* case, a defendant "must present a compelling case demonstrating that the presence of some other considerations would render jurisdiction unreasonable." *Id.* (internal quotation marks omitted).

The Court will accept the well-pleaded allegations (namely, the plausible, nonconclusory, and nonspeculative facts) of the complaint as true to determine whether the plaintiff has made a *prima facie* showing that personal jurisdiction exists. *Dudnikov*, 514 F.3d at 1070. Any factual conflicts must be resolved in the plaintiff's favor. *Wentz v. Memery Crystal*, 55 F.3d 1503, 1505 (10th Cir. 1995).

B. Personal Jurisdiction Analysis[2]

As noted, SecureW2 is a Dutch company. (ECF No. 37 ¶ 2.) Cloudpath's primary argument for personal jurisdiction over SecureW2 is that it contractually agreed to personal jurisdiction in Colorado. (ECF No. 64 at 3–7.) "[A] valid consent or a stipulation that the court has jurisdiction prevents the successful assertion of a Rule 12(b)(2) defense." 5B Charles Alan Wright et al., *Federal Practice & Procedure* § 1351

[2] Some of the declarations and exhibits submitted by the parties in support of or opposition to the Rule 12(b)(2) Motion were filed under Restricted Access. To the extent the Court quotes or summarizes such materials in this Order, the Court has concluded that the portions quoted or summarized do not qualify for Restricted Access under D.C.COLO.LCivR 7.2.

(3d ed., Apr. 2015 update) ("*Wright & Miller*"). The Court will therefore analyze the two contracts through which SecureW2 allegedly consented to personal jurisdiction in Colorado.

1. The MNDA

Cloudpath argues that SecureW2 "expressly submitted" to this Court's personal jurisdiction through a Master Non-Disclosure Agreement dated September 9, 2008 ("MNDA"). (ECF No. 37 ¶ 15.) MNDA § 14 states, in relevant part, that

> all actions related hereto shall be governed by the laws of the State of Colorado, USA, excluding its choice of law principles. With respect to any action arising under or related to this Agreement, [SecureW2] hereby: (i) agrees that [it] has sufficient contacts with Colorado to subject it to the personal jurisdiction of the state and federal courts of Colorado; . . . (iii) waives and agrees not to assert any claim that: (a) it is not subject personally to the jurisdiction of the above-named courts . . . .

(ECF No. 59-1 § 14.) Also relevant is MNDA § 17, which states that

> [t]he obligations set forth herein shall apply until termination of this Agreement. Further[,] the confidentiality obligations set forth herein shall remain in full force and effect for a period of five (5) years from the termination of this Agreement. Any causes of action accrued on or before such expiration shall survive the expiration of the applicable statute of limitations.

(*Id.* § 17.)

By way of employee declarations submitted in support of its Rule 12(b)(2) Motion, SecureW2 argues that it entered into the MNDA solely "to facilitate the negotiations . . . for a future referral agreement" which "never culminated," and "[t]he last negotiations between [the two companies] related to the referral agreement occurred in late-spring 2009." (ECF No. 59-2 ¶¶ 13–16; ECF No. 66 ¶¶ 4–6.)

SecureW2 therefore argues that the MNDA terminated in 2009, thus terminating the jurisdictional waiver.

Cloudpath responds that the purposes of the MNDA were broader than just a prospective referral relationship, and that neither it nor SecureW2 ever provided any indication to one another that the MNDA had been terminated. (ECF No. 64-1 ¶¶ 3–5.) Cloudpath argues, moreover, that the provision extending the MNDA's "confidentiality obligations" for five years after termination means that "the provisions related to enforcing the MNDA, including personal jurisdiction, must also have survived termination for at least the same five-year period." (ECF No. 64 at 5–6.)

Cloudpath raises a question of contract interpretation under Colorado law, which is usually a question of law for the Court. *See, e.g.*, *Ad Two, Inc. v. City & Ctny. of Denver ex rel. Manager of Aviation*, 9 P.3d 373, 376 (Colo. 2000). The Court's primary task in this regard is to "interpret the agreement in a manner that best effectuates the intent of the parties." *Allen v. Pacheco*, 71 P.3d 375, 378 (Colo. 2003). Intent is usually discerned "from the language of the instrument itself." *Ad Two*, 9 P.3d at 376. Indeed, "[w]ritten contracts that are complete and free from ambiguity will be found to express the intention of the parties and will be enforced according to their plain language. Extraneous evidence is only admissible to prove intent where there is an ambiguity in the terms of the contract." *Id.* (citation omitted). Thus, much turns on "whether an ambiguity exists," which itself turns on "whether the disputed provision is reasonably susceptible on its face to more than one interpretation." *Allen*, 71 P.3d at 378. This determination is necessarily made in the context of "the agreement as a whole." *Id.*

Taking the MNDA as a whole, the Court concludes—on this record at least—that an ambiguity exists through tension created by the relationship of MNDA § 14 to § 17. In particular, § 17 states that "[t]he obligations set forth herein shall apply until termination of this Agreement" and only makes explicit exception for "the confidentiality obligations," which persist for five additional years and survive any applicable statute of limitations to that extent. On the other hand, § 14's jurisdictional waiver states that it applies to "any action arising under or related to this Agreement." That would seem to apply to "any action," as it says, including one brought after termination. On the other hand, the jurisdictional waiver could also be considered one of the "obligations" that terminates per § 17. Both interpretations are reasonable, and this record is not sufficient for the Court to determine which is correct, or even whether the ambiguity can be resolved as a matter of law.

The Rule 12(b)(2) Motion presents an additional fact question: whether the parties actually terminated the MNDA. This likely turns, in part at least, on the purposes served by the MNDA, which also appear to be disputed.

Although contract interpretation is generally said to be a question of law, that is "only because it [typically] requires application of well-settled principles of contract interpretation to [undisputed] facts." *Rich v. Ball Ranch P'ship*, 345 P.3d 980, 983 (Colo. App. 2015). Here, the relevant facts are disputed. Assuming Cloudpath can prove its version of the facts, Cloudpath would establish the applicability of the MNDA's jurisdictional waiver. Cloudpath has therefore offered a *prima facie* case of personal jurisdiction, thus defeating the Rule 12(b)(2) Motion. This, of course, does not prevent SecureW2 from re-raising the personal jurisdiction question at a later stage, such as in a summary judgment motion. *See, e.g.*, 5B *Wright & Miller* § 1351 nn.32–40 and accompanying text.

2. The EULA

In its FAC, Cloudpath alleges that SecureW2 also consented to this Court's personal jurisdiction in an End-User License Agreement ("EULA"). (ECF No. 37 ¶¶ 15, 49.) Cloudpath did not attach any EULA to the FAC, but alleges that Cloudpath requires "all those who access its proprietary software products to execute" an "administrator-level EULA" prohibiting commercial exploitation of Cloudpath's proprietary technology. (*Id.* ¶¶ 223–26.)

In its Rule 12(b)(2) Motion, SecureW2 argues that the FAC does not make clear which EULA it executed (implying that there may have been more than one). (ECF No. 58 at 7.) SecureW2 also attaches "the only ostensibly applicable EULA," which is undated but bears a 2009 copyright and does not contain any jurisdictional waiver. (*Id.*) SecureW2 claims that Cloudpath produced this EULA to SecureW2 (for unexplained reasons), and that SecureW2 does not keep records of EULAs it executed "over seven years ago." (*Id.* at 4 n.1.)

In response, Cloudpath submits a declaration from one of its employees, Kevin Koster, stating that the relevant EULA was executed on August 26, 2008. (ECF No. 64-1 ¶ 7.) Koster's declaration then reprints "Section 20 of [that] version of the EULA" as follows:

> **Governing Law.** Unless specified in an Order Form, Colorado state law governs the interpretation of this Agreement, without regard to its choice of law rules.

> **Resolution of Disputes.** Any action seeking enforcement of this Agreement or any provision hereof will be brought exclusively in the state or federal courts located in the County of Jefferson, State of Colorado. Each party hereby agrees to submit to the jurisdiction of such courts.

(*Id.* ¶ 8 (boldface in original).) Neither Koster nor Cloudpath has placed the 2008 EULA itself into the record.

It is admittedly strange that Cloudpath would: (a) allege the EULA generically in its FAC (in contrast to the MNDA, which it identified by date); then (b) produce a 2009 version of the EULA that does not contain a jurisdictional waiver; and finally (c) defend against SecureW2's motion with the 2008 version of the EULA, although only by quoting excerpts in a declaration, not by attaching the EULA itself. The Court will assume, however, that Cloudpath complied with Federal Rule of Civil Procedure 11 when asserting that SecyreW2 executed the 2008 EULA. Under that assumption, certain factual disputes arise that the Court must resolve in Cloudpath's favor at this stage, such as the scope of the 2008 EULA, whether SecureW2 executed it, and whether it was ever terminated. For this additional reason, the Rule 12(b)(2) Motion must fail.

C. Pendant Jurisdiction

The foregoing is enough, for now, to establish personal jurisdiction over SecureW2 with respect to Cloudpath's claims that SecureW2 breached the MNDA (Count 14) and the EULA (Count 15). However, jurisdiction over these two particular causes of action does not immediately imply jurisdiction over additional causes of action. The question, rather, is whether these additional causes of action "arise from the same facts as the claim over which [the Court] has proper personal jurisdiction."

United States v. Botefuhr, 309 F.3d 1263, 1272 (10th Cir. 2002). If so, the Court may exercise "pendant personal jurisdiction" over the additional causes of action. *Id.*

In this case, those additional causes of action are as follows:

- violation of, and conspiracy to violate, the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and Stored Communications Act (Counts One, Two, and Three) based on alleged actions to steal Cloudpath's trade secrets;
- misappropriation of trade secrets, based on the same conduct (Count Four);
- tortious interference with contract, based on SecureW2's use of Cloudpath's trade secrets to lure away Cloudpath customers, and based on SecureW2's interference with Cloudpath's employment/agency and other contracts with Grimm, Haney, and Kashyap (Count Five);
- tortious interference with prospective business advantage, based on essentially the same conduct (Count Six);
- conversion, based on conspiracy to steal Cloudpath's trade secrets (Count Seven);
- civil theft, based on essentially the same allegations (Count Eight);
- unfair competition, based on all of the foregoing (Count Nine);
- unjust enrichment, based on all of the foregoing (Count Sixteen); and
- conspiracy to commit all of the foregoing (Count Seventeen).

(ECF No. 37 ¶¶ 102–88, 232–40.) These causes of action indisputably arise from the same facts as the breach-of-contract claims. Indeed, all of Cloudpath's causes of action are simply different ways of suing over the same general course of conduct—the alleged theft and misuse of its trade secrets. Accordingly, to the extent the Court has personal jurisdiction over Cloudpath's claims for breach of the MNDA and/or the 2008 EULA, the Court has pendant personal jurisdiction over all causes of action asserted against SecureW2.[3]

For all of the foregoing reasons, SecureW2's Rule 12(b)(2) Motion is denied.[4]

III. RULE 12(b)(6) ANALYSIS

A. Legal Standard

Under Federal Rule of Civil Procedure 12(b)(6), a party may move to dismiss a claim in a complaint for "failure to state a claim upon which relief can be granted." The 12(b)(6) standard requires the Court to "assume the truth of the plaintiff's well-pleaded factual allegations and view them in the light most favorable to the plaintiff." *Ridge at Red Hawk, LLC v. Schneider*, 493 F.3d 1174, 1177 (10th Cir. 2007). In ruling on such a motion, the dispositive inquiry is "whether the complaint contains 'enough facts to state a claim to relief that is plausible on its face.'" *Id.* (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Granting a motion to dismiss "is a harsh remedy which must be cautiously studied, not only to effectuate the spirit of the liberal rules of

[3] An interesting question is whether pendant personal jurisdiction in this case only encompasses alleged wrongful acts that took place within the five years following the termination of the MNDA (assuming it did terminate, and assuming that the EULA does not provide a continuing basis for personal jurisdiction). The parties have said nothing about this question, however, so the Court makes no ruling on it.

[4] Given this disposition, the Court need not reach Cloudpath's additional arguments for personal jurisdiction (such as SecureW2's alleged intentional targeting of Cloudpath in Colorado, *see* ECF No. 64 at 8–14), nor SecureW2's counterarguments (*see* ECF No. 58 at 10–15; ECF No. 65 at 5–9). The parties have adequately preserved these arguments and, to the extent still applicable, may re-raise them at a later stage.

pleading but also to protect the interests of justice." *Dias v. City & Cnty. of Denver*, 567 F.3d 1169, 1178 (10th Cir. 2009) (internal quotation marks omitted). "Thus, 'a well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and that a recovery is very remote and unlikely.'" *Id.* (quoting *Twombly*, 550 U.S. at 556).

B. CFAA Claim (Count One)

1. "Exceeds Authorized Access"

The CFAA criminalizes various specified forms of hacking and computer data theft if the affected computer is a "protected computer," meaning, among other things, a computer "which is used in or affecting interstate or foreign commerce or communication." *See* 18 U.S.C. § 1030(a), (e)(2)(B). Although primarily a criminal statute, the CFAA creates a private right of action in some circumstances:

> Any person who suffers damage[5] or loss[6] by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).

Id. § 1030(g). Of those cross-referenced subclauses, only subclause (I) is relevant here: "loss to 1 or more persons during any 1-year period . . . aggregating at least

[5] The CFAA defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8).

[6] The CFAA defines "loss" to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11).

$5,000 in value." *Id.* § 1030(c)(4)(A)(i)(I).

The foregoing portions of the CFAA are not currently in dispute here. Rather, the Rule 12(b)(6) Motion largely focuses on the scope of the following potential violations of the CFAA:

> Whoever—
>
> * * *
>
> **(2)** intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> * * *
>
> **(C)** information from any protected computer; [or]
>
> * * *
>
> **(4)** 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 . . . ; [or]
>
> **(5)** . . .
>
> **(B)** intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> **(C)** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss[;]
>
> * * *
>
> shall be punished as provided [elsewhere in the statute].

18 U.S.C. § 1030(a).

In its FAC, Cloudpath does not allege any of these violations specifically, at least not by citing to a statutory subsection or paragraph. Cloudpath instead invokes a mash-up of key statutory phrases, asserting that the various Defendants "knowingly and intentionally accessed Cloudpath's Systems to further a fraud, obtain something of value, and/or to recklessly cause damage and/or loss," that such access "was without authorization and/or in excess of authorized access," that Defendants "obtained data and information the value of which is in excess of $5,000 in any one-year period," and that Cloudpath suffered "damage and/or loss in an amount that equals or exceeds at least $5,000.00." (ECF No. 37 ¶¶ 104–14.)

These allegations conceivably cover all of the above-quoted potential CFAA violations. In its Response to Defendants' Motion to Dismiss, however, Cloudpath focuses entirely on the "exceeds authorized access" portion of §§ 1030(a)(2)(C) and 1030(a)(4). (ECF No. 46 at 3–9.) Presumably Cloudpath takes this approach because its FAC alleges that it permitted Grimm, Haney, and Kashyap to access Cloudpath's computer systems as part of their employment or other agency relationship. (*See* ECF No. 37 ¶¶ 37, 43, 47.) Thus, Cloudpath frames its FAC in terms of former employees or agents who were allowed to access Cloudpath computers but used their access for allegedly disloyal purposes. The question, then, is whether this qualifies as "exceed[ing] authorized access" as used in the CFAA.

"Exceeds authorized access" is a defined term. It means "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." 18 U.S.C. § 1030(e)(6). Although the definition appear straightforward, it has generated a circuit split—one in which the

Tenth Circuit has to date not taken a position. One collection of circuits holds that it extends to an employee/agent who use his or her access for purposes contrary to the employer/principal's interests. Obviously Cloudpath favors this position. Defendants naturally favor the other side of the circuit split, which holds that "exceeds authorized access" only applies to an employee/agent who uses otherwise-permitted computer access to obtain data that the employer/principal has declared off-limits to that employee/agent. As explained below, the Court ultimately agrees with the latter position.

2. The Circuit Split

So far, the First, Second, Fourth, Fifth, Seventh, Ninth, and Eleventh Circuits have expressed their views on the meaning of "exceeds authorized access." A chronological account of these courts' various decisions is helpful to understanding the issues involved.

a. *EF Cultural*

Apparently the first circuit to address the reach of "exceeds authorized access" was, indeed, the First Circuit. *See EF Cultural Travel B.V. v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). The plaintiff in *EF Cultural* was "the world's largest private student travel organization"; the defendants were mostly the plaintiff's former employees who had set up a competing business. *Id.* at 579. Part of the defendants' competition strategy was to undersell the plaintiff, and that required access to the plaintiff's pricing information. *Id.* Although pricing was available on the plaintiff's website, it was difficult to obtain a comprehensive price list: "EF's website listed 154,293 prices for various tours." *Id.* at 580 n.3. The defendants therefore commissioned a special computer program that could quickly gather the relevant data. *Id.* at 579. The computer program relied on one defendant's inside knowledge about the plaintiff's tour codes, which otherwise would have been gibberish. *Id.* at 579, 583.

The First Circuit held that the foregoing scenario stated an "exceeds authorized access" claim under the CFAA, although the analysis is a bit slippery. On the one hand, the court had to account for the fact that all of the data were technically available to anyone visiting the plaintiff's website. Thus, the defendants did not in fact access anything unavailable to the general public. *Id.* at 583. On the other hand, the court noted that the former employee who shared his knowledge about the tour codes had been subject to a confidentiality agreement and that the defendants "would face an uphill battle trying to argue that it was not against EF's interests for [the defendants] to use the tour codes to mine EF's pricing data." *Id.* The court therefore held that the defendants' "wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website." *Id.*

b. *IAC*

Five years after *EF Cultural*, the Seventh Circuit, per Judge Richard Posner, addressed a somewhat different form of former-employee wrongdoing. *See Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) ("*IAC*"). Rather than using trade secrets to his competitive advantage, Citrin, the former employee, formed an intent (before he quit) to go into business for himself (a violation of his employment contract) and he therefore deleted a significant amount of competitively important information from his company-issued laptop. *Id.* at 419. In particular, he used a "secure-erasure program, designed, by writing over the deleted files, to prevent their recovery." *Id.* Citron's former employer therefore sued him under what was then CFAA § 1030(a)(5)(A)(i), which prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." *See IAC*, 440 F.3d at 419.[7]

The primary question argued on appeal was whether Citrin caused any "transmission" within the meaning of the statute. *Id.* This question was apparently bogged down in ambiguity regarding whether Citrin had loaded the secure-erasure program from a disk, had downloaded it from the Internet, or had placed it on the laptop through some other means. *Id.* The Seventh Circuit held that this would make no difference because any of these methods would fall within the evil that Congress sought to address: "attacks by virus and worm writers, on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other." *Id.* at 420.

Although this holding apparently would have been enough to resolve the appeal, the Seventh Circuit volunteered that Citrin had also violated CFAA § 1030(a)(5)(A)(ii),[8] which prohibits "intentionally access[ing] a protected computer without authorization,

[7] The same prohibition still exists in the statute, but is codified at § 1030(a)(5)(A) rather than 1030(a)(5)(A)(i).

[8] Now codified at § 1030(a)(5)(B).

and as a result of such conduct, recklessly caus[ing] damage." *See IAC*, 440 F.3d at 420. The court reasoned that Citrin's "authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files . . . in violation of the duty of loyalty that agency law imposes on an employee." *Id.* The court acknowledged, however, that the "exceeds authorized access" prong of the CFAA "might seem the more apt description of what Citrin did." *Id.*

In this vein, the court analyzed *EF Cultural* and apparently endorsed it as a proper application of "exceeds authorized access" because the website involved "was open to the public, so [the knowledgeable defendant] was authorized to use it, but he exceeded his authorization by using confidential information to obtain better access than other members of the public." *Id.* In contrast, Citrin was simply "without authorization": "Citron's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420–21.

c. *LVRC*

The Ninth Circuit addressed the meaning of "exceeds authorized access" in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). The employer in *LVRC* was the operator of an addiction treatment center in Nevada; the employee, Brekka, was essentially a marketing officer. *Id.* at 1129. Brekka had administrator's rights to his employer's website, which permitted him to view statistics regarding website traffic. *Id.*

Eventually Brekka began considering an ownership interest in his employer. *Id.*

As part of his due diligence, he e-mailed to his personal account his employer's financial statements, budget documents, and patient admission reports. *Id.* at 1129–30. Soon after, Brekka elected not to take an ownership interest and he left the company. *Id.* Over a year later, his former employer noticed that someone had logged into its website with Brekka's administrative credentials. *Id.* The employer then sued Brekka under the "without authorization" prong of CFAA § 1030(a)(2) and (4), alleging that he had violated the statute both when he e-mailed documents to himself before resigning and when he apparently logged into the website after resigning. *Id.* at 1129, 1130.

For present purposes, the Ninth Circuit's analysis of Brekka's pre-resignation conduct is most relevant.[9] The court noted that "without authorization" in the CFAA was not specifically defined, but that its plain meaning related to permission: "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it." *Id.* at 1133. Moreover, the court found no language in the CFAA to support the employer's argument "that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest." *Id.*

The Ninth Circuit reached this conclusion by comparing "without authorization" to "exceeds authorized access": "a person who 'intentionally accesses a computer without authorization,' accesses a computer without any permission at all, while a person who 'exceeds authorized access,' has permission to access the computer, but accesses

[9] As to the alleged website login following his resignation, the Ninth Circuit affirmed the district court's holding that the company had failed to raise a genuine issue of fact that Brekka himself had logged in to the website, as opposed to other individuals who apparently used his company computer after his departure. *Id.* at 1136–37.

information on the computer that the person is not entitled to access." *Id.* (citations omitted). Thus, "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'" *Id.*; *see also id.* at 1135 ("The plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer."). Brekka certainly had "permission to access [his] computer" before he left the company, and so the Ninth Circuit held that the "without authorization" prong was inapplicable. *Id.* at 1133.

The Ninth Circuit also specifically rejected *IAC* and its duty-of-loyalty analysis. *Id.* at 1133–36. The court noted that the CFAA is "primarily a criminal statute" and so its interpretation, even in a civil lawsuit, establishes the scope of criminal liability. *Id.* at 1134. The Court further noted the Supreme Court's "warn[ing] against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants." *Id.* In this light, the court reasoned that

> [n]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer. If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner.

Id. Finally, in a footnote, the court held that the same reasoning would doom any argument from the employer that "exceeds authorized access" could turn on the duty of loyalty. *Id.* at n.7.

d. *John*

Following *LVRC* was the Fifth Circuit's decision in a criminal CFAA prosecution, *United States v. John*, 597 F.3d 263 (5th Cir. 2010). The defendant had been an account manager at Citigroup and had used her access to Citigroup's internal computer system to feed information to a relative who used it to incur fraudulent charges. *Id.* at 269. The Government obtained a conviction against the defendant for, among other things, exceeding her authorized access in violation of CFAA § 1030(a)(2)(A) (relating to "information contained in a financial record of a financial institution") and § 1030(a)(2)(C) (relating to "information from any protected computer"). *Id.* at 269–70.

The Fifth Circuit framed the question on appeal as "whether 'authorized access' or 'authorization' may encompass limits placed on *the use* of the information obtained by permitted access to a computer system." *Id.* at 271 (emphasis in original). The court's answer was yes, "at least when the user knows or reasonably should know that he or she is not authorized to access the computer and information obtainable from that access in furtherance of or to perpetrate a crime." *Id.* "To give but one example," said the court, "an employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business. An employee would 'exceed[] authorized access' if he or she used that access to obtain or steal information as part of a criminal scheme." *Id.* (alteration in original).

The Fifth Circuit further noted the First Circuit's *EF Cultural* decision. The court "d[id] not necessarily agree that violating a confidentiality agreement under circumstances such as those in *EF Cultural* . . . would give rise to criminal culpability," but it did “agree with the First Circuit that the concept of ‘exceeds authorized access’ may include exceeding the purposes for which access is ‘authorized.’” *Id.* at 272.

Citing *LVRC*, the court also noted “that the Ninth Circuit may have a different view of how ‘exceeds authorized access’ should be construed.” *Id.* The Fifth Circuit interpreted *LVRC*’s interpretation as turning primarily on the lack of notice that breach of a state law fiduciary duty could constitute a crime under the CFAA. *Id.* at 273. “There are no such concerns in the present case,” it reasoned, because “[a]n authorized computer user ‘has reason to know’ that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme.” *Id.*

e. *Rodriguez*

Not long after *John*, the Eleventh Circuit likewise evaluated a criminal prosecution under the CFAA. *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). The defendant in *Rodriguez* had been an employee of the Social Security Administration (“SSA”) who had permission to access databases containing American citizens’ private information. *Id.* at 1260. The SSA trained such employees on the narrow purposes for which they could use such access and warned them of criminal penalties for accessing information without such a purpose. *Id.* The defendant, however, used his privileges to stalk women. *Id.* at 1260–62. The Government charged him with, and he was convicted of, exceeding authorized access under CFAA § 1030(a)(2)(B) (relating to “information from any department or agency of the United States”). *Id.* at 1262.

The Eleventh Circuit upheld the conviction, distinguishing *LVRC* because the

SSA had a policy "that use of databases to obtain personal information is authorized only when done for business reasons." *Id.* at 1263. In other words, the Eleventh Circuit apparently saw *LVRC* as turning on the lack of a policy specifically denying company computer access, or access to information stored on company computers, for anything but business purposes. The Eleventh Circuit then went on to agree with, and extend, the Fifth Circuit's *John* decision:

> Rodriguez erroneously argues that he cannot be convicted under the [CFAA] because[, unlike the defendant in *John*,] his use of the information was not criminal. The problem with Rodriguez's argument is that his use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access. Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason.

Id.

f. *Nosal*

About a year-and-a-half after *Rodriguez*, the CFAA returned to the Ninth Circuit, this time as a criminal prosecution. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). The defendant in Nosal worked for an executive search firm, but then resigned to start a competing firm. *Id.* at 856. He persuaded some of his former colleagues to join him, but also to use their access to company databases to gather competitively sensitive information before departing. *Id.* The Government charged the defendant with aiding and abetting a violation of CFAA § 1030(a)(4) (relating to access with intent to defraud) because he allegedly convinced employees to exceed their authorized access in gathering information to be used against the company. *Id.* The district court had dismissed this charge in light of *LVRC*, and the Ninth Circuit, per

Judge Kozinski, affirmed.

The Ninth Circuit began by noting that the definition of “exceeds authorized access”

> can be read either of two ways: First, as Nosal suggests and the district court held, it could refer to someone who’s authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as “hacking.” . . . Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information.

Id. at 856–57.

The Ninth Circuit found that “[t]he government’s interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute,” and that “[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.” *Id.* The court particularly noted that Congress’s expressed purpose when enacting the CFAA in 1984 was “to address the growing problem of computer hacking.” *Id.* at 858. But, the Ninth Circuit reasoned,

> [t]he government’s construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.

Id. at 859.

The court was particularly concerned about how easy it is to exceed one's authorized access:

> Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement.

Id. at 860 (emphasis in original; footnote omitted). Moreover,

> [s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read. Consider the typical corporate policy that computers can be used only for business purposes. What exactly is a "nonbusiness purpose"? If you use the computer to check the weather report for a business trip? For the company softball game? For your vacation to Hawaii? And if minor personal uses are tolerated, how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?

Id.

The court also noted that nearly all popular websites have terms of service, including prohibitions on relatively innocuous behavior like allowing someone else to log in to your account. "Some may be aware that, if discovered [violating such rules], they may suffer a rebuke . . . or a loss of access, but few imagine they might be marched off to federal prison for doing so." *Id.* at 861.

The Ninth Circuit specifically rejected *Rodriguez*, *John*, and *IAC*:

> These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the [CFAA's] unitary definition of "exceeds authorized access." They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly . . . .

Id. at 862–63. Under such a narrow construction, the Ninth Circuit finally concluded that "the CFAA targets the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Id.* at 863 (internal quotation marks omitted, alterations incorporated). Thus, the purpose for which an individual accesses information is irrelevant so long as he or she may access it for *some* purpose.

g. *WEC*

A few months after *Nosal*, the Fourth Circuit followed suit in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) ("*WEC*"). An employee (Miller) privately decided to go into business against his employer and, before leaving, made a copy of his employer's competitively sensitive information regarding pricing, pending projects, technical capabilities, and so forth. *Id.* at 201–02. The employer, who allegedly lost business to Miller, sued for various forms of the "without authorization" and "exceeds authorized access" offenses under the CFAA. *Id.* at 203. The district court dismissed the CFAA claim because "WEC's company policies regulated *use* of information[,] not access to that information." *Id.* at 202 (emphasis in original; internal quotation marks omitted). On appeal, the Fourth Circuit ultimately agreed.

The Fourth Circuit noted the "two schools of thought" under the CFAA, which it attributed to the Seventh Circuit's *IAC* decision and the Ninth Circuit's *Nosal* and *LVRC* decisions. *Id.* at 203. Like the Ninth Circuit in *LVRC*, the Fourth Circuit was particularly concerned with the fact that the CFAA is also a criminal statute and so any interpretation, even in a civil context, would dictate criminal liability. *Id.* at 204. The Fourth Circuit also reprised, in somewhat different form, *Nosal*'s concern regarding employees' lack of notice that seemingly innocuous behavior could create criminal liability:

> [A]n interpretation [of the CFAA that turns on authorized use of information rather than authorized access] would impute liability to an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home and make headway in meeting his employer's goals. Such an employee has authorization to obtain and alter the information that he downloaded. Moreover, he has no intent to defraud his employer. But . . . because he obtained information in a manner that was not authorized (i.e., by downloading it to a personal computer), he nevertheless would be liable under the CFAA.

Id. at 206 (internal quotation marks omitted) . The court instead concluded that an individual "accesses a computer 'without authorization' when he gains admission to a computer without approval," and that an individual "'exceeds authorized access' when he has approval to access the computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access." *Id.* at 204.

The Fourth Circuit also criticized *IAC*'s agency theory because it implied "that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems." *Id.* at 206. The court "d[id] not think Congress intended an immediate end to the agency relationship and, moreover, the imposition of criminal penalties for such a frolic." *Id.*

h. *Valle*

The Second Circuit is the most recent entrant to the debate. *See United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). The defendant in *Valle*, a New York City police officer, was charged with exceeding his authorized access to police databases to find a woman he allegedly intended to kidnap and torture. *Id.* at 512–13. "It [was] undisputed that the NYPD's policy, known to Valle, was that these databases could only be accessed in the course of an officer's official duties and that accessing them for personal use violated Department rules." *Id.* at 513. He was convicted at trial and the district judge denied his motion for judgment of acquittal because it reasoned that Valle's conduct fell "'squarely within the plain language' of the statute because [he] had not been authorized [to use the police databases] without a law enforcement reason for doing so." *Id.* at 515 (quoting district court opinion).

The Second Circuit reversed and directed a judgment of acquittal. "The dispositive question [was] whether Valle 'exceeded authorized access' when he used his access to [police databases] to conduct a search for [the intended kidnapping victim] with no law enforcement purpose." *Id.* at 523. The court effectively adopted the Ninth Circuit's reasoning in *Nosal* and the Fourth Circuit's reasoning in *WEC*. *Id.* at 523–28. Like those courts, the Second Circuit wanted to avoid "criminaliz[ing] the conduct of millions of ordinary computer users," *id.* at 527, and was also particularly influenced by certain legislative history stating that the "the conduct prohibited [by the CFAA] is analogous to that of breaking and entering," *id.* at 525 (internal quotation marks omitted). "Consequently," the court said, "the legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend." *Id.*

3. Resolution

To summarize, the Second, Fourth, and Ninth Circuits reject any inquiry into an individual's purposes for accessing information, instead asking only whether the individual had any sort of permission to access whatever information he or she accessed. The First, Fifth, Seventh, and Eleventh Circuits, by contrast, hold that an improper purpose may cause someone to lose permission even if he or she would retain such permission for proper purposes.[10]

The undersigned previously faced this circuit split but was able to avoid taking a position because the employee in question violated company policy by retaining his company laptop for three weeks after his resignation, and it was a fair inference that he used those three weeks to access company information. *See SBM Site Servs., LLC v. Garrett*, 2012 WL 628619, at *5 (D. Colo. Feb. 27, 2012). Thus, the plaintiff had alleged a plausible claim for post-resignation unauthorized access, regardless of whether the former employee had exceeded authorized access. That scenario is

[10] The Eighth Circuit, while not presented with any challenge to the meaning of "exceeds authorized access," affirmed a conviction implicitly under this reasoning. *See United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011) (Department of Education contractor used access to student loan databases to look up President Obama's student loan information).

potentially a small part of this case (*see* Part III.B.4, *infra*), but the bulk of it centers around pre-resignation access to company data. The Court therefore cannot avoid the circuit split under these facts. As explained below, this Court essentially agrees with the Second, Fourth, and Ninth Circuits, although with two reservations.

The first reservation arises from statements, such as the Ninth Circuit's in *LVRC*, that "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'" 581 F.3d at 1133. If so, why may not an employer promulgate a policy such as, "Employees are authorized to use company computers solely to the extent they do so for company purposes"? Any employee who does otherwise is accessing a computer "without authorization." That is precisely the reasoning the Eleventh Circuit used in *Rodriguez* to uphold criminal liability against the SSA employee who misused his database access to stalk women. *See* 628 F.3d at 1263. That is also the basic reasoning behind Cloudpath's argument here: one may have authority to use a computer for certain purposes, but not for others.

The premise needed to shore up the Second, Fourth, and Ninth Circuits' reasoning—one that is implicit in those courts' decision but should be stated explicitly—is that "authorized" under the CFAA must mean something like "permitted to access at least some data on the computer." In other words, with respect to the hypothetical policy proposed above, the CFAA supposedly cares only that it begins with "Employees are authorized to use company computers . . . ." This implies that employees will be allowed to use a computer for at least one purpose, and everything else, such as a specific purpose for which the employer has granted that privilege, is irrelevant—it cannot affect the rights and liabilities established under the CFAA.

This is not a natural reading of "authorized." *See Smith v. United States*, 508 U.S. 223, 228 (1993) ("When a word is not defined by statute, we normally construe it in accord with its ordinary or natural meaning."). In ordinary life, none of us could get away with saying, "The IT department gave me a login and I stopped listening after that —I figured I could do whatever I wanted with the computer." We all know that authority is sometimes inseparable from the conditions placed upon it, particularly when we are entrusted with property that does not belong to us. *Cf. Nosal*, 676 F.3d at 865 (Silverman, J., dissenting) ("This is not an esoteric concept. A bank teller is entitled to access a bank's money for legitimate banking purposes, but not to take the bank's money for himself. A new car buyer may be entitled to take a vehicle around the block on a test drive. But the buyer would not be entitled—he would 'exceed his authority'—to take the vehicle to Mexico on a drug run.").

As it turns out, however, construing "authorized" as "permitted to access at least some data on the computer" is the only construction that avoids making "exceeds authorized access" entirely redundant to "without authorization." *See FTC v. Accusearch Inc.*, 570 F.3d 1187, 1198 (10th Cir. 2009) ("Under a long-standing canon of statutory interpretation, one should avoid construing a statute so as to render statutory language superfluous." (internal quotation marks omitted)). Again, the point in dispute here is whether the specific wording of an employer's policies can affect CFAA liability. If it can, then a policy worded as this Court proposed—"Employees are authorized to use company computers solely to the extent they do so for company purposes"—would mean that any employee *exceeding* that authorization would be *without* authorization. “Exceeds authorized access” would then be superfluous. By contrast, a distinction remains if “without authorization” means “not permitted to access any data on the computer,” and “exceeds authorized access” means “permitted to access at least some data on the computer, but accessing data outside the scope of that permission.”

Other statutory text seems to confirm this reading, even if not the most natural construction of “authorized.” The CFAA defines “exceeds authorized access” as “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.” 18 U.S.C. § 1030(e)(6) (emphasis added). This definition could be expressed as three elements:

1. the individual in question possesses some amount of permission to “access a computer”;
2. the computer in question contains information that the individual “is not entitled” to “obtain or alter,” either in a certain manner or at all (“*so* to obtain or alter”); and
3. the individual accesses the machine to obtain or alter information in a prohibited manner (which may include obtaining or altering it any manner).

Under this interpretation, however, the little word “so” starts to cause problems, leading to this Court’s second reservation regarding, in particular, the Fourth and Ninth Circuits’ reasoning in *WEC* and *Nosal*.

Nosal and *WEC* both faced arguments that (1) “so” means “in that manner,” and (2) “in that manner” can supposedly refer to restrictions on the purpose for which information is accessed. *WEC*, 687 F.3d at 205; *Nosal*, 676 F.3d at 857–58. Facing the Government's argument that the second proposition was necessary to prevent "so" from becoming superfluous, *Nosal* proposed that "so," interpreted as "in that manner," could refer to prohibited methods of obtaining data, like an individual downloading to a flash drive information he is allowed to see but not copy. *Nosal*, 676 F.3d at 858. *WEC* quotes this same proposal and concludes that, "in the Ninth Circuit's view, and ours, interpreting 'so' as 'in that manner' fails to mandate CFAA liability for the improper *use* of information that is accessed with authorization." *WEC*, 687 F.3d at 205 (emphasis in original).

Nosal, however, also speculated that "Congress could just as well have included 'so' as a connector or for emphasis." *Nosal*, 676 F.3d at 858. *WEC* agrees with this as well, but, unlike *Nosal*, goes on to formally adopt it as the correct interpretation. *WEC*, 687 F.3d at 205–06. *WEC* was particularly concerned about a hypothetical that is essentially indistinguishable from *Nosal*'s download-to-the-flash-drive proposal:

> [A]n interpretation [of the CFAA that turns on authorized use of information rather than authorized access] would impute liability to an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home and make headway in meeting his employer's goals. Such an employee has authorization to obtain and alter the information that he downloaded. Moreover, he has no intent to defraud his employer. But . . . because he obtained information "in a manner" that was not authorized (i.e., by downloading it to a personal computer), he nevertheless would be [potentially criminally] liable under the CFAA.

Id. at 206. *WEC* believed that, as between this possibility and the possibility that "so" is just "a connector or [included] for emphasis," the rule of lenity required it to choose "the more obliging route," meaning the latter possibility.

WEC's reasoning effectively reads "so" out of the statute. Although "so" is sometimes used in English for emphasis ("He is *so* handsome"), that reading makes no sense in this context. "So" is also used as a connector, but almost always as an illative. *See* Merriam-Webster Online, s.v. "so" (giving as an example, "the witness is biased and so [*i.e.*, therefore] unreliable"), *at* http://www.merriam-webster.com/dictionary/so (last accessed Dec. 18, 2015). That also makes no sense in the context of the CFAA definition. Thus, *WEC* does not really treat "so" as a connector or an intensifier, but as if it does not exist—preferring that outcome over endorsing an interpretation by which an individual commits a crime through impermissibly downloading company information to a personal computer, even with intentions to further company business.

This Court is not willing to go that far. Although *WEC*'s hypothetical is troubling, the Court is not convinced that "so," interpreted as "in that manner," never states a worthy criminal case. It may be particularly important to a company or government agency that certain information be accessed only on site, for example, as opposed to through a remote connection, because the risk is too high that external access could also allow a third party to intercept the data. Even with good intentions, an employee who ignores this restriction, and especially one who deliberately circumvents whatever remote access barriers might exist, might be justifiably prosecuted. Furthermore, as *WEC* itself recognizes, interpreting "so" as "in that manner" (its most natural sense in context) actually shores up the idea that Congress was focused on *manner* of access, not *purpose*. *See WEC*, 687 F.3d at 205.

This is additionally supported by the CFAA's definitions of "loss" and "damage." A private right of action under the CFAA requires "damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g). "Damage" means "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). If Congress meant the CFAA to provide a remedy for disloyal access to company information, it would make little sense for Congress to limit the remedy to compensation for the foregoing sorts of expenses. To the contrary, these definitions strongly suggest that Congress only meant to deter certain *means of access* (such as through hacking), not certain *purposes for access*.

Thus, the Court ultimately agrees with Second, Fourth, and Ninth Circuits' shared conclusion: "exceeds authorized access" in the CFAA does not impose criminal liability on individuals who are authorized to access company data but do so for disloyal purposes; it applies only to individuals who are allowed to access a company computer and use that access to obtain data they are not allowed to see for any purpose. Given this, Cloudpath's CFAA cause of action (Count One) is dismissed with prejudice to the extent Cloudpath alleges CFAA violations by any Defendant who was authorized to access the relevant information for at least some purpose at the time of the alleged violation. This dismissal also extends to any allegation of conspiracy to commit, or vicarious liability for, such a violation. As explained below, however, this does not entirely dispose of Count One.

4. Grimm's Post-Resignation Access

a. *Primary Liability*

Cloudpath alleges that Grimm continued to access Cloudpath information for two days *after* his resignation. (ECF No. 37 ¶¶ 85–86.) This would normally be enough to plausibly allege unauthorized access. *See SBM*, 2012 WL 628619, at *6. Defendants argue, however, that Grimm's access during those days shows that Cloudpath had not actually withdrawn his access upon resignation, and there is no allegation that Grimm "was otherwise required to relinquish access." (ECF No. 40 at 8.) In this vein, Defendants emphasize *LVRC*'s language that "'authorization' depends on actions taken by the employer." 581 F.3d at 1135.

To the extent Defendants mean to say that Cloudpath had an affirmative duty to take technical steps to prevent Grimm's further access (*e.g.*, terminating his login credentials), the Court disagrees. The CFAA says nothing about technical means of granting or preventing access.

To the extent Defendants mean to say that Cloudpath must allege that it explicitly told Grimm he could no longer access company data after terminating his employment, the Court again disagrees. Considering Cloudpath's allegations regarding (i) Grimm's role and (ii) the sensitivity and proprietary nature of the data Grimm allegedly accessed, it is more than a plausible inference that Grimm knew or should have known that his permission to access Cloudpath data turned, at a minimum, on his continuing employment. Indeed, Cloudpath alleges that, "[u]pon his termination with Cloudpath, Grimm agreed to immediately return any documents or copies thereof in his possession or control." (ECF No. 37 ¶ 44.) Assuming the truth of this allegation, as the Court must at this stage, this indicates Grimm's knowledge that he needed to return proprietary Cloudpath information—thus implying his knowledge that he no longer had permission to access proprietary Cloudpath information.

In addition, Cloudpath alleges that Grimm had authority to access company data "[s]trictly for purposes of his employment." (ECF No. 37 ¶ 43.) As discussed at length above, the CFAA does not care about Grimm's "purposes," but it certainly cares about his "employment." His employment is the basic reason why Cloudpath gave him permission to access company data at all. The Court therefore finds that Cloudpath has sufficiently alleged a CFAA violation against Grimm to the extent he accessed Cloudpath data after his resignation.[11] Defendants' Rule 12(b)(6) Motion is denied in that respect.

b. *Derivative Liability*

The CFAA extends to parties who "conspire[] to commit" any act it prohibits. 18 U.S.C. § 1030(b). Cloudpath alleges that all Defendants conspired with Grimm (and Haney) to unlawfully access Cloudpath's data. Although Cloudpath does not distinguish between conspiratorial acts taken before and after Grimm's resignation, the

[11] To maintain a civil action, the CFAA requires "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Again, "loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). Conceivably, the loss attributable solely to Grimm's alleged post-resignation conduct does not reach this threshold. But Defendants have not argued as much and there is no indication in the CFAA that Congress intended the $5,000 threshold to be jurisdictional. Accordingly, the Court will not address this issue further.

thrust of Cloudpath's FAC is that Defendants' entire course of conduct was motivated by an agreement between them to obtain data that would make their new venture more competitive. (*See, e.g.*, ECF No. 37 ¶¶ 73–75.) Accordingly, it is a fair inference that this alleged conspiracy extended to Grimm's post-resignation access.

Defendants argue that Cloudpath's CFAA conspiracy allegations specifically against SecureW2-USA "fall far short of plausibility." (ECF No. 40 at 13.) The Court finds the plausibility standard immaterial here because conspiracy liability, under the circumstances, would be functionally no different than vicarious liability, and Cloudpath has sufficiently pleaded SecureW2-USA's potential vicarious liability for Grimm's alleged post-resignation conduct. (*See* ECF No. 46 at 14.) Cloudpath alleges that Grimm joined SecureW2-USA no later than the day after he resigned from Cloudpath. (ECF No. 37 ¶¶ 82, 84.) If SecureW2-USA encouraged Grimm's post-resignation access, which is a reasonable inference from the FAC, then SecureW2-USA may be vicariously liable for the alleged CFAA violation. *See SBM*, 2012 WL 628619, at *6; *see also Charles Schwab & Co., Inc. v. Carter*, 2005 WL 2369815, *7 (N.D. Ill. Sept. 27, 2005).

Defendants have not argued that Cloudpath's derivative liability allegations fail as to any other Defendant. Cloudpath has therefore sufficiently alleged such liability against all Defendants. Defendants' Rule 12(b)(6) Motion is denied in that respect as well.

5. SecureW2's Use of Kashyap's Login Credentials

Cloudpath also claims that, between June 2012 in January 2013, someone other than Kashyap used Kashyap's Cloudpath login credentials to access Cloudpath's proprietary data. (ECF No. 37 ¶¶ 54–57.) Given Kashyap's alleged relationship to SecureW2, Cloudpath suspects that SecureW2 was the perpetrator, in conspiracy with Kashyap. (*Id.* ¶¶ 51, 53, 58–59, 63.) These allegations are plausibly pleaded. As such, they state a CFAA claim against SecureW2 for accessing Cloudpath's data without authorization, and against Kashyap for conspiracy to enable such access. Defendants' Rule 12(b)(6) Motion is also denied in that respect.

C. ECPA Claim (Count Two)

The Electronic Communications Privacy Act (ECPA) prohibits "intentionally intercept[ing] . . . any wire, oral, or electronic communication" without certain forms of authorization. 18 U.S.C. § 2511(1)(a). A private party damaged by such conduct may bring a civil lawsuit. *See id.*§ 2520. Defendants argue that Cloudpath's ECPA claim fails because Cloudpath has not alleged any interception of wire, oral, or electronic communications.

The ECPA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). Defendants argue (*see* ECF No. 40 at 9–10), and Cloudpath does not dispute, that this definition requires interception contemporaneous with transmission. *See, e.g.*, *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission."); *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) ("interception includes accessing messages in transient storage on a server during the course of transmission, but does *not* include accessing the messages stored on a destination server" (emphasis in original)).

Cloudpath attempts to fit its allegations into this definition, but ultimately fails. Cloudpath points to its allegations that Kashyap "redirected individuals who contacted him in his capacity as a sales agent of Cloudpath," encouraging them to purchase SecureW2's competing product instead, and that Kashyap "over quoted Cloudpath's product price to potential customers and failed to respond to customer, potential customer and partner requests and removed legal terms and conditions from customer quotations." (ECF No. 37 ¶¶ 64, 66.) These are not examples of interception contemporaneous with transmission. Moreover, from Cloudpath's allegations, it appears that Kashyap was the intended recipient of these communications. Accordingly, these allegations do not demonstrate interception within the meaning of the ECPA.

Cloudpath also points to its allegations that Grimm and Haney corrupted and altered certain data stored on third-party servers, thereby preventing accurate data from being transmitted from those servers to Cloudpath. (*Id.* ¶¶ 120–21; ECF No. 46 at 10.) But again, this only alleges that Grimm and Haney prevented communication from happening in the first place, not that they intercepted communication as it was being transmitted.

Because Cloudpath has failed to allege that any Defendant intercepted a communication within the meaning of the ECPA, Cloudpath's ECPA cause of action (Claim Two) is dismissed with prejudice.

D. SCA Claim (Count Three)

The Stored Communications Act (SCA) prohibits "intentionally access[ing] without authorization," and "intentionally exceed[ing] an authorization to access," any "facility through which an electronic communication service is provided," and "thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). This is a confusingly worded statute. For example, how does one "intentionally access[]" something "without authorization" and "thereby obtain[] . . . authorized access"? Luckily, the nature of Cloudpath's SCA allegations do not require the Court to resolve this conundrum.

Cloudpath argues that it has stated an SCA claim through its allegations that:

- "Kashyap redirected individuals who contacted him in his capacity as a sales agent of Cloudpath and expressed interest in purchasing Cloudpath products and services to purchase [SecureW2's] product instead";
- "[p]rior to his departure, Kashyap attempted to delete all of his emails from his Cloudpath account";
- "[f]rom September 2014 through his sudden resignation on January 5, 2015, Grimm took multiple actions, including but not limited to . . . deleting and corrupting[] sales leads and customer information from Cloudpath's Salesforce customer tracking software, [and] downloading and then deleting his entire email account (including sent and incoming mail) off of Cloudpath's email server"; and

- "[b]etween December 1 and December 19, 2014, Grimm deleted over 2,200 customer leads and contacts from Salesforce."

(ECF No. 37 ¶¶ 64, 67, 78, 80; *see also* ECF No. 46 at 11–13.) These allegations fail to show that Kashyap and Grimm lacked authorization to access any of the deleted or altered materials, except in the sense advanced in Cloudpath's CFAA argument (*i.e.*, that "exceeds authorized access" is connected to purposes rather than permission to access a computer). However, as other courts have recognized, the CFAA's "exceeds authorized access" phrase and the SCA's "exceeds an authorization to access" phrase are analogous. *See, e.g.*, *Cheng v. Romo*, 2012 WL 6021369, at *3 (D. Mass. Nov. 28, 2012). Having already interpreted the CFAA to foreclose Cloudpath's theory, the Court interprets the SCA in the same manner.

Cloudpath's allegations demonstrate that Kashyap and Grimm possessed authorized access, even if they misused it. Thus, Cloudpath's SCA cause of action (Count Three) must be dismissed with prejudice.

IV. CONCLUSION

For the reasons set forth above, the Court ORDERS as follows:

1. Defendants' Rule 12(b)(6) Motion to Dismiss Amended Complaint (ECF No. 40) is GRANTED IN PART and DENIED IN PART;
2. Cloudpath's Count One is DISMISSED WITH PREJUDICE IN PART and SUSTAINED IN PART to the extent explained in Part III.B, *supra*;
3. Cloudpath's Counts Two and Three are DISMISSED WITH PREJUDICE; and

4. Defendant SecureW2 B.V.'s Rule 12(b)(2) Motion to Dismiss Amended Complaint (ECF No. 58) is DENIED.

Dated this 13th day of January, 2016.

BY THE COURT:

William J. Martínez
United States District Judge