IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

TLS MANAGEMENT AND MARKETING SERVICES LLC, Plaintiff, v. **RICKY RODRIGUEZ-TOLEDO**, *et al.*, Defendants.	Civil No. 15-2121 (BJM)

OPINION AND ORDER

Alleging violations of Titles I and II of the Electronic Communications Privacy Act ("ECPA") and various Puerto Rico statutes,[1] TLS Management and Marketing Services LLC ("TLS") brought this action against Ricky Rodriguez-Toledo ("Rodriguez"), Lorraine Ramos ("Ramos"), the alleged conjugal partnership between Rodriguez and Ramos, Miguel A. Santo Domingo-Ortiz ("Santo Domingo"), Mari Lourdes Cardona-Jimenez ("Cardona"), the Santo Domingo-Cardona conjugal partnership, ASG Accounting Solutions Group, Inc. ("ASG"), Global Outsourcing Services LLC ("GOS"), Global Tax Strategy, Sandpiper LLC, and three unidentified insurance companies. Docket No. 74 ("Am. Compl."). Defendants[2] moved to dismiss the amended complaint for failure to state a claim, Docket Nos. 78, 79, 98–100, and TLS opposed. Docket No. 111. The case is before me on consent of the parties. Docket No. 93.

For the reasons set forth below, the motions to dismiss are **GRANTED IN PART AND DENIED IN PART**.

[1] The amended complaint alleges: violation of the Puerto Rico Commercial and Industrial Trade Secret Protection Act, P.R. Laws Ann. tit. 10 §§ 4131–4141; breach of contract, in violation of Articles 1044, 1054, 1077 and 1206 of the Puerto Rico Civil Code, P.R. Laws Ann. tit. 31 §§ 2994, 3018, 3052, 3371; conversion, in violation of Article 1802 of the Puerto Rico Civil Code, P.R. Laws Ann. tit. 31, § 5141; and tortious interference with various contracts, in violation of Article 1802 of the Puerto Rico Civil Code. P.R. Laws Ann. tit. 31, § 5141.

[2] The parties voluntarily agreed to dismiss without prejudice the claims against Global Tax Strategy, the alleged Rodriguez-Ramos conjugal partnership, and Sandpiper LLC. Docket Nos. 117, 126.

MOTION TO DISMISS STANDARD

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), "an adequate complaint must provide fair notice to the defendants and state a facially plausible legal claim." *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 12 (1st Cir. 2011). To do so, the complaint must set forth "factual allegations, either direct or inferential, regarding each material element necessary" for the action. *Gooley v. Mobil Oil Corp.*, 851 F.2d 513, 514 (1st Cir. 1988). When evaluating the complaint, the court first discards any "'legal conclusions couched as fact' or 'threadbare recitals of the elements of a cause of action.'" *Ocasio-Hernández*, 640 F.3d at 12 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). The remaining "[n]on-conclusory factual allegations" are fully credited, "even if seemingly incredible." *Ocasio-Hernández*, 640 F.3d at 12. The court engages in no fact-finding when considering the motion, and does not "forecast a plaintiff's likelihood of success on the merits." *Id.* at 13. Rather, the court presumes that the facts are as properly alleged by the plaintiff, and draws all reasonable inferences in the plaintiff's favor. *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012).

BACKGROUND[3]

TLS is a Puerto Rico limited liability company that employs tax lawyers, tax accountants, and business executives to provide tax planning and consulting services. Am. Compl. ¶¶ 11, 24. TLS has developed tax strategies, insurance strategies, customer lists, and other confidential information, and has stored that information on an online business account at the domain name "Dropbox.com" ("Dropbox").[4] *Id.* ¶¶ 60, 61. TLS's Dropbox is for the "exclusive use" of its employees, and Dropbox requires a business account to be used "in compliance with" an employer's "terms and policies." *Id.* ¶¶ 60, 75.

[3] This narrative is based on the well-pleaded allegations in the amended complaint. Docket No. 74.

[4] Dropbox "is a cloud storage product that allows a user to create an account to save and store digital content, including images and videos, in folders, and to share that content by providing others with the email address and password used to log in to the account." *United States v. Wilson*,—— F. Supp. 3d ——, 2016 WL 6683268, at *2 (D.D.C. Nov. 14, 2016).

ASG employs certified public accountants and offers, among other things, tax planning and tax preparation services. *Id.* ¶ 26. Rodriguez previously served as the "principal director" for ASG, while Ramos remains a "principal" for this company. *Id.* ¶¶ 13, 27, 65. In March 2012, TLS offered Rodriguez the company's "finance director" position, subject to his execution of a confidentiality and nondisclosure agreement. *Id.* ¶¶ 12, 28. Rodriguez accepted the offer, and was set to start the new position in August 2012. *Id.* ¶ 28. When Rodriguez accepted the offer, he also executed a subcontractor agreement between TLS and ASG ("Subcontractor Agreement"). *Id.* ¶ 29.

Under the Subcontractor Agreement, ASG was required to perform various tasks for the benefit of TLS, such as developing cash flow and financial models that projected the value of TLS's services to prospective clients. *Id.* ¶ 30. The Subcontractor Agreement prohibited ASG from disclosing confidential information, restricted the use of that information "for a purpose that is necessary in carrying out the provisions of th[e] agreement," and required ASG to inform TLS of any unauthorized disclosures of the confidential information. *Id.* ¶¶ 31–33. *Confidential information* was defined broadly to include information like TLS's "business methods" and "clients or prospective clients." *Id.* ¶ 32. Works made for hire under the Subcontractor Agreement were also classified as confidential. *Id.* ¶¶ 34, 35. The Subcontractor Agreement additionally required Rodriguez to return all confidential information upon the termination of his employment with TLS. *Id.* ¶ 40.

Rodriguez also executed a noncompetition agreement that "survive[d]" the termination of the Subcontractor Agreement. *Id.* ¶ 36. In July 2012, Rodriguez requested that he be allowed to commence employment with TLS in September 2012, and agreed to extend the Subcontractor Agreement until the beginning of that month. *Id.* ¶ 41. In August 2012, TLS offered Rodriguez a different position: he was offered the company's "managing director" position, so long as he signed a confidentiality and nondisclosure agreement. *Id.* ¶ 42. Rodriguez's nondisclosure agreement prohibited him from disclosing confidential

information (which was defined broadly to include things like TLS's "business methods" and "clients or prospective clients"), and required him to notify TLS of any disclosure of confidential information. *Id.* ¶¶ 45, 47. Rodriguez accepted the offer, and agreed to begin working as TLS's managing director in early September 2012. *Id.* ¶ 42. As the managing director, Rodriguez was issued a laptop, TLS e-mail account, and other equipment. *Id.* ¶ 50.

Alleged Unauthorized Access & Copying

Between February 2014 and January 2015, Rodriguez allegedly copied TLS's confidential information and allowed others to do the same. *Id.* ¶¶ 2–4, 58, 67–78. Some of this copying required access to TLS's Dropbox, and Rodriguez allegedly allowed others to access the Dropbox in his capacity as the "administrator" of the Dropbox account. *Id.* ¶¶ 2–4, 58, 67–78. The amended complaint identifies several incidents. First, in February 2014, Rodriguez "linked a device" owned by Ramos to TLS's Dropbox, and Ramos accessed the Dropbox sometime thereafter. *Id.* ¶¶ 4, 67. Ramos has never been an employee of TLS, and Rodriguez was not authorized to give Ramos access to the Dropbox. *Id.* ¶¶ 67, 76. And before he resigned from TLS, Rodriguez attempted to delete Ramos as a user of TLS's Dropbox. *Id.* ¶ 67. He also unlinked Ramos's device from TLS's Dropbox, which prevented TLS from remotely wiping the data transferred to Ramos's device. *Id.* ¶ 67.

Rodriguez's Dropbox log revealed that he linked several persons to TLS's Dropbox account. *Id.* ¶ 74. Rodriguez was not authorized to obtain information from Dropbox for purposes other than his duties as TLS's consultant and managing director. *Id.* ¶ 76. Yet, between April and August 2014, Rodriguez allowed Santo Domingo to access TLS's Dropbox, and the latter's personal e-mail address was used to access the Dropbox account.[5]

[5] Santo Domingo became an advisor at TLS in February 2013. *Id.* ¶¶ 52–54. Before commencing his employment with TLS, Santo Domingo signed a confidentiality and noncompetition agreement that included confidentiality provisions identical to the ones in the Subcontractor Agreement executed by Rodriguez. *Id.* ¶¶ 52–54.

Santo Domingo was able to access certain folders, including the contents of a folder titled "Tax Exemption Docs." *Id.* ¶ 70.

In April 2014, TLS's co-owner, David Runge ("Runge"), discussed with Rodriguez via e-mail "a new tax and insurance structure [that] TLS was studying." *Id.* ¶ 72. A few months later, in October 2014, Rodriguez sent TLS's confidential information from his TLS-issued e-mail address to his ASG-issued e-mail address. *Id.* ¶¶ 58, 68. Rodriguez also downloaded TLS's confidential information, including TLS's client e-mail list, by connecting USB or "flash storage" devices not issued by TLS "into his computer."[6] *Id.* ¶¶ 59, 73, 78. The last time Rodriguez did this was a few days before he resigned from TLS in January 2015. *Id.* ¶¶ 59, 78.

TLS would later discover one of Rodriguez's notes in TLS's Dropbox that detailed plans for a new business, referenced a "buy/sell agreement" (which TLS uses in all its tax and insurance products), and described a website design at the domain name "Global Tax Strategy.com." *Id.* ¶¶ 69, 71. Sometime after Rodriguez resigned from TLS in January 2015, Global Tax Strategy (which is run by Rodriguez and Santo Domingo) began operating a website. *Id.* ¶¶ 78, 79. That website included a section detailing the confidential insurance strategy Rodriguez and Runge discussed in April 2014. *Id.* ¶ 80. Global Tax Strategy's website also copied TLS's sales channels, which "work through" various financial advisors and marketing organizations known as "FMOs." *Id.* ¶ 81.

TLS Loses Clients

TLS alleges that Rodriguez has formed new companies (namely, GOS and Global Tax Strategy) since resigning from TLS, and that these new companies are eating TLS's lunch. *Id.* ¶¶ 83–91. In February 2015, for example, Rodriguez attempted to offer GOS's services to Ora Goldman, one of TLS's clients, via an e-mail sent from a GOS-issued e-mail address. *Id.* ¶ 82. Rodriguez was identified in that e-mail as GOS's "managing

[6] It is unclear from the allegations in the amended complaint whether the computer at issue was Rodriguez's personal computer or a TLS-issued computer. *See id.* ¶ 59.

director." *Id.* ¶ 82. In addition, in June 2015, Harris Hospice, Inc. terminated TLS's services, and the client's president, Jay Harris, requested that his membership interest in TLS be assigned to Sandpiper LLC, a company where Rodriguez is an "authorized person." *Id.* ¶¶ 83, 84. At least two other clients of TLS also terminated their service agreements and requested that their membership interests in TLS be transferred to companies in which Rodriguez is listed as an "authorized person." *Id.* ¶¶ 85–90.

DISCUSSION

Defendants contend that the amended complaint fails to state a claim under either Titles I or II of the ECPA, and that supplemental jurisdiction should not be exercised over the state-law claims. Docket Nos. 78, 79, 100. TLS maintains that the amended complaint adequately alleges a claim under both Titles I and II of the ECPA, and that the court should exercise ancillary jurisdiction over the related local-law claims. Docket No. 111.

I. Stored Communications Act

The complaint alleges that all defendants violated the Stored Communications Act ("SCA"). 18 U.S.C. §§ 2701–2712; Am. Compl. ¶ 93. The SCA is also known as Title II of the ECPA, "which was enacted in 1986 'to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.'" *Telecomms. Regulatory Bd. of P.R. v. CTIA-Wireless Ass'n*, 752 F.3d 60, 64 (1st Cir. 2014) (quoting S. Rep. No. 99–541, at 1–2 (1986)). Title II of the ECPA "creates civil liability for one who '(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.'" *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (quoting 18 U.S.C. § 2701(a)); *see also Jewel v. NSA*, 673 F.3d 902, 912 (9th Cir. 2011) ("Congress . . . spelled out a private right of action in the . . . SCA").

A claim arising under the SCA is subject to certain statutory exceptions, 18 U.S.C. §§ 2701(c)(1)–(3), and "virtually complete immunity" extends to a defendant who has engaged in conduct covered by these exceptions. *See United States v. Councilman*, 418 F.3d 67, 81 (1st Cir. 2005) (en banc). Section 2701(c)(2), for example, states that the SCA "does not apply with respect to conduct authorized . . . by a user of th[e electronic communication] service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). After reviewing the allegations in the complaint, "courts may dismiss a claim based on a statutory exception that appears on the face of the complaint." *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001) (court concluded that communications accessed by defendant fell "under § 2701(c)(2)'s exception," that the claim was thus "outside Title II" of the ECPA, and that the claim should be dismissed); *see also Orton v. Pirro, Collier, et al.*, No. 95 Civ. 3056, 1996 WL 18831, at *2 (S.D.N.Y. Jan. 18, 1996) (ECPA Title III claim dismissed where statutory consent exception was apparent from the face of the complaint).

A. Electronic Communication Service

At the outset, defendants contend that the SCA claims must be dismissed because Dropbox is not an "electronic communication service." Docket No. 78 at 6. Defendants suggest that Dropbox is not an "electronic communication service" because it does not provide "electronic storage," as that term is statutorily defined. *Id.* An *electronic communication* is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photooptical system that affects interstate or foreign commerce," with four specific exceptions not relevant here. 18 U.S.C. § 2510(12). An *electronic communication service* is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15). And *electronic storage* is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as "any storage

of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* §§ 2510(17)(A), (B).

The amended complaint provides sufficient factual allegations to conclude that Dropbox is an "electronic communication service." First, TLS adequately alleged that electronic communications are sent via Dropbox because the amended complaint states that Dropbox allows users to send content-filled "files" and "documents" over the Internet. *See* Am. Compl. ¶¶ 100, 109; 18 U.S.C. § 2510(12); *Councilman*, 418 F.3d at 72 ("the statutory definition of 'electronic communication' is broad"). Second, TLS adequately alleged that these electronic communications are kept in *electronic storage* because the amended complaint states that "Dropbox keeps files in intermediate storage when users opt to share them" and that TLS keeps "backups" of its "documents and files" on Dropbox's "cloud-based servers." *See* Am. Compl. ¶¶ 106, 109–111; 18 U.S.C. § 2510(17).

Third, TLS adequately alleged that Dropbox is an *electronic communication service* because the amended complaint states that Dropbox stores information on a server, that such information is "conveyed from a private website to users," and that Dropbox "features elements" of e-mail and a "computer bulletin board." Am. Compl. ¶¶ 97, 99. In this vein, the amended complaint also states that "the Dropbox server transmit[s] a copy of the file to the [user's] computer; that a user "can also use automatic transmission through shared folders"; and that "documents placed in shared folders are instantly transmitted from a [user's] computer to the cloud." *Id.* ¶ 98.

Notably, the allegations in the amended complaint pertaining to Dropbox's functionality, which must be taken as true at this stage, are quite similar to other descriptions. *See Wilson*,—— F. Supp. 3d ——, 2016 WL 6683268, at *2 (Dropbox "is a cloud storage product that allows a user to create an account to save and store digital content, including images and videos, in folders, and to share that content by providing others with the email address and password used to log in to the account."). And after construing the statute's definitions in the context of a private cause of action brought under

the SCA, at least one other court has recently held that Dropbox is an "electronic communication service." *See Lane v. Brocq*, No. 15 C 6177, 2016 WL 1271051, at *6 (N.D. Ill. Mar. 28, 2016) (plaintiffs adequately stated a claim under the SCA where they alleged that the defendant "accessed electronic files stored on cloud-based servers that were connected to the [I]nternet," namely, Dropbox). Thus, the amended complaint adequately alleges that Dropbox is an "electronic communication service."

B. Defendants' Access

Ramos and Santo Domingo contend that they cannot be liable under the SCA for accessing TLS's Dropbox because Rodriguez—the administrator of the Dropbox—granted them access. "The SCA excepts from liability . . . 'conduct authorized . . . by a user of that service with respect to a communication of or intended for that user.'" *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 (9th Cir. 2002) (quoting 18 U.S.C. § 2701(c)(2)). The plain meaning of this exception "allows a person to authorize a third party's access to an electronic communication if the person is 1) a 'user' of the 'service' and 2) the communication is 'of or intended for that user.'" *Konop*, 302 F.3d at 880. A "user" is defined as "any person or entity who—(A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13); *see also Konop*, 302 F.3d at 880 ("there is some indication in the legislative history that Congress believed 'addressees' or 'intended recipients' of electronic communications would have the authority under the SCA to allow third parties access to those communications").

In *Konop*, for example, the plaintiff (Konop) "created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union, Air Line Pilots Association." 302 F.3d at 872. "Konop controlled access to his website by requiring visitors to log in with a user name and password." *Id.* at 873. He also "created a list of people . . . who were eligible to access the website," and that list included "Gene Wong and James Gardner." *Id.* at 873. Later, "James Davis asked Wong for permission to

use Wong's name to access Konop's website" and "Wong agreed." *Id.* With Gardner's permission, Davis also accessed Konop's website with Gardner's credentials. *Id.* Under these circumstances, "the district court concluded that Wong and Gardner had the authority under § 2701(c)(2) to consent to Davis' use of the website because Konop put Wong and Gardner on the list of eligible users." *Id.* at 880.

The district court's decision was appealed. After assuming that Davis's conduct constituted access without authorization to a facility through which an electronic communication service was provided, the Ninth Circuit determined that the district court's "conclusion [was] consistent with other parts of the Wiretap Act and the SCA which allow intended recipients of wire and electronic communications to authorize third parties to access those communications." *Id.* Yet, the Ninth Circuit remanded the case because it was unclear from the record whether and when Wong and Gardner were "user[s]" of Konop's website. *See Id.* After the case returned to the lower court, it was determined that Gardner was indeed a "user" of Konop's website and that Gardner authorized Davis to use Konop's website. *See In re Hawaiian Airlines, Inc.*, 401 F. App'x 242, 243 (9th Cir. 2010). This being the case, the lower court and the Ninth Circuit determined that there was no liability under the SCA when Davis accessed Konop's website using Gardner's password. *Id.*

The allegations in the amended complaint state that "Dropbox is a facility through which an electronic communication service is provided." Am. Compl. ¶ 100. It is further alleged that Rodriguez "was granted access to TLS's business Dropbox account, where the" confidential information was stored, and that Rodriguez accessed the Dropbox in February 2014. *Id.* ¶¶ 51, 67. These allegations establish that Rodriguez was a "user" of TLS's Dropbox. *See* 18 U.S.C. § 2510(13). Moreover, the amended complaint also alleges that Rodriguez, via his capacity as administrator, allowed Ramos and Santo Domingo to access TLS's Dropbox. Am. Compl. ¶¶ 113, 117.

Even assuming that TLS is correct in arguing that the access given to Santo Domingo and Ramos was "without authorization," this alleged conduct falls within the

statutory exception of § 2701(c)(2) because—as in *Konop* and *Hawaiian Airlines*—Rodriguez, who was an authorized user of the Dropbox, allowed Ramos and Santo Domingo to view a communication "intended for" a user of the electronic communication service. *See* 18 U.S.C. § 2701(c)(2). Similarly, Rodriguez did not incur liability under the SCA by allowing others to access the Dropbox because the face of the amended complaint reveals that he was an authorized user of the Dropbox. *See Konop*, 302 F.3d at 880 ("the district court [correctly] concluded that Wong and Gardner had the authority under § 2701(c)(2) to consent to Davis' use of the website *because Konop put Wong and Gardner on the list of eligible users*.") (emphasis added). Because the allegations necessary to determine whether the statutory exception is applicable appear on the face of TLS's amended complaint, the SCA claims against Santo Domingo, Ramos, and Rodriguez are dismissed.[7] *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 507 (court concluded that communications accessed by defendant fell "under § 2701(c)(2)'s exception," that the claim was thus "outside Title II" of the ECPA, and that the claim should be dismissed).

To be sure, TLS presses that Rodriguez abused his access to the confidential information in the Dropbox. The allegations relating to the *misuse* of confidential information are inadequate to state a claim under Title II, for the SCA "prohibits only unauthorized access and not the misappropriation or disclosure of information." *See, e.g.*, *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) ("there is no violation of section 2701 [by] a person with authorized access to the database no matter how malicious or larcenous his intended use of that access"). Put another way, the SCA is "violated when 'the trespasser gains access to information to which

[7] The SCA claims against ASG, GOS, Cardona, and the Santo Domingo-Cardona conjugal partnership are tied to the conduct of Rodriguez, Ramos, and Santo Domingo, and so those SCA claims are also dismissed. *See* Am. Compl. ¶¶ 16, 122. Cardona also argues that the amended complaint fails to allege any specific conduct for which she is liable. Docket No. 98. Because the amended complaint makes only cursory references to Cardona and fails to allege any specific conduct for which she is liable, all claims against her are dismissed.

he is not entitled to see, not [when] the trespasser uses the information in an unauthorized way.'" *Bovino v. MacMillan*, 28 F. Supp. 3d 1170, 1177 (D. Colo. 2014) (quoting *Int'l Ass'n of Machinists & Aerospace Workers v. Werner–Masuda*, 390 F. Supp. 2d 479, 497 (D. Md. 2005) (internal quotation marks omitted)) Thus, the SCA claims against all defendants are dismissed.

II. Wiretap Act

TLS brought the Wiretap Act claims against all the defendants that remain in this action, except Cardona and the Cardona-Santo Domingo conjugal partnership. *See* Am. Compl. ¶ 125. The ECPA amended the Federal Wiretap Act, 18 U.S.C. §§ 2510–2522, "by extending to data and electronic transmissions the same protection already afforded to oral and wire communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). Because the "1968 Wiretap Act [w]as amended by Title I of the ECPA," Title I of the ECPA is also known as the Wiretap Act. *See Councilman*, 418 F.3d at 81 n.15; *In re Pharmatrak, Inc.*, 329 F.3d at 18. "The post-ECPA Wiretap Act provides a private right of action against one who 'intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.'" *In re Pharmatrak, Inc.*, 329 F.3d at 18 (quoting 18 U.S.C. § 2511(1)(a), and citing 18 U.S.C. § 2520 (provides a private right of action)).

To state a claim "under Title I of the ECPA," the plaintiff's complaint must allege "that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." *See In re Pharmatrak, Inc.*, 329 F.3d at 18. *Intercept* is defined 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." 18 U.S.C. § 2510(4). And, like a claim arising under the SCA, a claim under the Wiretap Act "is subject to certain statutory exceptions, such as consent." *See In re Pharmatrak, Inc.*, 329 F.3d at 18; *see also United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998) ("the

intersection of the Wiretap Act . . . and the Stored Communications Act . . . is a complex, often convoluted, area of the law").

The amended complaint essentially alleges that Rodriguez *intercepted* an electronic communication, and that the other defendants, with the help of Rodriguez, endeavored to intercept TLS's confidential information from the Drobox. Am. Compl. ¶ 128. Defendants assert that the amended complaint inadequately alleges the second element of a claim under the Wiretap Act. Docket No. 79 at 12–14. In essence, they argue that the "Wiretap Act requires allegations that Rodriguez intercepted communications in flight" or "contemporaneous" with transmission, and that the Wiretap Act does not encompass any interceptions that occur while the electronic communications are "in electronic storage." Docket No. 78 at 14. In support of this theory, defendants rely on cases like *Konop*, 302 F.3d at 877, and *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994). Endorsing "the reasoning of *Steve Jackson Games*," the Ninth Circuit held that "to be 'intercepted' in violation of the Wiretap Act, [the electronic communication] must be acquired during transmission, not while it is in electronic storage." *See Konop*, 302 F.3d at 878.

While the defendants' position is not entirely untenable, they have not presented a persuasive argument for dismissing all the Wiretap Act claims at this juncture for three reasons. First, the amended complaint specifically alleges that Dropbox keeps "files in intermediate storage" and that Rodriguez, Ramos, and Santo Domingo used their computers to "acquire TLS's electronic communications *contemporaneously* with their transmission to TLS's Dropbox." Am. Compl. ¶¶ 106, 131 (emphasis added). In this vein, TLS further alleged that Rodriguez was able "to intercept copies of messages within a second of each message's arrival and assembly in its intended destination," and that "[o]nce a document was stored in a shared folder, Dropbox *contemporaneously* transmitted copies to the[defendants'] computers and other linked devices." *Id.* ¶¶ 130, 131 (emphasis added). These allegations, when read in context, suggest that (1) Rodriguez intercepted electronic

communications *before* they arrived to their final destination, and (2) that these interceptions occurred *contemporaneous* with the transmission of the electronic communications.

And though defendants dispute the allegations in the amended complaint that relate to Dropbox's functionality, this factual dispute may not be resolved when evaluating a motion to dismiss for failure to state a claim. *See, e.g.*, *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999) (court evaluating a Rule 12(b)(6) motion "does not resolve contests surrounding the facts"). For example, after saying that TLS "goes at great length[s] to portray Dropbox'[s] features as those of a temporary, intermediate storage, incidental to electronic transmission," defendants argue that, in actuality, "Dropbox is a permanent electronic storage solution and not a temporary, intermediate option incidental to transmission." Docket No. 78 at 6 (bold emphasis removed). In response, TLS argues that defendants have a "basic misconception of Dropbox, its features, and its capabilities," and presses its view of Dropbox's functionality. Docket No. 111 at 1, 4.

Second, though defendants' position is supported by *Steve Jackson Games* and other cases that have followed the Fifth Circuit's approach, a *part* of the defendants' argument has been rejected by the First Circuit. *See Councilman*, 418 F.3d at 87 (Torruella, J., dissenting) ("every court that has passed upon the issue before us has reached a conclusion opposite to that of the en banc majority: that the Wiretap Act's prohibition on intercepting electronic communications does not apply when they are contained in electronic storage . . . .")(citing cases like *Steve Jackson Games* and *Konop*). In *Councilman*, the defendant argued that "Congress intended to exclude any communication that is in (even momentary) electronic storage." 418 F.3d at 72. The defendant also argued that "because the messages at issue, when acquired, were in transient electronic storage, they were not 'electronic communication[s]' and, therefore, section 2511(1)'s prohibition on 'intercept[ion]' of any 'electronic communication' did not apply." *Id.* at 79.

The First Circuit (en banc) rejected both of the defendant's arguments. *Id.* at 79–80. With respect to the first argument, the First Circuit concluded "that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications." *Id.* at 79. And as to the argument that the messages were not *intercepted*, the First Circuit reasoned that it had already rejected that argument "in holding that an e-mail message does not cease to be an 'electronic communication' during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage." *Id.* at 79. In so holding, the First Circuit noted that the appeal did "not implicate the question of whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient or, instead, extends to an event that occurs after a message has crossed the finish line of transmission (whatever that point may be)." *Id.* at 79.

Here, because the amended complaint, when read in context, alleges that Dropbox keeps files in "intermediate storage" *before* transmitting those files to other Dropbox users, the complaint adequately alleges that Dropbox uses "transient electronic storage that is intrinsic to the communication process for such communications." *See Councilman*, 418 F.3d at 79. Such allegations are sufficient to establish a Wiretap Act claim under First Circuit law. *See id.* And because the amended complaint also alleges that the alleged interceptions occurred *contemporaneous* with the transmission of the electronic communications, the court need not address at this juncture whether there would be liability under the Wiretap Act if this were not the case. *See id.* (*Councilman* court declined to address the "existence or the applicability of a contemporaneity or real-time requirement" where the "facts of th[e] case and the arguments" did not "invite consideration of" that issue).

Third, while the Wiretap Act, like the SCA, contains statutory exceptions, the allegations in the amended complaint arguably negate the applicability of the "consent" exception under Title I. *See* 18 U.S.C. § 2511(2)(d); *In re Pharmatrak, Inc.*, 329 F.3d at 18.

The Wiretap Act provides that it "shall not be unlawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.*" 18 U.S.C. § 2511(2)(d) (emphasis added). The "legislative history and caselaw" addressing this exception "make clear that the 'criminal' or 'tortious' purpose requirement is to be construed narrowly, covering only acts accompanied by a specific contemporary intention to commit a crime or tort." *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 515 ("the legislative record suggests that the element of 'tortious' or 'criminal' *mens rea* is required to establish a prohibited purpose under § 2511(2)(d)").

In this case, the amended complaint specifically alleges that "Rodríguez, Ramos, Santo Domingo, and the corporate defendants they represent . . . intercepted the [c]onfidential [i]nformation *with tortious intent*." Am. Compl. ¶ 132 (emphasis added). And they did this, the amended complaint alleges, to "benefit economically from the" confidential information "they intercepted." *Id.* ¶ 133. The amended complaint later states that this alleged tortious conduct violated several Puerto Rico statutes, including, among others, the Puerto Rico Commercial and Industrial Trade Secret Protection Act. Am. Compl. ¶¶ 138–151. These allegations, which must be taken as true, are sufficient to take the Wiretap Act claims outside the shelter of the statutory exception provided by § 2511(2)(d). *See, e.g.*, *United States v. Lam*, 271 F. Supp. 2d 1182, 1184 (N.D. Cal. 2003) (exception under § 2511(2)(d) inapplicable where codefendant recorded conversations "as a means of keeping business records for his unlawful gambling activities" and it was undisputed that the recordings were made for "an unlawful purpose"). Thus, because the defendants have failed to establish persuasively that the allegations in the amended complaint fail to state a claim under the Wiretap Act, these claims are not dismissed.

III. State-Law Claims

TLS has brought several claims arising under Puerto Rico law, and contends that supplemental jurisdiction should be exercised over these claims. The amended complaint alleges: violation of the Puerto Rico Commercial and Industrial Trade Secret Protection Act, P.R. Laws Ann. tit. 10 §§ 4131–4141; breach of contract, in violation of Articles 1044, 1054, 1077 and 1206 of the Puerto Rico Civil Code, P.R. Laws Ann. tit. 31 §§ 2994, 3018, 3052, 3371; conversion, in violation of Article 1802 of the Puerto Rico Civil Code, P.R. Laws Ann. tit. 31, § 5141; and tortious interference with various contracts, in violation of Article 1802 of the Puerto Rico Civil Code. P.R. Laws Ann. tit. 31, § 5141. Defendants did not argue that the amended complaint failed to state a claim for the local law claims; rather, they held fast to their position that the state-law claims should be dismissed because the alleged violations of Titles I and II of the ECPA failed as a matter of law. Docket Nos. 78 at 15, 79 at 5.

"A federal court exercising jurisdiction over an asserted federal-question claim must also exercise supplemental jurisdiction over asserted state-law claims that arise from the same nucleus of operative facts." *Roche v. John Hancock Mut. Life Ins. Co.*, 81 F.3d 249, 256 (1st Cir. 1996) (citing 28 U.S.C. § 1367(a) ("in any civil action of which the district courts have original jurisdiction, the district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy")). Each of the state-law claims in the amended complaint "arise from the same nucleus of operative facts" as the federal claims, and so supplemental jurisdiction will be exercised over those claims. Thus, TLS's claims arising under Puerto Rico law are not dismissed.

CONCLUSION

For the foregoing reasons, the motions to dismiss are **GRANTED IN PART AND DENIED IN PART**. The SCA claims against all defendants are **DISMISSED**. All claims against Cardona are **DISMISSED**. The Wiretap Act and state-law claims remain.

IT IS SO ORDERED.

In San Juan, Puerto Rico, this 22nd day of December 2016.

S/Bruce J. McGiverin

BRUCE J. MCGIVERIN
United States Magistrate Judge