

**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**

TLS Management and Marketing Services LLC (“TLS”) brought this action against, among others, Ricky Rodriguez-Toledo (“Rodriguez”), Lorraine Ramos (“Ramos”), Miguel A. Santo Domingo-Ortiz (“Santo Domingo”), ASG Accounting Solutions Group, Inc. (“ASG”), and Global Outsourcing Services LLC (“GOS”), alleging violation of, *inter alia*, the Wiretap Act (18 U.S.C. §§ 2510–2522) and several state-law provisions. Docket No. 74. After the Wiretap Act and state-law claims survived a motion to dismiss, Docket No. 173, Rodriguez and Ramos (collectively “defendants”) moved for summary judgment as to the Wiretap Act claim. Docket Nos. 188, 229. TLS opposed. Docket Nos. 209, 274. This case is before me on consent of the parties. Docket No. 93.

For the reasons set forth below, the motion for summary judgment is **DENIED**.

**SUMMARY JUDGMENT STANDARD**

Summary judgment is appropriate when the movant shows that “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). A dispute is “genuine” only if it “is one that could be resolved in favor of either party.” *Calero-Cerezo v. U.S. Dep’t of Justice*, 355 F.3d 6, 19 (1st Cir. 2004). A fact is “material” only if it “might affect the outcome of the suit under the governing law.” *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). The moving party has the initial burden of “informing the district court of the basis for its motion, and

identifying those portions” of the record “which it believes demonstrate the absence” of a genuine dispute of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986).

The court does not act as trier of fact when reviewing the parties’ submissions and so cannot “superimpose [its] own ideas of probability and likelihood (no matter how reasonable those ideas may be) upon” conflicting evidence. *Greenburg v. P.R. Mar. Shipping Auth.*, 835 F.2d 932, 936 (1st Cir. 1987). Rather, the court must “view the entire record in the light most hospitable to the party opposing summary judgment, indulging all reasonable inferences in that party’s favor.” *Griggs-Ryan v. Smith*, 904 F.2d 112, 115 (1st Cir. 1990). And the court may not grant summary judgment “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Anderson*, 477 U.S. at 248.

### BACKGROUND<sup>1</sup>

Broadly speaking, TLS claims that Santo Domingo, Rodriguez, Ramos, and the companies spearheaded by Rodriguez (GOS and ASG) violated the Wiretap Act by intercepting TLS’s electronic communications occurring via Dropbox,<sup>2</sup> a cloud-based

---

<sup>1</sup> Except where otherwise noted, the following facts are drawn from the parties’ Local Rule 56 submissions: defendants’ Statement of Uncontested Facts (“SUF”), Docket No. 187; TLS’s Opposing Statement of Facts (“OSF”), Docket No. 210 at 1–4; TLS’s Additional Statement of Facts (“ASF”), Docket No. 210 at 5–9; defendants’ Reply Statement of Facts (“RSF”), Docket No. 228 at 2–5; and defendants’ reply to TLS’s ASF (“RASF”), Docket No. 228 at 5–8. Local Rule 56 is designed to “relieve the district court of any responsibility to ferret through the record to discern whether any material fact is genuinely in dispute.” *CMI Capital Market Inv. v. Gonzalez-Toro*, 520 F.3d 58, 62 (1st Cir. 2008). It requires a party moving for summary judgment to accompany its motion with a brief statement of facts, set forth in numbered paragraphs and supported by citations to the record, that the movant contends are uncontested and material. D.P.R. Civ. R. 56(b), (e). The opposing party must admit, deny, or qualify those facts, with record support, paragraph by paragraph. *Id.* 56(c), (e). The opposing party may also present, in a separate section, additional facts, set forth in separate numbered paragraphs. *Id.* 56(c). Although defendants also attempted to shoehorn additional facts into the record via a “sur-reply” to TLS’s ASF, Local Rule 56 does not allow the filing of such a statement. Because Local Rule 56 does not permit the filing of this statement, because defendants proffer insufficient justification for omitting these facts from the SUF, and because defendants effectively attempt to expand the evidentiary record by skirting the mechanism set by Local Rule 56, this statement will be disregarded. Docket No. 228 at 9–13. To be sure, even assuming *arguendo* that the statements in defendants’ “sur-reply” could be considered, the statements would—at best—only serve to create genuine disputes of material fact.

<sup>2</sup> Dropbox is “a web-based file hosting service that uses ‘cloud’ storage to enable users to store and share files with others across the Internet using file synchronization.” *See Frisco Med. Ctr., L.L.P. v. Bledsoe*, 147 F. Supp. 3d 646, 652 (E.D. Tex. 2015).

Internet service permitting storage and sharing of electronic files across multiple devices. Docket No. 210-1 at 8–9. Defendants’ summary judgment motion homes in solely on the Wiretap Act’s requirement that an electronic communication be *intercepted*. So, after addressing two matters affecting the scope of the motion before the court, only the background relevant to the Wiretap Act’s interception requirement need be addressed.

### ***Threshold Matters***

Defendants initially filed a seven-page motion for summary judgment that zeroed in on the Wiretap Act’s interception requirement. *See* Docket No. 188 at 4–7. But, after TLS’s opposition responded to that sole contention, defendants changed horses and asserted, in a 17-page reply brief, several new bases for dismissing TLS’s Wiretap Act claim; bases that could have been—but were not—raised in defendants’ initial motion for summary judgment. *Compare* Docket No. 188, *with* Docket No. 229. Because “legal argument[s] . . . raised for the first time in a reply brief” may be “considered waived for the purpose of” the motion at issue, these new, belated contentions need not be addressed. *NExTT Sols., LLC v. XOS Techs., Inc.*, 113 F. Supp. 3d 450, 458 (D. Mass. 2015); *see also* *Rivera-Muriente v. Agosto-Alicea*, 959 F.2d 349, 354 (1st Cir. 1992) (“legal argument made for the first time in an appellant’s reply brief comes too late and need not be addressed”).

In replying to TLS, defendants attempted to bypass procedural rules twice more. First, and as noted above, defendants improperly attempted to file a “sur-reply” to TLS’s additional statement of facts—although such a statement is not permitted by Local Rule 56. *See* D.P.R. Civ. R. 56. Second, defendants’ reply statement of facts relies on an expert report that jettisons the court’s “[s]cheduling [o]rder and constitutes a backdoor attempt to offer new theories and opinions.” *See* *Advanced Analytics, Inc. v. Citigroup Glob. Markets, Inc.*, 301 F.R.D. 31, 39 (S.D.N.Y. 2014). Per the court’s scheduling order, expert witness reports were required to be served by early December 2016. Docket No. 117. Yet, when defendants moved for summary judgment in late January 2017, they also moved to expand the time to serve expert reports. Docket No. 189. That request was denied, Docket No. 244,

and so the expert report proffered by defendants in April 2017, as well as any statements based on this report, will be disregarded when evaluating the summary judgment motion. *See Fernandez-Salicrup v. Figueroa-Sancha*, 790 F.3d 312, 319–22 (1st Cir. 2015) (court did not abuse its discretion at summary judgment stage by excluding statements of material fact relying on expert report where party failed to produce report before court-ordered deadline). As a corollary, the court will deem admitted TLS-proffered facts based on expert opinions if those facts are not disputed by contrary evidence calling for an expert opinion.

### ***Interception of Electronic Communications***

Rodriguez (a “principal” for ASG and a managing director for GOS) and Ramos (a “principal” for ASG) accessed TLS’s Dropbox account using an ASG-issued laptop controlled by Rodriguez. ASF ¶¶ 2–4; RASF ¶¶ 2–4. ASG was granted limited authorization to access TLS’s Dropbox, and could use TLS’s confidential information only as necessary under ASG’s subcontractor agreement. ASF ¶¶ 5, 6; RASF ¶¶ 5, 6. Rodriguez created user accounts on the Dropbox for non-TLS employees—allowing them to view, copy, and download shared folders into their devices. ASF ¶ 14; RASF ¶ 14; SUF ¶ 3.

In July 2014, Rodriguez created a folder on TLS’s Dropbox titled “Global Outsourcing Services”—i.e., GOS—and saved several of TLS’s files in that folder. ASF ¶¶ 15, 16; RASF ¶ 15, 16. Although defendants conclusorily assert that not “all” these files constituted TLS’s confidential information, RASF ¶ 16, Rodriguez fails to identify which documents do not qualify as TLS’s confidential information and fails to proffer evidence that would negate the reasonable inference that at least *some* of the copied documents constituted TLS’s confidential information. *See* RASF ¶ 16; Docket No. 228-1 ¶¶ 44, 45. What is more, Rodriguez was not permitted to share indiscriminately with Ramos and ASG all the confidential information that he copied into the GOS folder.<sup>3</sup> ASF ¶ 17.

---

<sup>3</sup> Although defendants deny ASF ¶ 17, their opposing statement, RASF ¶ 17, fails to provide a contrary statement of fact, and, instead, directs the court to ferret through several paragraphs in a declaration. This tactic improperly asks the court to guess what issue of fact is

TLS commenced this action in August 2015. Docket No. 1. In September 2015, TLS sent defendants letters asking them to “preserve all documents, data, and electronic information from all sources related to the subject matter of this litigation.” ASF ¶ 9; RASF ¶ 9. And these letters specifically notified defendants that such information could be stored on “laptop computers” and “personal computers used and accessed at home and elsewhere.” ASF ¶ 9; RASF ¶ 9. Notwithstanding—in November 2015—Rodriguez and Ramos discarded a laptop (the “Laptop”) they used to access TLS’s Dropbox. ASF ¶¶ 11, 13; RASF ¶¶ 11, 13. TLS’s Dropbox log shows that several devices—particularly, the Laptop—were synched to TLS’s Dropbox. SUF ¶¶ 1, 2; ASF ¶ 18; RASF ¶ 18.

TLS’s expert opined that a computer’s Dropbox application “contemporaneously downloads the electronic communications transmitted to linked Dropbox folders to each device that has” the application. ASF ¶ 20; RASF ¶ 20. Accordingly, “the electronic communications transmitted to shared folders are automatically downloaded to the hard drives of the users’ synched devices.” ASF ¶ 20; RASF ¶ 20. For this reason, according to TLS’s expert, “TLS’s electronic communications would have been intercepted if the Laptop, which was linked to TLS’s Dropbox Account, had the Dropbox application and was active when any electronic information was transmitted to its synched shared folders.” ASF ¶ 21; RASF ¶ 21. And so, for example, when a document file was “transmitted to a shared folder,” the “synched folder in the Laptop would contemporaneously receive the same electronic communication” and download a “copy to its hard drive.” *Id.*

In light of the above, TLS’s expert “would have been able to opine that [d]efendants engaged in the contemporaneous interception of TLS’s electronic communications if he could have inspected the Laptop.” ASF ¶ 19; RASF ¶ 19. In this vein, defendants add that TLS’s expert did not have an opportunity to examine the Laptop because, when he issued

---

disputed, and so ASF ¶ 17 is deemed admitted. *See CMI Capital Market Inv.*, 520 F.3d at 62 (court need not “ferret through the record to discern whether any material fact is genuinely in dispute”). Defendants used a similar tactic for RASF ¶¶ 21–24, and so ASF ¶¶ 21–24 are deemed admitted.

the report in December 2016, defendants had already “discarded” the Laptop. RASF ¶ 19. TLS’s expert opined that certain folders were “programmed” to “synch” to the Laptop. ASF ¶ 22; RASF ¶ 22. But TLS’s expert opined that, without studying the Laptop’s “analytic data,” he cannot “determine if the Laptop was powered on and had the Dropbox application when electronic communications were transmitted to the [certain] folders” on TLS’s Dropbox. ASF ¶ 22; RASF ¶ 22. And, for the same reason, TLS’s expert cannot “determine if [d]efendants’ interceptions were contemporaneous.” ASF ¶ 22; RASF ¶ 22.

With access to the Laptop, on the other hand, TLS’s expert could have determined whether the Laptop was powered on and had the Dropbox application when electronic communications were transmitted to the GOS folder or any other folder on TLS’s Dropbox. Had TLS’s expert confirmed that these conditions were met after inspecting the Laptop, he would have opined that “any electronic communication transmitted to the folder[s] would have instantly downloaded to the Laptop” and that such transmission “would have constituted a contemporaneous interception of TLS’s electronic communications.” ASF ¶ 23; RASF ¶ 23. But alas, according to TLS’s expert, there is “no other way” to determine whether the electronic communications were contemporaneously intercepted. ASF ¶ 24.

TLS previously moved for spoliation sanctions against defendants for discarding the Laptop, and, after considering defendants’ allegedly innocuous reasons for chucking the Laptop, I found that Rodriguez acted with the intent to deprive TLS from using information electronically stored on the Laptop. Docket Nos. 133, 138, 152, 212. And, because the Laptop was effectively ditched in bad faith, I also found that this spoliation warranted TLS’s requested adverse-inference instruction. *See* Docket No. 212 at 2, 5. The parties rehash many of the same arguments I previously considered, and I find insufficient evidence to disturb the spoliation-based adverse inference. Docket Nos. 212, 277.

## **DISCUSSION**

Defendants contend that summary judgment is warranted because no reasonable jury could find that they violated the Wiretap Act’s interception requirement. Docket No.

188. TLS retorts that defendants deprived them of critical evidence necessary to establish the Wiretap Act claim, and that the spoliation-based adverse inference—coupled with the other record evidence—allows TLS to survive defendants’ motion for summary judgment.

The Electronic Communications Privacy Act (“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 United States v. Councilman*, 418 F.3d 67, 81 n.15 (1st Cir. 2005) (en banc). “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 (statutory provision blessing a private right of action)).

To establish a Wiretap Act claim, a plaintiff must show “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).

The Fifth Circuit and several others have “approved the judicial definition of ‘intercept’ as acquisition contemporaneous with transmission.” *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994). And, although the First Circuit held in *Councilman* that electronic communications may be intercepted even if they “were in transient electronic storage,” that case 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).” 418 F.3d at 79–80. For this reason, the First Circuit (en banc) declined to decide “either the existence or the applicability of a contemporaneity or real-time requirement.” *See id.* at 80.

In this case, TLS’s expert opined that the Dropbox application on a device “*contemporaneously* downloads the electronic communications transmitted to linked Dropbox folders to each device that has” installed the application. ASF ¶ 20 (emphasis added); RASF ¶ 20. This functionality would mean—according to TLS’s expert—that when a document file was “transmitted to a shared folder,” the “synched folder in the Laptop would *contemporaneously* receive the same electronic communication” and download a “copy to its hard drive.” ASF ¶ 20 (emphasis added); RASF ¶ 20. Because that is the only expert opinion that may be considered on this record, this court need not decide “either the existence or the applicability of a contemporaneity or real-time requirement,” *see Councilman*, 418 F.3d at 80, because even if such a requirement exists—as the Fifth Circuit and others have held—there is sufficient evidence from which a reasonable jury could find that such a requirement has been met. *See, e.g., Konop*, 302 F.3d at 878.

Yet, defendants suggest that there is “no evidence of wiretapping activity” because Rodriguez used Dropbox’s “features exactly the way the application works.” Docket No. 188 at 4. But the broad definition of “intercept” under the statute includes “acquisition [that] occurs ‘when the contents of a wire communication are captured or *redirected in any way.*’” *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (emphasis added) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992)). *United States v. Szymuszkiewicz*, 622 F.3d 701, 703–07 (7th Cir. 2010) (Easterbrook, J.), aptly illustrates this principle. In that case, “the defendant inserted a command into his supervisor’s copy of Microsoft Outlook that directed a copy of all incoming messages to him,” and the Seventh Circuit held that this was sufficient to meet the Wiretap Act’s interception requirement. *See In re Vizio, Inc., Consumer Privacy Litig.*, — F.3d —, 2017 WL 1836366, at \*13 (C.D. Cal. Mar. 2, 2017); *see also Klumb v. Goan*, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012)



(*interception* may be accomplished by “[p]rogramming a computer, either through the use of spyware or legitimate means, to automatically forward” the electronic communication).

Here, Rodriguez added user accounts on the Dropbox for non-TLS employees—thereby programming the Dropbox application to allow these individuals to view, copy, and download shared folders into their devices. Accordingly, as in *Szymuszkiewicz*, where the defendant intercepted an electronic communication by programming Microsoft Outlook to direct a copy of electronic communications to the defendant’s computer, Rodriguez intercepted an electronic communication by programming TLS’s Dropbox to direct copies of those electronic communications to the non-TLS employees’ devices. *See Szymuszkiewicz*, 622 F.3d 701; *see also Noel*, 568 F.3d at 749 (*interception* occurs “when the contents of a wire communication are captured or redirected in any way”). Thus, defendants’ first contention does not entitle them to summary judgment.

Defendants also underscore—and TLS does not dispute—that TLS’s expert cannot directly show, as an evidentiary matter, that the Laptop *contemporaneously* received electronic communications because the Laptop was discarded. Docket No. 188 at 5; Docket No. 209 at 7. Indeed, TLS’s expert opined that if he could have inspected the Laptop, he could have verified whether the Laptop had the Dropbox application installed when documents were transmitted to TLS’s Dropbox, and whether the Laptop was turned on at those times. TLS’s expert further opined that, if both of these conditions were present, then he could have opined that the electronic communications from TLS’s Dropbox were contemporaneously intercepted. To bridge the perceived evidentiary gap,<sup>4</sup> TLS contends that the spoliation-based adverse inference fills the supposed void.

---

<sup>4</sup> The parties agree that the Laptop needed to be turned on to synch with TLS’s Dropbox. *See* ASF ¶ 20; RASF ¶ 20. Yet, because defendants do not suggest that the Dropbox application was ever uninstalled from the Laptop, and because defendants acknowledge that the Laptop was functioning as late as October 2014 and that the Laptop was not discarded until November 2015, a reasonable jury could infer—at the very least—that the Laptop was turned on and synched from TLS’s Dropbox at some point between July 2014 to October 2014. ASF ¶ 11; RASF ¶ 11; Docket No. 133-1 at 3. This reasonable inference—together with the opinions of TLS’s expert—provides an alternative basis for denying defendants’ motion for summary judgment.

Courts have held that, “[i]n borderline cases, an inference of spoliation, in combination with ‘some (not insubstantial) evidence’ for the plaintiff’s cause of action, can allow the plaintiff to survive summary judgment.” *Byrnie v. Town of Cromwell Bd. of Educ.*, 243 F.3d 93, 107 (2d Cir. 2001) (quoting *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998)); *see also Talavera v. Shah*, 638 F.3d 303, 312 (D.C. Cir. 2011) (when evaluating motion for summary judgment, “[t]he spoliation inference must be considered along with [the party]’s other admissible evidence”); *Nation-Wide Check Corp. v. Forest Hills Distributors, Inc.*, 692 F.2d 214, 218–19 (1st Cir. 1982) (Breyer, J.) (“The issue before the court was not whether the destruction was sufficient, standing alone, to warrant an adverse inference about the documents’ contents; it was simply whether the destruction was at all relevant to the tracing issue, and if so, whether it was sufficiently probative *in conjunction with the other evidence* to support the tracing conclusion”) (emphasis added). That is because “holding the prejudiced party to too strict a standard of proof regarding the likely contents of the destroyed evidence would subvert the prophylactic and punitive purposes of the adverse inference, and would allow parties who have intentionally destroyed evidence to profit from that destruction.” *See Kronisch*, 150 F.3d at 128.

In this case, defendants used the Laptop to access TLS’s Dropbox, and that Laptop was intentionally discarded in November 2015—around two months after TLS sent defendants letters asking them to preserve any laptop computers, and around three months after this action commenced. TLS’s expert opined that he would have been able to opine that documents transmitted to TLS’s Dropbox were contemporaneously intercepted if he could have had an opportunity to inspect the Laptop. The foregoing circumstances make this a “borderline” case. *See Byrnie*, 243 F.3d at 107. And because TLS proffered sufficient admissible evidence that the Laptop potentially had critical and damaging electronically stored information, and because the Laptop was intentionally discarded in bad faith, I find that TLS’s admissible evidence—coupled with the spoliation-based adverse inference—could allow a reasonable jury to find that defendants’ Laptop contemporaneously

intercepted electronic communications from TLS's Dropbox. *See Nation-Wide Check Corp.*, 692 F.2d at 218–19. Thus, defendants' motion for summary judgment is denied.

### CONCLUSION

For the foregoing reasons, defendants' motion for summary judgment is **DENIED**. The parties are strongly encouraged to re-assess their positions and re-explore settlement.

**IT IS SO ORDERED.**

In San Juan, Puerto Rico, this 28<sup>th</sup> day of July 2017.

*S/ Bruce J. McGiverin*

BRUCE J. MCGIVERIN

United States Magistrate Judge