

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
FORT MYERS DIVISION

DAVID SCHWARTZ,

Plaintiff,

v.

Case No.: 2:21-cv-283-SPC-KCD

ADP, INC. and AUTOMATIC  
DATA PROCESSING, INC.,

Defendants.

---

**OPINION AND ORDER**<sup>1</sup>

Defendants, ADP, Inc. and Automatic Data Processing, Inc. (together, “ADP”) move the Court for summary judgment on Plaintiff David Schwartz’s remaining claims. ([Doc. 125](#)). The Court is fully briefed. ([Doc. 129](#); [Doc. 131](#); [Doc. 132](#)).

We’ve been here before. ADP first moved for summary judgment six months ago. ([Doc. 91](#)). Schwartz responded that ADP’s motion was premature and that there was substantial discovery to be done. ([Doc. 94](#)). The Court denied the motion without prejudice, concluding there was good cause to grant Schwartz’s request for more time, and it noted that Schwartz had identified a

---

<sup>1</sup> Disclaimer: Papers hyperlinked to CM/ECF may be subject to PACER fees. By using hyperlinks, the Court does not endorse, recommend, approve, or guarantee any third parties or their services or products, nor does it have any agreements with them. The Court is not responsible for a hyperlink’s functionality, and a failed hyperlink does not affect this Order.

host of issues he intended to probe and that he had only recently received responses to written discovery that he needed time to address. (Doc. 107).

Six months have passed, the discovery period has concluded, and ADP's renewed and amended motion is timely. (Doc. 90). Because there is no genuine issue of material fact, the Court grants ADP's renewed and amended motion for summary judgment.

## **BACKGROUND**

ADP hired Schwartz in 2015 and terminated him in 2018. Many times, during his employment, Schwartz reported concerns about several of ADP's business practices he alleges were unlawful. Schwartz alleges ADP retaliated against him before, during, and after his termination because of his whistleblower activities.

The parties' conflict turned litigious when ADP sued Schwartz in state court for breach of contract and misappropriation of trade secrets. Schwartz counterclaimed for wrongful termination. Then ADP filed another state court action for defamation.

Schwartz filed this present lawsuit after ADP allegedly accessed and monitored Schwartz's electronic communications and accounts after the state-court litigation attracted attention and publicity. Schwartz raised a host of claims, many of which the Court has dismissed. (Doc. 57). What remains are

counts under the Stored Communications Act (“SCA”)<sup>2</sup> (Counts 2 and 8), the Wiretap Act<sup>3</sup> (Counts 3 and 9), and Florida’s Security of Communications Act (“FSCA”)<sup>4</sup> (Counts 5 and 11).<sup>5</sup> ADP argues Schwartz lacks evidence for the elements of his claims, and summary judgment is appropriate on all remaining counts.

In support of its motion, ADP first presents the declaration of Greg Crader,<sup>6</sup> an Apple employee who, in his capacity as a “Legal Specialist,” responds to legal process for customer data. (Doc. 125-1). Crader declares that, in response to a subpoena, Apple conducted a reasonable search for documents to determine whether Schwartz’s Apple accounts were subject to unauthorized

---

<sup>2</sup> 18 U.S.C. §§ 2701 *et seq.*

<sup>3</sup> 18 U.S.C. § 2520(a).

<sup>4</sup> Fla. Stat. §§ 934 *et seq.*

<sup>5</sup> The operative pleading is the Third Amended Complaint (“Complaint”) (Doc. 50).

<sup>6</sup> Crader’s declaration was not sworn before a notary, but its execution accords with 28 U.S.C. § 1746, which provides:

Wherever, under any law of the United States or under any rule, regulation, order, or requirement made pursuant to law, any matter is required or permitted to be supported, evidenced, established, or proved by the sworn declaration, verification, certificate, statement, oath, or affidavit, in writing of the person making the same . . . , such matter may, with like force and effect, be supported, evidenced, established, or proved by the unsworn declaration, certificate, verification, or statement, in writing of such person which is subscribed by him, as true under penalty of perjury, and dated, in substantially the following form: . . . “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)”.

Courts may consider a declaration executed in accordance with § 1746 as an affidavit. *United States v. Four Parcels of Real Prop. in Greene & Tuscaloosa Ctys. in State of Ala.*, 941 F.2d 1428, 1444 n.36 (11th Cir. 1991) (citations omitted).

access, and that investigation did not identify evidence of unauthorized access. Crader further declares (1) that Apple never told Schwartz that his Apple accounts were subject to unauthorized access, (2) that no Apple employee concluded Schwartz's Apple accounts were subject to unauthorized access, and (3) that the documents Apple produced do not show that Schwartz's Apple accounts were subject to unauthorized access.

ADP also provides an excerpt from the deposition of Cindy Jimenez, ADP's corporate representative. ([Doc. 125-2](#)). Jimenez states that ADP's mobile device management ("MDM") software, AirWatch, was installed on Schwartz's personal iPhone and his ADP-issued iPad. She explains the software is designed as a conduit to allow approved devices to access ADP resources, but it cannot be used to reveal the content of a user's communications, nor can it be used to access a user's Apple accounts either directly or through Apple servers. Furthermore, Apple security does not allow ADP to access the content of a user's communications. Jimenez explained that she contacted Apple about Schwartz's allegations, and she authenticated the thread of that communication, in which Apple explained that unless both ADP and Schwartz had acted to restore a device to its pre-MDM settings, the device would show network activity for standard activation needs. In other words, unless and until both ADP and Schwartz had taken all necessary steps to remove the MDM technology, some benign connection may still appear.

For his part, Schwartz offers the deposition transcript of Nathaniel Webb,<sup>7</sup> whose ADP employment coincided with Schwartz's. (Doc. 129-3). During his deposition, Webb discussed receiving text messages from Schwartz, and he stated he provided those texts to ADP a week or two before the deposition, but he had not given the texts to anyone else. (Doc. 129-3 at 33–34, 37). Schwartz's counsel then inquired about how Webb could explain that ADP had produced the texts in a deposition more than a year earlier, and Webb said he did not know how they would have obtained it. (Doc. 129-3 at 38).

Eight months after Webb's deposition, he executed an errata sheet in which he changed his testimony that he had never shared Schwartz's text message with anyone at ADP. He changed his testimony to state that he shared the text message with Gaby Lozada (Webb's ADP supervisor) in October 2019. (Doc. 129-3 at 3).

---

<sup>7</sup> Several times during the direct examination, Schwartz's counsel seems to attempt to intimidate Webb. (Doc. 129-3 at 11 (pointedly noting that a former FBI agent with a background in cyber forensics and white-collar crime is an expert consultant on Schwartz's case and present for the deposition); Doc. 129-3 at 15–16 (asking about a Department of Revenue form, the ability to trace the IP address of the device used to complete such a form, the fact that Schwartz had subpoenaed the Department of Revenue to obtain documents related to these forms, and asking Webb if he had been contacted by the Florida Department of Law Enforcement about improperly completed forms); Doc. 129-3 at 34–35 (asking Webb if Schwartz told him he could be in trouble if he forged a client's name on a Department of Revenue form, and asking if Schwartz had told Webb about the FBI consultant); Doc. 129-3 at 49–50 (asking Webb, in essence, if you didn't do anything that would put you in jail, why would you feel intimidated?)). In response to questioning, Webb states that he did, in fact, feel intimidated and threatened—both by Schwartz and his counsel. (Doc. 129-3 at 37–38; Doc. 129-3 at 42–44; 129-3 at 49–50). The Court frowns on these tactics.

Schwartz also offers his own affidavit, in which he details when and how he obtained his personal privacy data from Apple, states when he relinquished control of his ADP-issued iPad, describes Webb’s deposition testimony and the changes thereto as they relate to the timing of the parties’ pending litigation, and outlines his damages from ADP’s alleged statutory violations. ([Doc. 129-4](#)).

And then there is Exhibit R to Schwartz’s Complaint ([Doc. 50-18](#)), which is an unauthenticated composite exhibit of informational pages and reports Schwartz downloaded from Apple Support. It includes an FAQ section, Apple’s published information about its personal information storage, and dozens of pages of sign-on information reports that, Schwartz claims, reveal many times when ADP has accessed Schwartz’s personal devices.

Schwartz’s claims rely heavily on Exhibit R.<sup>8</sup> In fact, Schwartz was asked to state the basis for his claim that ADP had hacked his Apple accounts, and on April 15, 2022, he responded, “At this time, other than Exhibit R to the operative Complaint, At this time, Plaintiff has nothing further at this time.” ([Doc. 125-5 at 3](#); [Doc. 125-9 at 5](#)). But Schwartz has provided no expert

---

<sup>8</sup> Schwartz also relies on Exhibits W, X, Y, and Z to the Complaint. Exhibit W is a document pulled from Apple Support entitled, “Apple ID & Privacy.” ([Doc. 50-23](#)). Exhibit X is 42 pages of computer code, in which “iPhone Distribution: ADP” appears three times. ([Doc. 50-24](#)). Exhibit Y is a document entitled, “ADP Mobile Device Deletion Acknowledgement,” which Schwartz signed on May 7, 2015. ([Doc. 50-25](#)). And Exhibit Z is Webb’s deposition transcript. ([Doc. 50-26](#)).

guidance about what he believes Exhibit R reveals or, indeed, about any of the technical aspects of his claims.

## RELEVANT LAW

### Legal Standard

“The court shall grant summary judgment if 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 fact is “material” if it “might affect the outcome of the suit under the governing law.” [Anderson v. Liberty Lobby, Inc.](#), 477 U.S. 242, 248 (1986). And a material fact is in genuine dispute “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Id.* If “the movant adequately supports its motion,” the nonmoving party must show “specific facts exist that raise a genuine issue for trial.” [Stephens v. Mid-Continent Cas. Co.](#), 749 F.3d 1318, 1321 (11th Cir. 2014) (citation omitted).

Courts view evidence and draw all reasonable inferences in the light most favorable to the nonmoving party. [Rojas v. Florida](#), 285 F.3d 1339, 1341–42 (11th Cir. 2002). All inferences are part conjecture. [Daniels v. Twin Oaks Nursing Home](#), 692 F.2d 1321, 1326 (11th Cir. 1982). But an “inference is not reasonable if it is ‘only a guess or a possibility,’ for such an inference is not based on the evidence but is pure conjecture and speculation.” *Id.* at 1324. And “a mere scintilla of evidence” does not a genuine issue of material fact

make, so a nonmoving party may not simply say, “the jury might, and legally could, disbelieve the moving party’s evidence.” *Hinson v. Bias*, 927 F.3d 1103, 1115–16 (11th Cir. 2019) (internal quotation marks and citation omitted).

### **Statutory Elements**

An SCA claim arises after someone (1) “intentionally accesses without authorization a facility through which an electronic communication service is provided” or “intentionally exceeds an authorization to access that facility”; and (2) “obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” 18 U.S.C. § 2701(a); *see also id.* § 2707(a); *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006).

The Wiretap Act provides an action against someone who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a); *see id.* § 2520(a). As defined, “intercept” is “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). So a Wiretap Act plaintiff must show the “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.” *Hamilton Grp. Funding, Inc. v. Basel*, 311 F. Supp. 3d 1307,



1314 (S.D. Fla. 2018). Interception “encompasses only acquisitions contemporaneous with transmission.” *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003). In other words, “a contemporaneous interception—*i.e.*, an acquisition during ‘flight’—is required to implicate the Wiretap Act with respect to electronic communications.” *Id.* at 1048–49; *see also United States v. Barrington*, 648 F.3d 1178, 1202–03 (11th Cir. 2011). For that reason, “unauthorized access to an email account, standing alone, does not constitute interception.” *Bruce v. McDonald*, No. 3:13cv221–MHT (WO), 2014 WL 931522, at \*5–6 (M.D. Ala. Mar. 10, 2014) (collecting cases).

The FSCA was modeled after the Wiretap Act. *Minotty v. Baudo*, 42 So. 3d 824, 831 (Fla. Dist. Ct. App. 2010). And the causes of action are similar (if not identical). *See Fla. Stat. § 934.10(1)*; *see also id. § 934.02(3)* (defining “intercept”). Given their similarity, “Florida follows federal courts as to the meaning of provisions” in the FSCA. *E.g., Minotty*, 42 So. 3d at 831. One Florida court has suggested in dicta that Florida law follows federal court interpretation on whether interception must be contemporaneous. *O’Brien v. O’Brien*, 899 So. 2d 1133, 1136–37 (Fla. Dist. Ct. App. 2005). And at least one court has held that the FSCA “does not provide a cause of action to those whose electronic communications were acquired from electronic storage rather than intercepted during contemporaneous transmission.” *Handley v. Wilson*, No.

08-14444-CIV-MARTINEZ-LYNCH, 2010 WL 11607357, at \*8–9 (S.D. Fla. Feb. 10, 2010).

## DISCUSSION

ADP broadly argues “Schwartz has no evidence of intent, purpose, or that [ADP] tried or succeeded in unlawfully accessing or intercepting [Schwartz’s] content or communications.” (Doc. 125 at 2). Schwartz disagrees and contends there is at least enough evidence creating issues for the trier of fact. (Doc. 129 at 2).

ADP argues Schwartz lacks evidence of any statutory violation because he cannot (1) identify anyone who acted on ADP’s behalf; (2) establish communications were “accessed,” for the SCA; (3) establish communications were “intercepted,” for the Wiretap Act and FSCA; or (4) show ADP acted, much less with the required unlawful intent.

Schwartz maintains that genuine issues of material fact preclude summary judgment. He dismisses the Apple declaration as “a self-serving statement” that deficiently fails to describe the process used and evidence relied on to determine whether Schwartz’s accounts were unlawfully accessed. Next, Schwartz contends ADP’s corporate representative, Jimenez, could not

answer many important questions<sup>9</sup> and the testimony she gave created issues of material fact. Finally, Schwartz attacks Webb's amendment to his testimony and contends Webb's about-face creates a credibility issue for the trier of fact to consider. The Court is not persuaded by Schwartz's arguments. Resolution of this motion begins with the statutory elements and ends with the burden of proof.

Schwartz has the ultimate burden of proving the elements of his claims. For his SCA claims, Schwartz must prove ADP (1) "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "exceeds an authorization to that facility"; and (2) "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." See [18 U.S.C. § 2701\(a\)](#); see also *id.* § 2707(a); *Snow*, 450 F.3d at 1321. For his Wiretap Act and FSCA claims, Schwartz must prove ADP "(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 *Hamilton Grp. Funding*, 311 F. Supp. 3d at 1314.

---

<sup>9</sup> Schwartz spends four pages of his eighteen-page response detailing the topics he intended to explore and the information he intended to glean during this deposition but could not. ([Doc. 129 at 4–7](#)).

And as movant, ADP has the initial burden on summary judgment of proving that there is no genuine dispute as to any material fact and that it is entitled to judgment as a matter of law. [Fed. R. Civ. P. 56\(a\)](#). Should ADP satisfy this burden, Schwartz must show “specific facts exist that raise a genuine issue for trial.” *See* [Stephens, 749 F.3d at 1321](#). A “mere scintilla of evidence” will not do. *See* [Hinson, 927 F.3d at 1115–16](#).

But a scintilla of evidence is all that Schwartz has. The only evidence Schwartz has of ADP obtaining an electronic communication—setting aside the intricacies of *how* that communication must be obtained to fall within the scope of these statutes—is ADP’s possession of the text messages Schwartz sent to Webb, and the potential that it was obtained before Webb provided it to ADP’s counsel. Seemingly the only evidence Schwartz has to back up his assertion that the text messages were obtained unlawfully is Webb’s now-recanted deposition testimony.

Similarly, the only evidence Schwartz seems to have of ADP accessing his personal accounts is Exhibit R. But Exhibit R is simply screenshots from Apple Support followed by dozens of pages of sign-on information reports. Schwartz has provided no explanation or expert testimony to contextualize this data. So, at best, Exhibit R is an unauthenticated composite exhibit showing that IP addresses allegedly associated with ADP have at some point and in some capacity been linked with Schwartz’s Apple ID.

What Schwartz lacks entirely—and what these statutes require—is evidence of ADP’s intent to access or intercept his communications. So ADP has demonstrated that Schwartz has not established a factual basis for the elements of his claims. But what’s more, ADP has also produced evidence of its own that establish those elements cannot be met: (1) the Apple declaration that shows its investigation did not identify evidence that Schwartz’s accounts were subject to unauthorized access; and (2) the testimony of the ADP corporate representative who stated both that its MDM software cannot reveal the content of a user’s communications, and that Apple security does not allow ADP to access the content of a user’s communications. ADP has established it is entitled to judgment as a matter of law.

And so the burden shifts to Schwartz to produce specific facts that raise a genuine issue for trial. *See [Stephens](#), 749 F.3d at 1321*. He has not carried this burden. Summary judgment for ADP is appropriate.

## CONCLUSION


ADP has carried its burden by demonstrating there is no factual basis for Schwartz’s claims under the SCA, the Wiretap Act, and the FSCA. So the burden shifts to Schwartz to present evidence that creates a genuine issue of material fact for trial. Because Schwartz has not met this burden, his claims fail.

Accordingly, it is now

**ORDERED:**

1. Defendants' Renewed and Amended Motion for Summary Judgment ([Doc. 125](#)) is **GRANTED**.
2. The Clerk is **DIRECTED** to enter judgment for Defendants and to **CLOSE THE CASE**.

**DONE** and **ORDERED** in Fort Myers, Florida on December 29, 2022.

  
**SHERI POLSTER CHAPPELL**  
**UNITED STATES DISTRICT JUDGE**

Copies: All Parties of Record