RECORD NO. 18-1306

IN THE
United States Court of Appeals
FOR THE FOURTH CIRCUIT

PATRICK HATELY, an individual,

Plaintiff - Appellant,

v.

DR. DAVID WATTS, an individual,

Defendant - Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
AT ALEXANDRIA

OPENING BRIEF OF APPELLANT PATRICK HATELY

Eric James Menhart
LEXERO LAW
316 F Street, NW
Suite 101
Washington, DC 20002
(202) 904-2818

Counsel for Appellant

LANTAGNE LEGAL PRINTING 801 East Main Street Suite 100 Richmond, Virginia 23219 (804) 644-0477
A Division of Lantagne Duplicating Services

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 18-1306 Caption: Hately v. Watts

Pursuant to FRAP 26.1 and Local Rule 26.1,

Patrick Hately
(name of party/amicus)

who is Appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/Eric J Menhart Date: 03/26/2018

Counsel for: Patrick Hately

CERTIFICATE OF SERVICE

****

I certify that on 03/26/2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/Eric J Menhart (signature) 03/26/2018 (date)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES & RULES

JURISDICTIONAL STATEMENT

This matter was properly filed in the United States District Court for the Eastern District of Virginia. The district court had jurisdiction over this case, docketed as No. 1:17-cv-00502-AJT-JFA ("*Hately II*"), pursuant to 28 U.S.C. §1331. The district court's federal question jurisdiction was based on alleged violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (the "*CFAA*"), and the Stored Communications Act, 28 U.S.C. §§ 2701 *et seq.*, (the "*SCA*"). Pursuant to 28 U.S.C. § 1357, the district court had supplemental jurisdiction over the state law claims of Plaintiff-Appellant Patrick Wade Hately ("*Hately*") under the Virginia Computer Crimes Act, Va. Code Ann. §§ 18.2-152.1 *et seq.*, (the "*VCCA*").

The Court of Appeals has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291. The final judgment, disposing of all parties' claims and from which Mr. Hately now appeals, was entered in favor of Defendant-Appellee David J. Watts ("*Watts*") on March 14, 2018. Mr. Hately's Notice of Appeal was filed on March 15, 2018. No motions that would alter the time to appeal have been filed.

STATEMENT OF ISSUES

CENTRAL ISSUES

In order to maintain a civil cause of action under the VCCA, an individual must incur an injury to person or property. As a result of Watts's violations of the

VCCA, Mr. Hately, an IT professional in cyber security and cyber forensic analysis, was forced to spend substantial professional time and money to discover the extent of his e-mail account's breached security, determine what information had been accessed, discover and confirm Watts' identity, the method by which the Watts had accessed his private information, identify and contact the domain administrator of his e-mail account, recover deleted e-mail communications, and ultimately, to report the violations to law enforcement. Do these consequential damages in the form of expenditures of professional time and money amount to an injury to person or property under the VCCA?

For an electronic communication to be protectable under the SCA, it must be in "electronic storage" when it is accessed by an unauthorized individual; "electronic storage" includes "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Watts's remote accessing of Mr. Hately's e-mail communications entailed his virtual entry into the computer servers of Mr. Hately's electronic communication service; the e-mail communications that Watts obtained had previously been read by Mr. Hately, who then retained them for his own future reference. Were the e-mails that Watts obtained subject to protection under the SCA?

STATEMENT OF CASE

INTRODUCTION

Mr. Hately appeals from the trial court's ruling that the SCA was not violated when Watts remotely accessed Mr. Hately's private e-mail account without Mr. Hately's permission or authorization. In accessing Mr. Hately's e-mail account, Watts also obtained, accessed, and read multiple private e-mail communications between Mr. Hately and a third-party.

Mr. Hately also appeals the trial court's interlocutory judgment dismissing his state law claims under the VCCA, premised upon Watts' same conduct. In dismissing Mr. Hately's state law claims, the trial court ruled that he lacked the necessary injury to person or property to maintain a civil action.

While initially contemplated in the notice of appeal, Mr. Hately does not appeal the trial court's interlocutory judgment dismissing his claims under the CFAA.

STATEMENT OF THE FACTS

On October 13, 2015, then twenty-nine-year-old Patrick Wade Hately awoke to a notification on his cellular telephone. The notification alerted Mr. Hately that the password to his private e-mail account had been changed. The change had occurred while the former Marine Corps Sergeant was sleeping.

Mr. Hately's e-mail account had been issued to him in August of 2008 by Blue Ridge Community College ("*Blue Ridge*"). Blue Ridge is a member of the Virginia Community College System ("*VCCS*"), an accessible educational institution serving residents of Virginia. Upon matriculating, each VCCS student is issued a unique e-mail address ending in "@email.vccs.edu." It is undisputed between the parties that VCCS email addresses "use GSuite for Education, which includes Gmail. Each student's VCCS email account is a Google Email (Gmail) account with an address that ends in "@email.vccs.edu." *See* JA at 1437. Mr. Hately went on to graduate with an associate degree of arts and sciences in 2013, but he continued to use the VCCS account as his primary e-mail address.

At the time Mr. Hately was issued his VCCS e-mail address, in 2008, he was in a long-term relationship with a romantic partner. With this relationship in mind, the password Mr. Hately chose for his VCCS e-mail account was a combination of his name and hers, along with the date on which they had first met. When this romantic relationship ended in the spring of 2015, Mr. Hately continued use of this same password. Unbeknownst to Mr. Hately – and well after the relationship's demise – the woman with whom Mr. Hately had been previously involved began to monitor his personal affairs. She did so, *inter alia*, by accessing his VCCS e-mail account with the sentimental password that was known to her.

On October 12, 2015, Mr. Hately's former romantic partner reached out to Defendant-Appellant Watts. Watts and the woman were co-workers, sometime-friends, and – for a brief time – the objects of one another's romantic endeavors. The woman informed Watts that she had access to Mr. Hately's e-mail account. Through that access, the woman told him, she had come across e-mail communications that she believed would be of interest to Watts and, potentially, of use in Watts's then-active divorce proceedings.

On the night of October 12th, and into the early hours of the following morning, the woman and Watts engaged in multiple telephone conversations. For these calls, Watts used a prepaid, secondary cellular telephone that he had obtained for "confidential" communications, on the purported advice of an unnamed legal counsel.[1] These so called "burner phones" are routinely utilized to avoid detection and hide activities.

Through these phone conversations in the middle of the night, the woman walked Watts through the process of accessing Mr. Hately's VCCS e-mail account. Once inside the account, Watts found what he had been promised: e-mail

[1] If such advice had been given, the ethically questionable advice was presumably meant as a workaround for Watts's upcoming discovery obligations in his then-active divorce proceedings. His estranged wife's attorneys were unlikely to ask for records of a cellular telephone that they were unaware existed, and if they did, the calls to and from Watts's prepaid telephone did not result in records that he could then produce. Watts never provided the name of the attorney that supposedly provided this advice.

exchanges between Mr. Hately and Watts's estranged wife. During his later deposition, faced with overwhelming factual evidence against him, Defendant Watts ultimately admitted to accessing the account, consistent with the Plaintiff's allegations in the Complaint. *See* Joint Appendix ("JA") at 1047-1048 ("Q. Well, let me restate the question. Did you access, on or about October 13th, 2015, Patrick Hately's Virginia Community College System e-mail account? A. Yes.").

Mr. Hately woke up the following morning to discover that his password had been changed. Hately immediately began to engage in efforts to ensure recovery and security of the account, which contained numerous valuable communications, highly personal data, and other valuable content. After working to regain access to the e-mail account, however, Mr. Hately's subsequent investigation revealed that not one, but three separate, unknown Internet Protocol ("*IP*") addresses had accessed his private e-mail account while he was asleep.

Two of the IP addresses were associated with the types of devices that Mr. Hately knew his former romantic partner owned. In the coming days, after hours of investigation and research, Mr. Hately would learn information that would lead him to suspect that the third IP address belonged to Defendant Watts.

Over the course of the next several days, Mr. Hately expended large amounts of professional time, as well as money, investigating these unauthorized accesses of his VCCS e-mail account, which he had previously believed was

private. Ultimately, Mr. Hately reported the incidents to law enforcement. Subsequent civil litigation followed.

LITIGATION HISTORY

Mr. Hately initially filed a complaint in the United States District Court for the Eastern District of Virginia, naming both his former romantic partner and Watts as defendants, docketed as No. 1:16-cv-1143-GBL-MSN ("*Hately I*"), and alleging the same five causes of action under the CFAA, SCA, and VCCA that were subsequently at issue before the trial court in *this* litigation – *Hately II*. *See* JA at 1-14. Although Mr. Hately had secured evidence that conclusively pointed to the woman's role in the unauthorized accesses of his e-mail account, his initial evidence against Watts was more circumstantial, because most of the factual support necessary to support the claims was in the possession of third parties.

Shortly before responsive pleadings were due to be filed in *Hately I* – and thus also prior to the opening of discovery – Mr. Hately acknowledged that, despite the evidence and his suspicions, he was not yet in possession of unequivocal proof of Watts's connection to the unauthorized accesses of his e-mail account. Mr. Hately therefore filed a notice of his voluntary dismissal of Watts as a defendant, without prejudice, to which Watts then consented. *See* JA at 3.

The remaining defendant in *Hately I*, Mr. Hately's former romantic partner, subsequently filed a motion to dismiss Mr. Hately's first amended complaint. The

motion was granted as to the CFAA and VCCA claims, on the grounds that Mr. Hately had failed to properly allege damages sufficient to maintain the causes of action. *See* JA at 46. The Motion to Dismiss was granted as to several of the claims "**WITHOUT PREJUDICE**." *Id.* (emphasis in original). However, the SCA claim remained.

Mr. Hately continued his prosecution of the SCA claim in *Hately I*, and through subsequent third-party discovery, obtained a transcript of a deposition that had been held in Watts' divorce proceedings. The deponent was the remaining defendant in *Hately I*, and in her deposition, she had confirmed that she provided Watts with the password to Mr. Hately's VCCS e-mail account. She further testified that, to her knowledge, Watts had used Mr. Hately's password to access the account and read Mr. Hately's e-mail communications.

With this testimony in hand, now plainly supporting claims against Watts, Mr. Hately sought to amend his first amended complaint in *Hately I*. Mr. Hately's proposed amendments would return the litigation to its original form, reinstating Watts as a defendant *and* re-pleading the damages allegations, as the *Hately I* court had allowed him to do. *See* JA at 47.

After filing his proposed second amended complaint, but before the issuance of the magistrate's recommendation on his motion to amend, Mr. Hately received additional evidence confirming Watts's active role in accessing Mr. Hately's e-

mail account and corresponding emails. First, from the Office of the Commonwealth's Attorney for the County of Frederick, Commonwealth of Virginia, Mr. Hately received a copy of the report detailing law enforcement's investigation into his claims. *See* JA at 1200. In it, law enforcement details a conversation with Watts in which he fully admits to accessing Mr. Hately's e-mail account. ("The report also includes information about a subpoena that was issued to Watts's Internet Service Provider ("*ISP*"), the response to which confirmed that one of the IP addresses associated with the unauthorized accesses of Mr. Hately's account was assigned to Watts during the relevant time.") *Id.* Second, Mr. Hately received a copy of the actual subpoena that was issued to Watts's ISP and the ISP's actual response thereto, both of which came from the Frederick County, Virginia, Sheriff's Office. *See* JA at 1351-1355.

The *Hately I* defendant opposed Plaintiff's amendments, and the magistrate's report and recommendation on the matter ruled in her favor. In his report and recommendation, the magistrate found several grounds for denying Mr. Hately's motion to amend *Hately I*'s first amended complaint. First, the magistrate opined that "[p]ermitting [Mr. Hately] to add claims at this juncture would be highly prejudicial to [the remaining defendant]." This finding was sufficient to support the magistrate's recommendation that Mr. Hately's motion to amend be denied, but the magistrate continued:

> [Mr. Hately's] proposed Second Amended Complaint would also prejudice former Defendant David Watts, whom [Mr. Hately] voluntarily dismissed from the case before discovery commenced. Amending the complaint to rename Mr. Watts at this late stage in the litigation would prejudice Mr. Watts because he had no opportunity whatsoever to participate in discovery.

See JA at 4. Plaintiff Hately timely appealed the Magistrate's findings to the District Court Judge.

Upon review, the *Hately I* district court *did not* adopt the magistrate's opinion that the amendments would be unduly prejudicial to third-party Watts. Instead, the district court relied *exclusively* on the magistrate's finding that the amendments would be unduly prejudicial to *Hately I*'s remaining defendant, Mr. Hately's former romantic partner. *See* JA at 149. ("The Court adopts the Magistrate Judge's recommendation to deny [Mr. Hately's] Motion to Amend because permitting [Mr. Hately] to amend his complaint would unduly prejudice Defendant."); *id.* at 151 (alteration added) ("In sum, allowing [Mr. Hately] to amend his complaint would unduly prejudice Defendant.").

The district court in *Hately I* was aware of the magistrate's findings of prejudice to both Watts and the remaining *Hately I* defendant in the latter's report and recommendation on Mr. Hately's motion to amend, as well as a *third* basis the magistrate found to support his recommendation that the motion be denied. In its *own* order on the issue, the *Hately I* district court summarized the magistrate's recommended holdings thusly:

> [T]he Magistrate Judge issued a Report and Recommendation, which recommended that the Court deny [Mr. Hately's] Motion to Amend based on the grounds that amending the complaint would prejudice Defendant and Watts, *and that amending the complaint would be futile*.

Id. at 147. (emphasis added). The district court explicitly refused to adopt the magistrate's finding that Mr. Hately's efforts to amend his complaint were futile, writing:

> The second issue is whether the Court should accept the Magistrate Judge's recommendation to deny [Mr. Hately's] Motion to Amend based on the grounds that amending the complaint would be futile because it would still fail to sufficiently allege damages. Because the Court finds that amending the complaint would prejudice Defendant and the Court will analyze damages under the SCA at the summary judgment stage, *the Court need not address whether amending the complaint would be futile.*

Id. at 144-145. (emphasis added). Thus, the magistrate's opinion on the futility of Mr. Hately's state law claims in *Hately I* was *also* inapplicable to *Hately II*; the issue was not actually determined and could not serve as the basis for a later assertion of collateral estoppel.

Within the district court's order adopting the magistrate's overall recommendation to deny Mr. Hately's motion to amend in *Hately I*, the court took a moment to summarize the procedural posture of the case, explaining its *previous* ruling on the remaining *Hately I* defendant's motion to dismiss Mr. Hately's first amended complaint. The district court recalled:

> Although defendant moved to dismiss the Virginia Computer Crime Claims on multiple grounds, the Court dismissed the Virginia Computer Crime Claims because [Mr. Hately] failed to sufficiently allege how he sustained any injury to person or property by reason of a violation of the Virginia Computer Crimes Act ("VCCA").

Id. at 146.

In *Hately I*, Mr. Hately's damages allegations that had been dismissed as insufficient were those of the first amended complaint. *See* JA at 28. The damages allegations found within Mr. Hately's proposed second amended complaint were significantly different than those that had been previously dismissed. *Cf.* JA 28-45 to JA 47-82.

The filing of Mr. Hately's proposed second amended complaint in *Hately I*, which contained the heightened damages allegations, was disallowed *only* on the grounds that it was prejudicial to the remaining defendant. *Id.* at 144-145.

Notably, one of the reasons the district court ruled that Mr. Hately's motion to amend would prejudice the remaining *Hately I* defendant was because "allowing [Mr. Hately] to amend his complaint a second time *would change the nature of this litigation*." *Id.* at 151 (emphasis added). The district court explained: "The amendment [] would add four claims to what would otherwise be a narrow case involving a single cause of action under the SCA, affecting a key issue throughout this litigation – *i.e.*, *Defendant's exposure to damages*." *Id*. (emphasis added).

In finding that Mr. Hately's proposed second amended complaint would shift "the nature" of the *Hately I* litigation because it would expand a one-claim case to five causes of action, the district court *necessarily saw merit* in Mr. Hately's newly-proposed allegations of damages. If Mr. Hately's damages allegations were lacking in merit, "the nature" of the litigation as to the remaining *Hately I* defendant would remain the same.

After filing a complaint in *Hately II*, similar to the proposed but disallowed second amended complaint of *Hately I*, Watts filed a motion to dismiss Mr. Hately's CFAA and VCCA claims. Watts argued:

> The dismissal of [Mr. Hately's] CFAA and VCCA claims in [*Hately I*] constitute valid, final judgments on those issues, namely that: (1) [Mr. Hately] lacks sufficient compensable losses to meet or exceed the $5,000 threshold under the CFAA; and (2) [Mr. Hately] lacks the required injury to his person or property necessary to bring claims under the VCCA.

Id. at 314. Although the district court's findings on the CFAA and VCCA claims in *Hately I* reflected different damages allegations from those at issue in *Hately II*, the district court in *Hately II* accepted Watts's argument and dismissed four of Mr. Hately's five claims. *See* JA at 368. As explained in detail below, this conclusion in *Hately II* was erroneous.

Mr. Hately continued to prosecute his SCA claim, and at summary judgment, this claim was also disposed in Watts' favor. *See* JA at 1571. This appeal follows.

SUMMARY OF ARGUMENT

I. THE VIRGINIA COMPUTER CRIMES ACT

In contemplating Mr. Hately's claims under the VCCA, the district court ruled in Watts' favor on his motion to dismiss, adjudging that Mr. Hately had not sustained the necessary injury to person or property. This ruling ignores binding Fourth-Circuit precedent that deems consequential damages sufficient to state the injury necessary to maintain a civil action under the statute.

Ruling in the alternative, the district court applied the doctrine of collateral estoppel to prevent Mr. Hately from purportedly "relitigating" the same issue of damages under the VCCA that had been litigated in *Hately I*. The doctrine's application was in error, however, because the issue of damages was not the same as in the prior matter; the damage allegations that were deemed insufficient in *Hately I* differed significantly from the damage allegations before the district court in *Hately II*. Because the issue before the court in *Hately II* was not the same issue that had been litigated in *Hately I*, the doctrine of collateral estoppel was improperly applied.

II. THE STORED COMMUNICATIONS ACT

A. CENTRAL ARGUMENTS

In contemplating Mr. Hately's claim under the SCA, the district court ruled in Watts' favor on the parties' cross-motions for summary judgment. In so doing,

the district court read additional, uncontemplated requirements into the text of the statute. The relevant text already constrains the SCA's protections to only those electronic communications that are in "electronic storage." The District Court unnecessarily limited the scope of "electronic storage" under both subsection (A) and subsection (B) of the definition, the latter of which includes "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B).

The District Court also improperly determined that the "purpose of backup protection" must belong to the electronic communication service, *i.e.*, that "backup protection" must be *the electronic communication service's* purpose in its retention of electronic communications, rendering a *user* of the service's purposes in retaining communications immaterial.

This interpretation impermissibly limits this portion of the statute's protections to only those communications retained by an electronic communication service, and only when the service's purpose in retention is "backup protection." While a communication must be retained by the electronic communication service to be protectable, and it must be retained for the purpose of "backup protection," the district court's interpretation leaves communications that are stored by the service for anyone *else's* purpose of "backup protection" vulnerable; unauthorized

individuals would be free to access such communications without fear of penalty or reprisal.

The District Court also conflated the two definitions of "electronic storage," adding the requirement that subsection (B) applied only to copies of communications "made by the ECS while the communication was in transit, and stored by the ECS for its own backup or administrative purposes." *See* JA at 1579. This temporal limitation has no basis in the statute or any persuasive precedent. Further, an ECS's backup purposes are not synonymous with its administrative purposes.

Watts accessed Mr. Hately's e-mail account without authorization. Watts then accessed Mr. Hately's e-mail communications without authorization. Watts obtained one of many copies of Mr. Hately's e-mail communications, which either had not yet been read by Mr. Hately or had been previously-read but retained for "backup purposes." Watts accordingly violated the SCA.

B. ANCILLARY OR ALTERNATIVE ARGUMENTS

The District Court also drew a heretofore unknown distinction between "service copies" of an electronic communication maintained by an ECS and "storage copies," deeming the latter protectable under the statute and the former open to unauthorized accesses. In so doing, the district court made clear that a user of an e-mail account like Mr. Hately's would *never* be able to independently access

a copy of an e-mail that is in backup storage. This conclusion is directly contrary to the rulings of virtually every other court that has examined this issue.

Ruling in the alternative, the district court held that when Watts opened Mr. Hately's e-mail account and commanded the ECS to send him "service copies" of Mr. Hately's e-mails, the ECS transformed into an RCS, rendering the SCA inapplicable. However, when Watts accessed "service copies" of Mr. Hately's e-mails, he *received* electronic communications. When Watts accessed "service copies" of Mr. Hately's e-mails, he gained the ability to *send* electronic communications.[2] The ECS thus remained an ECS, providing Watts with "the ability to send or receive . . . electronic communications." 18 U.S.C. § 2510(15).

Even if Mr. Hately's ECS mutated into an RCS when delivering e-mails to Mr. Hately's account, it does not follow that such e-mails would cease to be protectable under the SCA, as the unauthorized individual would nonetheless be accessing a facility – the ECS/RCS's computer servers – through which an electronic communication service is provided. Simply because an e-mail is being delivered by an RCS does *not* mean that it was not stored by the ECS for purposes of backup protection.

[2] Opening an e-mail message in an e-mail inbox – whether read or unread – provides an individual with the ability to, *inter alia*, read, reply to, or forward its contents. This falls within the very definition of an "electronic communication service," which is a service that "providers to *users* thereof the ability to send or receive . . . electronic communications." 18 U.S.C. § 2510(15) (emphasis added).

ARGUMENT

I. INTRODUCTION

This appeal arises from two discrete rulings from the district court. The first is the granting of Watts's motion to dismiss four of Mr. Hately's five claims, although only three of those four, the Virginia statutes,[3] are now being appealed. *See* JA at 394. The second is the granting of summary judgment as to Mr. Hately's fifth claim in Watts's favor. *See* JA at 1571. There are few, if any, disputes as to the material facts. Only questions of law remain to be decided.

II. STANDARD OF REVIEW

"Because this appeal involves the district court's grant of a motion to dismiss, the standard of review is de novo." *Ndeh v. Midtown Alexandria, L.L.C.*, 300 Fed. Appx. 203, 206 (4th Cir. 2008) (citing *Sucampo Pharms., Inc. v. Astellas Pharma, Inc.*, 471 F.3d 544, 550 (4th Cir. 2006)). "'Like the district court, [this Court] must assume all [well-pled facts] to be true.'" *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 253 (4th Cir. 2009) (second alteration in original) (first alteration added) (quoting *Trulock v. Freeh*, 275 F.3d 391, 399 (4th Cir. 2001) (quotations and emphasis omitted)). "[A]lso[] like the district court, [this Court] draw[s] all reasonable inferences in favor of the plaintiff." *Id.*

[3] Plaintiff does not appeal the District Court's dismissal of the Computer Fraud and Abuse Act (CFAA) claim.

(alterations added) (citing *Edwards v. City of Goldsboro*, 178 F.3d 231, 244 (4th Cir. 1999)).

Similarly, this Court "review[s] grants of summary judgment de novo." *Podberesky v. Kirwan*, 38 F.3d 147, 155 (4th Cir. 1994) (alteration added) (citing *Higgins v. E.I. DuPont de Nemours & Co.*, 863 F.2d 1162, 1167 (4th Cir. 1988)). In reviewing a district court's award of summary judgment, this Court "view[s] the facts, and all reasonable inferences that may be drawn from those facts, in the light most favorable to the [nonmoving party]." *Scoggins v. Lee's Crossing Homeowner's Ass'n*, 718 F.3d 262, 269 (4th Cir. 2013) (citing *Bonds v. Leavitt*, 629 F.3d 369, 380 (4th Cir. 2011); *S.C. Green Party v. S.C. State Election Comm'n*, 612 F.3d 752, 755 (4th Cir. 2010)).

In addition, "[t]he instant appeal presents [two] question[s] of statutory interpretation, which [are] question[s] of law that [are] review[ed] de novo." *Stone v. Instrumentation Lab. Co.*, 591 F.3d 239, 241-43 (4th Cir. 2009) (alterations added) (citing *United States v. Turner*, 389 F.3d 111, 119 (4th Cir. 2004)).

III. DISCUSSION OF ISSUES

A. MR. HATELY'S CLAIMS UNDER THE VIRGINIA COMPUTER CRIMES ACT

1. *Below, the district court explicitly acknowledged Mr. Hately's consequential damages in the form of expenditures of professional time and money. The Fourth Circuit has deemed such consequential damages sufficient to maintain an action under the VCCA's "any damages" language.*

In ruling on Watts's motion to dismiss in *Hately II*, the district court acknowledged three categories of damages that Mr. Hately had incurred. At oral argument, the court described the final category as follows:

> The third category of approximately $3,700 is for reviewing records, restoring e-mails, and researching and implementing security enhancements, which also includes [Mr. Hately's] time spent reviewing telephones, online accounts, e-mail records, restoring deleted messages, changing passwords, contacting various vendors about allegedly unauthorized access, and researching and implementing security enhancements.

See JA at 376. (alteration added).

These damages have also been acknowledged by Watts, rendering them undisputed. *See* JA at 325. (alteration and omissions added) ("In the Complaint, the losses alleged by [Mr. Hately] include: . . . (3) Reading a year's worth of telephone records to create a whiteboard; (4) Identifying the domain administrator at his community college to determine who managed his school account; (5) Speaking to, and emailing with, the domain administrator; (6) Reviewing his full email history; (7) Restoring email messages; . . . (13) Researching multiple-factor authentication;

(14) Adding a second form of authentication; and (15) Enhancing the security on his mobile phone.").

Analyzing Mr. Hately's damages, the district court in *Hately II* explicitly acknowledged the potential validity of these consequential damages, stating: "The third category of loss, the personal investigation of the violation, falls into a category of damages *that could plausibly be recoverable* . . ." *See* JA at 381. (emphasis added). Nonetheless, the district court went on to dismiss Mr. Hately's claims under the VCCA, reasoning:

> [T]he Court has considered whether the plaintiff has adequately alleged damages without regard to the prior proceedings [and concludes] that he has not alleged facts that make plausible his claim that he has sustained injury to person or property as those terms have been construed under the Virginia Computer Crimes Act.

See JA at 383. (alterations added).

Responding to and investigating Watt's unauthorized access of his e-mail account required the devotion of Mr. Hately's professional time and resources. When a monetary value is assigned to Mr. Hately's time and resources, consequential damages are apparent. Moreover, the Fourth Circuit has *already expressly ruled* that consequential damages *are* among the damages contemplated by the VCCA. *See A.V. v. iParadigms, LLC* 562 F.3d 630, 646-47 (4th Cir. 2009).

In *iParadigms*, the defendant-corporation asserted counterclaims against the plaintiff alleging, *inter alia*, violations of the VCCA. iParadigms pointed to the fact

that it had "assigned several employees to determine what happened [after the plaintiff's violations]," and "numerous man-hours were spent responding to [the plaintiff's violations]." *Id.* at 645 (alterations added).

Summarizing the findings of the trial court, the Fourth Circuit wrote: "The district court concluded that iParadigms's counterclaim failed as a matter of law," finding "that iParadigms 'failed to produce any evidence of actual or economic damages,' and 'only presented evidence of consequential damages resulting from the steps taken by iParadigms in response to [the plaintiff's violations].'" *Id.* at 645-46 (alteration added) (internal citations omitted). Based upon these findings, the district court dismissed iParadigms's counterclaim.

On appeal, the Fourth Circuit reversed, "conclud[ing] that the evidence of consequential damages presented by iParadigms came within the 'any damages' language of the VCCA . . ." *Id.* at 647 (alteration added).

Just as iParadigms performed its own investigation of the computer-related violations, so too did Mr. Hately. Like iParadigms's employees, following Watts's unauthorized access of his e-mail account, Mr. Hately spent numerous man-hours attempting to determine what had happened, who had caused it, and how to prevent it from happening again. Like the counterclaim in *iParadigms*, this Court should reverse the district court's ruling dismissing Mr. Hately's causes of action under

the VCCA, as his allegations of consequential damages clearly align with those previously accepted by the Fourth Circuit in *iParadigms*.

2. *Below, the district court improperly applied the doctrine of collateral estoppel, ruling that Mr. Hately's litigation of the issue of damages in Hately I precluded him from "relitigating" it in Hately II. This application was based upon a misunderstanding of which issues had actually been litigate, and decided, in Hately I.*

The district court in *Hately II* erroneously explained the procedural posture of *Hately I* thusly:

> Here, [the district court in *Hately I*] did *finally decide* the specific issue [of] whether [Mr. Hately] met the loss or damages allegation requirements. In adopting the magistrate judge's report and recommendations, the court stated that the court dismissed the CFAA claim because [Mr. Hately] failed to sufficiently allege that he incurred over $5,000 in losses or damages cognizable under the CFAA.

See JA at 378 (alterations added, emphasis added).

The *Hately II* district court's summary of *Hately I*, above, was erroneous. First, *Hately I* did *not* "finally decide" the "loss or damages allegations requirements." As explained in detail, *supra*, the Motion to Dismiss in *Hately I* was granted "**WITHOUT PREJUDICE**." *See* JA at 46. (emphasis in original).

The United States Supreme Court has explained that dismissals without prejudice do not constitute a "final determination" to which collateral estoppel can be applied. *See e.g. Cooter & Gell v. Hartmarx Corp.*, 496 U.S. 384, 396, 110 S. Ct. 2447, 110 L. Ed. 2d 359 (1990) ("[D]ismissal . . . without prejudice is a

dismissal that does not operat[e] as an adjudication upon the merits under Rule 41(a)(1), and thus does not have a res judicata effect."); *see also Lynk v. LaPorte Superior Court No. 2*, 789 F.2d 554, 566 (7th Cir. 1984) ("by definition," neither res judicata nor collateral estoppel arise from a dismissal without prejudice). This, alone, precluded the district court from attempting to collaterally estop Hately's subsequent claims.

There were other problems with the *Hately II* court's analysis. The district court explained the requisite elements for the application of collateral estoppel thusly:

> The principles that apply with respect to collateral estoppel require that the proponent of that doctrine demonstrate that [(1)] the issue of fact is identical to the one previously litigated, [(2)] [the issue of fact] was actually resolved in a prior proceeding, [(3)] the issue was critical or necessary to the judgment in a prior proceeding, [(4)] the judgment in the prior proceeding is final and valid, and [(5)] the party to be foreclosed by the prior resolution had a fair and full opportunity to litigate the issue in prior proceedings.

See JA at 376. (alterations added). Applying this doctrine to the facts of *Hately II*, the district court then stated: "Here, [Mr. Hately] does not appear to dispute the first three requirements or the fifth requirement can't be satisfied, nor could he reasonably." *See* JA at 376-377 (alteration added). However, this assessment of Mr. Hately's argument is plainly inaccurate.

As to the first element of collateral estoppel – that the issue of fact must be identical to one previously litigated – the issue of damages contemplated by the

court in *Hately II* was *not* identical to the issue previously litigated in *Hately I*. Rather, Mr. Hately repeatedly noted that the damages alleged in *Hately I* – which the district court had considered insufficient when contemplated pursuant to a motion to dismiss – had been thoroughly transformed prior to Mr. Hately's filing of the complaint in *Hately II*. *See* JA at 333 (alterations and emphasis added) (". . . [Mr. Hately] moved the Court to Amend the First Amended Complaint and accept the Second Amended Complaint as the operative pleading . . . [Mr. Hately] sought to re-introduce his claims under the CFAA and VCAA *by offering additional evidence of damages* . . .").

As to the second element, that "[the issue of fact] was actually resolved in a prior proceeding," there can be no such showing. The damages alleged in *Hately I*, were absolutely not the same as the damages alleged in *Hately II,* which were substantially more voluminous and detailed. *Cf.* JA 28-45 (*Hately I*); to JA 153-180, ¶¶ 73-123 (*Hately II*).

As to the third element, the damages issue as to the Virginia statutes was not "critical or necessary to the judgment in a prior proceeding." This is because only one statute could proceed in *Hately I*, namely, the Stored Communications Act. The law applicable to damages calculations are notably different between the Virginia statues and the Stored Communications Act, as the Fourth Circuit previously explained in *iParadigms*, *supra.*

Fourth, as to the judgment in the prior proceeding being "final and valid," there was only a judgment as to the Stored Communications Act. There was no judgment, of any kind, related to the Virginia state statutes, because they had been dismissed, without prejudice, early in the prior proceeding.

Finally, as to whether "the party to be foreclosed by the prior resolution had a fair and full opportunity to litigate the issue in prior proceedings," Hately had initially alleged violations of the Virginia state statutes, but those claims were dismissed "**WITHOUT PREJUDICE**" (emphasis in original) by the *Hately I* court.

While it is true that the *Hately I* court eventually denied Hately's attempt to amend his complaint in that matter, the denial was based entirely on *purported prejudice to the prior Defendant*, and *not* futility of the proposed amendments:

> The second issue is whether the Court should accept the Magistrate Judge's recommendation to deny [Mr. Hately's] Motion to Amend based on the grounds that amending the complaint would be futile because it would still fail to sufficiently allege damages. Because the Court finds that amending the complaint would prejudice Defendant and the Court will analyze damages under the SCA at the summary judgment stage, *the Court need not address whether amending the complaint would be futile.*

Id. at 144-145 (emphasis added). As demonstrated, the District Court in *Hately I* expressly declined to find that the proposed amendments were futile, and recognized that the addition of the new allegations had the potential to change the litigation in a way that might prejudice the defendant in *Hately I*. Despite this, the

Hately II court collaterally estopped Hately from pursuing his state law claims despite Hately *never having been given the opportunity* to make such allegations in Hately I.

The record is clear that the damages allegations before the district court in *Hately I* were entirely different from those at issue in *Hately II*. *Cf.* JA 28-45 (*Hately I*); to JA 153-180, ¶¶ 73-123 (*Hately II*). Moreover, the dismissal of the state law causes of actions were clearly "**WITHOUT PREJUDICE**" (emphasis in original) in *Hately I*. There is no holding from the *Hately I* order on the motion to dismiss that was ever applicable in *Hately II*, and dismissal of the state law causes of action based on principles of collateral estoppel was improper.

B. MR. HATELY'S CLAIM UNDER THE STORED COMMUNICATIONS ACT

The Stored Communications Act is one piece of the Electronic Communications Privacy Act (the "*ECPA*") and is often referred to as Title II of the latter legislation. It is undisputed that "the legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) (citing S. Rep. No. 99-541, at 35-36 (1986)), *cert. denied*, 537 U.S. 1193, 123 S. Ct. 1292, 154 L. Ed. 2d 1028 (2003).

Mr. Hately alleges that Watts violated the SCA, 18 U.S.C. § 2701, *et seq.*, when he accessed Mr. Hately's e-mail account without permission and read through multiple e-mail exchanges to which Watts was not a party. Section 2701 provides:

> (a) Offense – Except as provide in subsection (c) of this section whoever –
>
> (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 a system shall be punished as provided in subsection (b) of this section.

See 18 U.S.C. § 2701. The SCA also provides a method by which an aggrieved individual[4] might obtain civil relief. 18 U.S.C. § 2707.

"Like the [common law] tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2003). "The Act reflects Congress's judgment that

[4] Below, the district court observed that Watts had accessed Mr. Hately's e-mail account without authorization and accepted as true Mr. Hately's allegations (and Watts's admissions) that Watts had read e-mail messages that he found in the account. The court concluded that "the dispositive issue reduce[d] to whether the emails at issue here were in 'electronic storage' as required by § 2701(a)." *See* JA at 1574. The district court did not interrogate the intentionality of Watts's conduct, with the implication being that no reasonable finder of fact could adjudge Watts's accessing of Mr. Hately's e-mail account as anything but intentional.

users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Id.*

"Courts have settled that determining whether there was unauthorized access under the SCA is akin to determining whether there was a trespass to property." *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) (citing *Theofel*, 359 F.3d at 1072-73). "[W]here the facts indisputably present a case of an individual logging onto another's e-mail account without permission and reviewing the material therein, a summary judgment finding of an SCA violation is appropriate." *Id.* (citing *Wyatt Tech. Corp. v. Smithson*, No. 05-1309, 2006 WL 5668246, **9-10 (C.D. Cal. 2006)).

Judicial application of the SCA is not without its difficulties. Indeed, its complications have been well-documented by frustrated courts and observers alike. *See, e.g.*, *Levin v. ImpactOffice LLC*, No. TDC-16-2790, 2017 U.S. Dist. LEXIS 106480, 2017 WL 2937938 (D. Md. July 10, 2017) ("applying the definitions of 'electronic storage' is a difficult endeavor because the technology relating to emails and other electronic communications has changed since the enactment of the SCA and the issuance of many of the judicial opinions interpreting the law").

The instant matter is primarily concerned with the issue of "electronic storage" under the Stored Communications Act. The SCA defines "'electronic storage' as '(A) any temporary, intermediate storage of a wire or electronic

communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17), *incorporated by* 18 U.S.C. § 2711(1). The instant case presents this issue of first impression for the Fourth Circuit.

1. Other Circuits Have Recognized the Stored Communications Act's Applicability and Enforceability in Similar Factual Circumstances

While the Fourth Circuit is directly considering this issue for the first time, several other Courts of Appeals[5] have reviewed the issues raised in this instant matter. In virtually all cases, the legal positions maintained by Plaintiff in the instant appeal were adopted by the reviewing Courts of Appeals. Only one Circuit, the Eighth Circuit, has taken a position that supports Defendant. However, even the Eighth Circuit stopped well short of outright rejection of the law as proscribed by the other Courts of Appeals.

The First Circuit addressed these issues in *United States v. Councilman*. In that matter, the First Circuit found:

> The term "electronic communication" includes transient electronic storage that is intrinsic to the communication process for such communications. That conclusion is consistent with our precedent. *See Blumofe v. Pharmatrak, Inc.* (*In re Pharmatrak Privacy Litig.*), 329 F.3d 9, 21 (1st Cir. 2003) (a rigid

[5] The Sixth, Seventh or Tenth Circuits do not, in Appellant's view, have directly applicable cases, or the cases are effectively duplicative of precedent in other Circuits discussed in more detail herein.

> "storage-transit dichotomy . . . may be less than apt to address current problems").

United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005).

The Second Circuit has also not directly addressed the issue, but there is some language that is, again, consistent with Plaintiff's legal position. *See Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503 n.1 (2d Cir. 2005) (citations omitted) (rejecting arguments that "communication over the Internet can only be electronic communication while it is in transit, not while it is in electronic storage").

The Third Circuit addressed this issue by first taking note of the United States Supreme Court's reminder that "[a] fair reading of legislation demands a fair understanding of the legislative plan." *In re Google Inc.*, 806 F.3d 125, 147 (3d Cir. 2015) (*citing King v. Burwell*, 135 S. Ct. 2480, 2496, 192 L. Ed. 2d 483 (2015). Next, the Third Circuit proclaimed that "we agree with the Fifth Circuit that the Act clearly shows a specific congressional intent to deal with the particular problem of private communications in network service providers' possession." *Id.* Finally, the Third Circuit found that:

> The origin of the Stored Communications Act confirms that Congress crafted the statute to specifically protect information held by centralized communication providers. Sen. Rep. No. 99-541 (1986)'s entire discussion of [the Stored Communications Act] deals only with facilities operated by electronic communications services such as "electronic bulletin boards" and "computer mail facilit[ies]," and the risk that communications temporarily stored in these facilities could be accessed by hackers.

Id. In addition, prior Third Circuit precedent is consistent with *In Re Google*. One case declared that "it seems questionable that the transmissions were not in backup storage -- a term that neither the statute nor the legislative history defines." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003).

Here in the Fourth Circuit, the issue at bar has not yet been directly decided, and the instant appeal asks that guidance be granted. However, the Fourth Circuit previously upheld a district court's award of punitive damages when the SCA violation involved a defendant accessing an employee's personal email account with America On-Line ("AOL"). *See Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199, 202, 209 (4th Cir. 2009). Moreover, most District Courts within this Circuit have determined that the SCA is enforceable in similar circumstances. *See e.g. Hoofnagle v. Smyth-Wythe Airport Comm'n*, 2016 U.S. Dist. LEXIS 67723, 2016 WL 3014702, at *10 (W.D. Va. May 24, 2016) (denying defendants' motion for summary judgment where Plaintiff had already opened emails stored on service provider's server because emails were in "electronic storage" for purposes of the SCA); *Hately v. Torrenzano*, 2017 U.S. Dist. LEXIS 80011, at *20 (E.D. Va. May 23, 2017) ("if Plaintiff can prove that emails remained on the servers for purposes of backup protection even after he opened the emails, then Plaintiff can establish the 'electronic storage' element of an SCA claim"); *Skapinetz v. CoesterVMS.com, Inc.*, 2018 U.S. Dist. LEXIS 21648, at *8 (D. Md. Feb. 9, 2018) ("Plaintiff

sufficiently pled that the emails were in the 'electronic storage' of their internet service provider, Google, at the time of Defendants' unauthorized access."); *Levin v. ImpactOffice LLC*, Civil Action No. TDC-16-2790, 2017 U.S. Dist. LEXIS 106480, at *10 (D. Md. July 10, 2017) ("the emails were in 'electronic storage' under the second definition, in that they were in 'storage . . . for purposes of backup protection of such communication[.]'"). As demonstrated, the weight of authority in this very Circuit, prior to the Fourth Circuit's formal direction on this issue, is consistent with that found in most other courts across the country.

The Fifth Circuit also supports Plaintiff's legal position. As early as 1994, the Fifth Circuit recognized the applicability of the SCA to situations like the case at bar:

> Central to the issue before us, the BBS also offered customers the ability to send and receive private E-mail. Private E-mail was stored on the BBS computer's hard disk drive temporarily, until the addressees 'called' the BBS (using their computers and modems) and read their mail. After reading their E-mail, the recipients could choose to either store it on the BBS computer's hard drive or delete it . . . The E-mail in issue was in "electronic storage."

See Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994). More recently, the Fifth Circuit affirmed its prior findings, noting that "Courts have interpreted the statute to apply to providers of a communication service such as telephone companies, Internet or e-mail service providers, and bulletin board services." *Garcia v. City of Laredo*, 702 F.3d 788, 792 (5th Cir. 2012).

The Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004), a leading case in the space, is oft-cited in this instant Appellate brief, and in the record below. *See e.g.* JA 1450-1451. As discussed throughout this brief, the Ninth Circuit's holdings are completely consistent with Plaintiff's legal positions in this case.

In the Eleventh Circuit, again, precedent supports the Plaintiff. The Eleventh Circuit has found that "the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS)." *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003). Of note, the United States Supreme Court denied cert in that matter, choosing not to disturb the Eleventh Circuit's findings. 538 U.S. 1051, 155 L. Ed. 2d 1095, 123 S. Ct. 2120 (2003).

Only in the Eighth Circuit has a position contrary to the other Circuits been maintained. In *Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 839 (8th Cir. 2015), a case primarily concerned with free speech issues regarding public employees, the Eighth Circuit found that one draft email, and one "sent" email were not protected under the Stored Communications Act. *Id.* (neither "draft of the Dr. Tan email nor the sent Holland email" were protected).

Even after this result, the Eighth Circuit demurred when given the chance to outright reject *Theofel* and its ilk. Notably, the Court found that "we need not

decide whether *Theofel* or one of its critics is correct." *Id.* at 842. Moreover, the Eighth Circuit expressly left open the possibility that *Theofel* could be applicable to the *recipient* of the email. ("If *Theofel* has any application here, it would be to protect a copy of the email stored with [the recipient's] email service, not [the sender's]"). In short, the most negative Court of Appeals treatment of this issue, anywhere, still stopped well short of outright rejecting the other Circuits' findings, and expressly noted that there could be SCA protection of a recipient's email messages, just as the other Court of Appeals have found.

As demonstrated, the clear weight of authority adopts Plaintiff's legal position. A similar result should occur in this matter.

2. *Below, the district court accepted as true Watts's assertion that his reading of Mr. Hately's e-mails was limited to those e-mails that had previously been delivered to and read by Mr. Hately, and the court ruled that this precluded application of subsection (A) of the definition of "electronic storage." However, Watts offered no evidence as proof of his statement, the Act does not distinguish between delivered/read communications and undelivered/unread communications, and neither the Supreme Court nor the Court of Appeals for the Fourth Circuit have provided guidance on the correct interpretation of "temporary, intermediate storage."*

Subsection (A) of the SCA's definition of "electronic storage" is limited to "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). Basing its decision "on the text and structure of the SCA," the district court below concluded "that § 2510(17)(A)'s definition of 'electronic storage' only

encompasses those emails that are unread or not downloaded; in other words, it covers emails only up to the point where the emails have been initially transmitted to their recipient and read or initially downloaded." *See* JA at 1575 (citing multiple authorities).

The district court accepted as true Watts's unprovable assertion that he "did not open or view any email from the Email Account that was unopened, marked as unread, previously deleted, or in the Email Account's 'trash' folder, and that Watts did not change the status of, or modify, any email from the Email Account in any way." *See* JA at 1576. Thus, the court concluded, Mr. Hately "ha[d] failed to establish as a matter of law that Watts accessed emails in 'electronic storage' under § 2510(17)(A)." *Id.*

That Watts opened Mr. Hately's unread e-mails or altered the status of an e-mail in Mr. Hately's inbox cannot be definitively proven, but neither can Watts's insistent assertions to the contrary. In reviewing Watts's motion for summary judgment, the district court was obligated to "view the facts in the light most favorable to the party opposing the motion." *See* JA at 1573 (citing *Porter v. U.S. Alumoweld Co.*, 125 F.3d 243, 245 (4th Cir. 1997)). Thus, it was improper for the court to accept Watts's unprovable assertion that he only read previously-opened e-mails as true, and the entrance of summary judgment in Watts's favor was incorrect.

Despite the district court's improper weighting of the disputed facts, the SCA claim should have nonetheless been adjudicated in Mr. Hately's favor. "Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient." *Theofel*, 359 F.3d at 1075 (citing multiple authorities). "This definition is generally understood to cover email messages that are stored on a server before they have been delivered to, or retrieved by, the recipient." *Levin*, 2017 U.S. Dist. LEXIS 106480, WL 2937938, at *7 (quoting multiple authorities). However, in recent years, several district courts in this Circuit have eschewed the read/unread distinction as determinative of whether an SCA violation has occurred. *See Hoofnagle,* 2016 U.S. Dist. LEXIS 67723; *Skapinetz*, 2018 U.S. Dist. LEXIS 21648, *supra.*

Some district courts in sister circuits have similarly elected not to differentiate between "read" and "unread" electronic communications, finding it unnecessary to investigate the "status" of communications that were unlawfully obtained. Sometimes, this decision hinges on a reading of the SCA that penalizes, without more, the obtaining of unauthorized *access* to electronic communications, rather than the obtaining of the communications themselves. *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 587 F. Supp. 2d 548, 555-56 (S.D.N.Y. 2008) (in adjudicating defendant's counterclaim, court found that plaintiff violated SCA simply by accessing three of defendant's e-mail accounts,

and plaintiff's obtaining of defendant's incoming *and outgoing* e-mail communications amounted to another, separate SCA violation, leaving the status of the obtained e-mails unaddressed), *adopted by* 587 F. Supp. 2d 548 (2008); *Wyatt Technology Corp. v. Smithson*, 2006 WL 5668246, *9 (granting summary judgment in favor of counter-claimant alleging that the plaintiff violated the SCA by accessing the defendant's personal e-mail on a private foreign server, and monitoring the personal e-mail account, without authorization).

Other times, courts find the SCA's applicability to be so obvious in a situation – such as those occasions on which it is alleged that the defendant has read the plaintiff's e-mail communications – that there is no need to consider the "status" of the e-mail that was unlawfully obtained. *See Lane v. Le Brocq*, No. 15 C 6177, 2016 U.S. Dist. LEXIS 40667, *18 (N.D. Ill. Mar. 28, 2016) (internal citations omitted) ("Plaintiffs [] allege that Defendant accessed electronic files stored on cloud-based servers that were connected to the interne[t]. They further allege that some of the data he accessed consisted of emails. These allegations are sufficient to trigger the SCA."); *id.* at *21-22 (plaintiffs' allegations that defendant "exceeded his authority by intentionally accessing materials that he had been expressly forbidden from accessing adequately states a claim under the SCA"); *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 337 (E.D. Pa. July 3, 2013) (citing multiple authorities) (noting that "[t]he parties agree that email messages

remaining on an internet service provider's server after delivery fall within the Act's definition of electronic storage" without interrogating the status of the email messages in question); *Markert*, *supra*, 2010 U.S. Dist. LEXIS 44828, at *18-19 (emphasis added) (where defendants argued "that it is not a violation of the Act to retrieve [] e-mails from storage after transmission is complete," the court found that the SCA "applies when information is retrieved from electronic storage *even after* transmission is complete," and did not concern itself with whether plaintiff's e-mails were read or unread); *Fischer*, *supra*, 207 F. Supp. 2d at 925-26 (addressing defendants' argument that plaintiff's Hotmail e-mails were not in "electronic storage" because the SCA does not apply to e-mails already transmitted to a user's e-mail account, the district court concluded that "the legislative history shows that Congress intended the Stored Communications Act to cover the exact situation in this case," leaving unanswered the question of whether plaintiff's e-mails had been previously delivered and read); *MidAmerica Prods., Inc. v. Derke*, No. 601381/08, 2013 N.Y. Misc. LEXIS 1211, *9-10 (N.Y. Sup. Ct. Mar. 28, 2013) (denying summary judgment on SCA claim because "[t]he parties have raised issues of fact as to who, whether [one defendant or the other], or both, accessed [the] emails, and whether [the defendants] had authorization to access [the] email account," where "the evidence presented indicate[d] that the emails accessed were accessed . . . after delivery").

The Court of Appeals for the Ninth Circuit has also had occasion to take this approach. *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900-03 (9th Cir. 2008) (finding that incoming and outgoing text messages, necessarily previously read, were within the purview of the SCA without delving into the question of each message's "status"), *rev'd in part on other grounds*, *City of Ontario v. Quon*, 560 U.S. 746 (2010). *See also Konop*, *supra*, 302 F.3d at 879 (parties agreed that postings on password-protected website, open to only a particular group of people, were "electronic communications" in "electronic storage").

Similarly, on an appeal regarding the propriety of awarding certain damages, the Court of Appeals for the Fourth Circuit did not question the jury's verdict finding the defendant liable for a violation of the SCA. *Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009). On the facts laid out by the appellate court, it was clear that the defendant had accessed the plaintiff's e-mail account and made copies of several e-mails *from* the plaintiff. *Id.* at 202. However, there were no details that indicated that the defendant had accessed e-mails *to* the plaintiff, and thus no distinction regarding the "status" of the e-mails (*i.e.*, read, unread, drafted, deleted) was ever drawn. *Id.*

There is ample authority upon which this Court might rely in ruling that the "statuses" of Mr. Hately's e-mails are not dispositive, or even necessarily relevant,

in determining whether Watts violated the SCA when he logged into Mr. Hately's account and opened and read Mr. Hately e-mails without authorization. Courts have previously held that a violation of the Act occurs simply by gaining unauthorized *access* to another's electronic communications, as Watts undisputedly did when he logged in to Mr. Hately's e-mail account. Other courts have read the Act's limitations to require accessing the electronic communications themselves but have not required that the communication be "unread" in order to be protectable under subsection (A). *See supra.*

As demonstrated, it is unnecessary to follow the district court's line of reasoning to find flaws in its application of the provisions of the SCA. It is enough that Watts accessed Mr. Hately's e-mail account, and that Watts read Mr. Hately's e-mails, to adjudge Watts liable for his conduct under the SCA.

3. *Below, the district court concluded that Watts accessed "service copies" of Mr. Hately's e-mails, rather than the "storage copies" maintained by VCCS for its "purposes of backup protection," and that the purposes for which Mr. Hately retained his e-mails was immaterial, ultimately ruling that this precluded application of subsection (B) of the definition of "electronic storage." However, neither the Act nor any other court have ever used such terms or drawn such a distinction, the SCA does not restrict the "purpose of backup protection" to VCCS only, and the fact of multiple copies of Mr. Hately's e-mails existing has been repeatedly deemed sufficient in finding unlawfully accessed e-mails to be in electronic storage "for purposes of backup protection."*

In adjudicating Mr. Hately's SCA claim in favor of Watts, the district court concluded that subsection (B) of the definition of "electronic storage" was also inapplicable, relying on the following facts:

> The only material evidence in the record on this issue is that (1) students can access directly through their email accounts copies of emails until the student decides to delete a particular email; (2) the VCCS email system stores copies of student emails for the purposes of backup protection; (3) student users, such as Hately, and therefore Watts using Hately's password, cannot access these copies stored for backup protection through their student accounts simply by logging into a student's email account; (4) these stored VCCS system backup copies are available to users only by special request and are therefore not immediately accessible to students.

See JA at 1577. The district court thus concluded "the emails Watts accessed were 'service copies,' that is, copies of an email immediately accessible to the user by logging in to the email client, rather than the backup 'storage copies' maintained by VCCS, which are available only upon special request." *Id.*

The court's analysis fails to acknowledge that these "service copies" of Mr. Hately's e-mails are *also* stored by VCCS and Google. Thus, they are *also* in "electronic storage" within an "electronic communication service." "Storage under these circumstances thus literally falls within the statutory definition." *Theofel*, 359 F.3d at 1075 ("An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again – if, for example, the message is accidentally erased from the user's own computer.").

Further, the language of the SCA does not include the term "copy." The district court's ruling improperly reads new language into the Act and creates a brand-new distinction that nowhere to be found within the statute. The district court's opinion then creates two different categories of copies: "service copies" and "storage copies." *See supra.* This distinction is completely lacking in precedent, by any court, anywhere.

Higher courts have already addressed those situations in which a copy of an electronic communication should be considered to be in backup storage, as well as those scenarios when application of the term would be inappropriate. *Theofel*, 359 F.3d at 1076 ("[Amicus] [] argues that we upset the structure of the Act by defining 'electronic storage' so broadly as to be superfluous . . . [This] claim relies on the argument that any copy of a message necessarily serves as a backup to the user, the service or both. But the mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose. We see many instances where an ISP could hold messages not in electronic storage – for example, e-mail sent to or from the ISP's staff, or messages a user has flagged for deletion from the server. In both cases, the messages are not in temporary, intermediate storage, nor are they kept for any backup purpose.").

The Ninth Circuit has already articulated occasions on which an electronic communication should be considered *not* within the definition of "electronic

storage." *Supra*. Mr. Hately's e-mails that were accessed by Watts do not fall within the previously-detailed exceptions, nor are they analogous thereto. After initially reading the e-mails that Watts read, Mr. Hately retained them for future reference; he did not delete them. In so doing, Mr. Hately maintained the e-mails with VCCS and Google, where he could again access or download them through a web browser if it became necessary. Thus, Mr. Hately stored the e-mails with the electronic communications services for his own "purposes of backup protection." And, "the statue does not specify *whose* 'purposes of backup protection' are relevant." *Cheng*, No. 11-10007-DJC, 2013 U.S. Dist. LEXIS 179727, 2013 WL 6814691, at *8 n.3 (citing multiple authorities). Mr. Hately's purpose of backup protection is equally as valid as VCCS's in its own, separate retention, and qualifies his e-mails for protection under subsection (B) of the definition of "electronic storage."

The district court felt otherwise. Presenting a very strained reading of the definition, the court wrote:

> Based on the plain and ordinary meaning of the text and also the structure of the SCA, the Court concludes that the "backups" in paragraph (B) are most logically and reasonably read as referring only to backups of the transitory communications described in paragraph (A), created and stored separate and apart from the copies maintained to facilitate continuing access by the user through his account. As the Supreme Court of South Carolina summarized the scope of § 2510(17), "electronic storage refers only to temporary storage, made in the course of transmission, by an ECS provider [per paragraph (A)], and to backups of such communications[,]" per paragraph (B).

> *Jennings v. Jennings*, 736 S.E.2d 242, 248 (S.C. 2012) (Toal, C.J., concurring in the result) (emphasis omitted).
>
> Read this way, "such communication" in § 2510(17)(B) refers to communication "temporar[ily and] intermediate[ly]" stored "incidental to the electronic transmission thereof," as described in (A). Under this view of the SCA, once an email has been delivered and opened, its transmission is complete, the ECS is no longer storing it "incident to transmission" and therefore it is not it "electronic storage" for the purposes of § 2510(17)(A). A service copy maintained to be available to the user until the user deletes the message is neither a "copy of *such*" communication, nor is it maintained by the ECS for backup protection. Instead, paragraph (B) refers to a copy of a communication, made by the ECS while the communication was in transit, and stored by the ECS for its own backup or administrative purposes.

See JA at 1579. (emphasis and alterations in original). The district court impermissibly reads additional new requirements into the SCA, stating that in order for an electronic communication to be considered to be in "backup storage," a copy must have been made of it *while it was in transit*. This is completely unsupported by the text of the statute.

Equally concerning is the Court's finding that a message must be "stored by the ECS for its own backup or administrative purposes." Again, this finding is completely unsupported by the statute. The statute plainly states that "electronic storage" includes "*any* storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 USCS § 2510(17)(B) (emphasis added).

Compare the clear language of this subsection of the law to the District Court's holding, which states that this statutory text should mean that protection is only provided "to a copy of a communication, made by the ECS while the communication was in transit, and stored by the ECS for its own backup or administrative purposes." *See* JA at 1579.

The District Court's misapplications are clear. First, the statute applies to "*any* storage" while the District Court finds protection only for a "copy" "made by the ECS while the communication was in transit." Notably, the definitions found in the statute make no mention of the word "copy" in any instance.

Second, the District Court finds that the communication must be "stored by the ECS for its own backup or administrative purposes." Quite oppositely, the statute protects "*any* storage of such communication by an electronic communication service for purposes of backup protection," (emphasis added) and makes no limitation, whatsoever, as to who decides to retain the communication. The District Court's addition of language such as "its own" is plainly and conspicuously missing from the statute.

On this second issue, as to who determines the "backup" status,the District Court's purported limitation is especially concerning, because the "electronic communication service," is only a service that provides "*users thereof* the ability to send or receive wire or electronic communications." 18 USCS § 2510(15). In short,

an "electronic communication service" cannot lawfully exist under the statute without *users* having the ability to receive wire or electronic communications. The District Court's finding that the statute only protects an ECS' "own backup or administrative purposes" is erroneous on two levels. It introduces language and standards that are not anywhere in the statutory text *and* similarly ignores that the statute expressly demands that ECS services exist only to be "provide[d] to users." *Id.* While Plaintiff does not dispute that electronic communication services are protected under the statute, "users," without which ECS would not exist, are necessarily subject to the same protections, if not *greater* protection.

Moreover, referring to 18 USCS § 2510(17), "in contrast to subsection (A), subsection (B) does not distinguish between intermediate and post-transmission storage. Indeed, [the] interpretation [found in *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001), *aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2003)] renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary, intermediate storage' within the meaning of subsection (A)." *Theofel*, 359 F.3d at 1075-76. The Ninth Circuit in *Theofel* correctly read the statute and concluded that, "[b]y its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission." *Id.* at 1076.

"To conclude that only *unopened* emails could be deemed to be stored for backup purposes would render § 2510(17)(B) 'superfluous,' because such 'temporary, intermediate' emails would already be deemed in 'electronic storage' under § 2510(17)(A)." *Levin*, No. TDC-16-2790, 2017 U.S. Dist. LEXIS 106480, 2017 WL 2937938, at *13 (emphasis added) (citing *Theofel* at 1075-76). Again, as demonstrated, precedent favors Plaintiff on this issue, and demands that the matter be remanded for further proceedings.

4. *Below, the district court concluded that VCCS was acting as an RCS, rather than an ECS, with respect to the "service copies" of Mr. Hately's e-mail messages and ruled that this renders the "service copies" unprotectable. However, all persuasive authority is strongly indicative of the contrary conclusion, suggesting that if VCCS does play an RCS role, it is with respect to its "storage copies," and even if VCCS did act as an RCS with respect to the "service copies" of Mr. Hately's e-mails, there is nothing in the statute that would make this detail dispositive of Mr. Hately's SCA claim.*

As an alternative basis for determining that Watts is not liable to Mr. Hately's for his unauthorized accessing of Mr. Hately's e-mail communications, the District Court found that "[e]ven if the service copies at issue here were copies of temporary versions of the emails stored by VCCS 'for purposes of backup protection,' they would still not be 'in electronic storage' [] because VCCS was not acting as an ECS with respect to those service copies." *See* JA at 1580.

The District Court's findings on this issue, and the supporting analysis, were *very clearly* erroneous, for numerous reasons.

First, as discussed above, the idea of "service copies" is not in the statute and has not been introduced by *any* other reviewing court. Introduction of additional complexity to an already challenging statute is at once error and ill-advised.

Second, the District Court's opinion plainly confuses an end user's private, *personal* computer, which is accessible only to the user, with an "electronic communication service." One clear example of this misapplication is the District Court's citation to *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 522 ("Clearly, the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers."). In that case, the Plaintiffs alleged that DoubleClick's placement of web "cookies" on the personal computer hard drives of Internet users was unlawful. Notably, these users accessed DoubleClick-affiliated web sites in their day-to-day web browsing habits, and DoubleClick subsequently placed small text files on the web browsers' computers, for purposes of tracking the users for advertising purpose. In *DoubleClick*, the computer hardware and purposes were completely inapposite to the present matter because that matter involved personal computers, and not an "electronic communication service."

In *DoubleClick* there were millions of personal computers that were owned and operated by end users solely for the benefit of the end users. By way of

example, a computer in the *DoubleClick* category would be a private attorney's laptop, owned and controlled by the attorney user. That piece of hardware is not a "service" because, in contrast to an "electronic communication service" an attorney's computer does not provide "the ability to send or receive wire or electronic communications" to hundreds, thousands, or even millions of people. Compare this to VCCS/Google, where the online services are provisioned and designed to be accessed and employed by numerous authorized users, at all times of the day. One could walk down the streets of Richmond and easily meet numerous people with authorized Gmail, Yahoo Mail, Hotmail or VCCS email accounts. There are clear, plain differences between the personal computers at issue in *DoubleClick*, and the "electronic computer services" at issue in this case. The District Court's application of *DoubleClick* to the instant matter was accordingly erroneous.

Third, the Ninth Circuit addressed the ECS versus RCS statuses in *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), *rev'd in part on other grounds*, *City of Ontario v. Quon*, 560 U.S. 746 (2010). The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Applying this definition to the facts in *Quon*, the Ninth Circuit concluded that, "[o]n its face, this describes the text-messaging pager services that Arch Wireless provided." *Id.* at

901. So, too, does this describe the e-mail services that VCCS/Google provided to Mr. Hately.

"Contrast that definition with that for an RCS, which 'means the provision to the public of computer storage or processing services by means of an electronic communication system.'" *Id.* (quoting 18 U.S.C. § 2711(2)). Applying this definition in turn, the Ninth Circuit explained:

> Arch Wireless did not provide to the City "computer storage"; nor did it provide "processing services." By archiving the text messages on its server, Arch Wireless was certainly "storing" the messages. However, Congress contemplated this exact function could be performed by an ECS as well, stating that an ECS would provide (A) temporary storage incidental to the communication; and (B) storage for backup protection.

Id. (citing 18 U.S.C. § 2510(17)). The court then turned to the legislative history for additional insights:

> In the Senate Report, Congress made clear what it meant by "storage and processing of information." It provided the following example of storage: "physicians and hospitals maintain medical files in offsite data banks." Congress appeared to view "storage" as a virtual filing cabinet, which is not the function Arch Wireless contracted to provide here. The Senate Report also provided an example of "processing information": "businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services." . . . Neither of these examples describes the service that Arch Wireless provided to the City.

Id. Like Arch Wireless in *Quon*, VCCS and Google provide Mr. Hately with electronic communication services, and not "remote computing services."[6]

This analysis makes sense. Consider the Gmail email service with the "Google Drive" service. Gmail is an email service, which is plainly contemplated as an "electronic communication service." Google Drive is a file storage and synchronization service that advertises "free Google online storage, so you can keep photos, stories, designs, drawings, recordings, videos – anything."[7] Despite being owned by the same company, Gmail and Google Drive are separate products, advertised differently, and providing plainly different purposes. Google Drive is an example of a product that would likely qualify as a "RCS," but not an "ECS" had there been an access of, for example, scanned copies of printed emails that Plaintiff might have stored on Google Drive. Google Drive is a "virtual filing cabinet," and comfortably qualifies as an "RCS," but not an "ECS."

As to the question of "processing services," there is no plausible way to claim that the VCCS account would qualify as a "RCS" under such analysis. By way of example, the U.S. Department of Labor classifies certain industries into identifiable groups, known as "Standard Industrial Classification." One such

[6] Again, much of the "RCS" discussion and argument herein, was not, in any way, part of the record below, and was introduced by the District Court, *sua sponte*, only in the final ruling.

[7] *See* Google Drive, *available at* https://www.google.com/drive/ (last visited May 19, 2018).

category is "Industry Group 737 Computer Programming, Data Processing, And Other Computer Related Services."[8] The Department of Labor's definition of such services includes:

> Establishments primarily engaged in providing computer processing and data preparation services. The service may consist of complete processing and preparation of reports from data supplied by the customer or a specialized service, such as data entry or making data processing equipment available on an hourly or time-sharing basis.

Id. By way of modern day example, these services would include heavy data processing companies, like "BA Merchant Services," for handling financial transaction processing, and "Acxiom Corporation," which collects, analyzes and sells customer and business information used for targeted advertising campaigns. There is no viable argument that the web-based email accounts contemplated herein are in the same category as these large data "processing" firms.

Even if Mr. Hately's ECS mutated into an RCS when delivering e-mails to Mr. Hately's account, it does not follow that such e-mails would cease to be protectable under the SCA, as the unauthorized individual would nonetheless be accessing a facility – the ECS/RCS's computer servers – through which an electronic communication service is provided. Simply because an e-mail is being

[8] *See* Description for 7374: Computer Processing and Data Preparation and Processing Services; Occupational Safety and Health Administration, *available at* https://www.osha.gov/pls/imis/sic_manual.display?id=151&tab=description (last visited May 19, 2018).

delivered by an RCS does *not* mean that it was not also stored and provided by the ECS for purposes of backup protection.

Finally, it bears repeating that it is undisputed between the parties that, like Plaintiff Hately, "VCCS students use GSuite for Education, which includes Gmail. Each student's VCCS email account is a Google Email (Gmail) account with an address that ends in "@email.vccs.edu." *See* JA at 1437. While VCCS is the "branded version" or "wrapper," the underlying technology and platform is identical to the standard Gmail platform. When the parties refer to the "VCCS account," or similar, it refers to the "vccs.edu" domain name and the graphical branding thereto. VCCS and Gmail are not, for purposes of this case, evaluated differently. The district court did not appear to treat VCCS and Gmail differently, which was correct under the factual circumstances.

As discussed, the lower court's analysis related to "ECS" and "RCS" was erroneous for numerous reasons and should not be adopted on appeal.

CONCLUSION

For all the reasons set forth herein, the matter should be reversed and remanded for further proceedings.

PLAINTIFF'S POSITION ON ORAL ARGUMENT

Plaintiff believes that this matter should be resolved in Plaintiff's favor based solely on the substantial record and written briefs. Accordingly, Plaintiff

does not formally request oral argument. However, if the court would find oral argument valuable in its consideration, Plaintiff would welcome the opportunity to present oral argument at the court's direction.

Respectfully Submitted

/s/ Eric James Menhart
Eric James Menhart
LEXERO LAW
316 F Street, NW
Suite 101
Washington, DC 20002
Counsel for Appellant

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

Certificate of Compliance with Type-Volume Limitation,
Typeface Requirements and Type Style Requirements

1. This brief complies with the type-volume limitation of Fed. R. App. 32(a)(7)(B) because:

   The word count of this brief is 12,855.

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   This brief has been prepared in a proportionally spaced typeface using Microsoft Word, Times New Roman, 14 point.

May 21, 2018

/s/ Eric James Menhart
Eric James Menhart

CERTIFICATE OF SERVICE

I hereby certify that I have this May 21, 2018, filed the foregoing Brief of Appellant using the Court's CM/ECF system which will send notification of such filing to the following counsel:

Jonathan David Frieden
James Paul Menzies Miller
ODIN, FELDMAN & PITTLRMAN, PC
1775 Wiehle Avenue
Suite 400
Reston, Virginia 20190
(703) 218-2100

/s/ Eric James Menhart
Eric James Menhart