

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CAROL LEE WALKER : CIVIL ACTION
: :
v. : NO. 17-40
: :
SENIOR DEPUTY BRIAN T. :
COFFEY, *et al.* :

KEARNEY, J.

December 11, 2018

MEMORANDUM

An employer's internal lawyer agreed to produce emails sent to or from one of its employees in response to a defective subpoena from state prosecutors. We previously held, and find again today, the defective subpoena did not unduly coerce an internal lawyer to voluntarily produce documents. We earlier dismissed the employee's Fourth Amendment claim based on the prosecutor's qualified immunity and our Court of Appeals affirmed. In a second amended complaint, the employee now sues the prosecutor and case agent for violating the Stored Communications Act in obtaining these emails on the employer's servers. But the fact remains the employer agreed to produce— and participated in collecting — email on its servers produced to the prosecutors. Even absent this authorization, the prosecutors are today entitled to qualified immunity from liability under the Stored Communications Act. The employee cannot show clearly established law requiring prosecutors to consider every email stored on an employer's server as backup protected (covered by the Stored Communications Act) or the prosecutors must always use a warrant to obtain these emails especially when, as today, the employer's internal lawyer turned over the emails on its server without coercion. We grant the employer's motion to dismiss the Stored Communications Act claim in the accompanying Order.

I. Allegations

Carol Lee Walker worked at Penn State University and used an employee email account it provided.¹ Penn State maintained the email system on its servers.² Ms. Walker alleges Penn State “stored and/or backed up” her emails on its “computer systems and/or servers.”³

In July 2015, the Commonwealth charged Ms. Walker and her husband Ray Walker with several computer and related conspiracy crimes.⁴ After an August 19, 2015 hearing the Commonwealth dismissed all charges against Ms. Walker except conspiracy to commit forgery.⁵ The Office of the Attorney General assigned Brian Coffey as the attorney and Paul Zimmerer as the agent for Ms. Walker’s case.⁶ Following the August 19, 2015 hearing, Ms. Walker alleges Messrs. Coffey and Zimmerer “hatched a scheme to conduct additional investigation” of Ms. Walker and her husband by obtaining her “stored electronic communications” from Penn State’s servers.⁷

Messrs. Coffey and Zimmerer requested Ms. Walker’s emails from her employee email account but Penn State demanded a subpoena.⁸ Mr. Coffey then prepared a subpoena directed to John Corro, Penn State’s General Counsel and Senior Security/Systems Analyst.⁹ The subpoena did not list the “place, date, time, and party on behalf of whom testimony [was] demanded.”¹⁰ Mr. Coffey subpoenaed the production of “any & all emails/compute [sic] files/documents/attachments to or from Carol Lee Walker, CLW9@psu.edu” followed by several email addresses.¹¹

On October 20, 2015, the Honorable Thomas K. Kistler of the Court of Common Pleas of Centre County witnessed the subpoena and the Prothonotary signed it.¹² The next day, Mr. Zimmerer went to Penn State’s General Counsel’s Office and presented the subpoena to Assistant General Counsel Katherine Allen.¹³ Despite the missing information, Ms. Allen did not contest the validity of the subpoena and assisted Messrs. Coffey and Zimmerer in obtaining Ms. Walker’s

emails.¹⁴ Ms. Walker alleges this subpoena is “illegal and fraudulent” because it lacked the place, date, time, and party from whom they demanded testimony.¹⁵

Ms. Walker initially sued Messrs. Coffey and Zimmerer under Section 1983 for an illegal search and seizure of her emails under the Fourth Amendment.¹⁶ We dismissed Ms. Walker’s Amended Complaint after finding qualified immunity protects Messrs. Coffey and Zimmerer from liability for Ms. Walker’s Fourth Amendment claims.¹⁷ Ms. Walker moved for reconsideration and leave to file a second amended complaint on May 8, 2017, and attached a proposed complaint including new claims under the Stored Communications Act.¹⁸ On May 17, 2017, we denied the motion finding amendment would be futile.¹⁹

On September 20, 2018, our Court of Appeals affirmed our finding qualified immunity shielded Messrs. Coffey and Zimmerer for Ms. Walker’s Fourth Amendment claim.²⁰ Our Court of Appeals vacated our order denying leave to amend so we could more fully address potential liability under the Stored Communications Act.²¹

In her Second Amended Complaint, Ms. Walker sues Messrs. Coffey and Zimmerer under Sections 2701(a), 2703(a), and 2703(b) of the Stored Communications Act alleging the same facts. Messrs. Coffey and Zimmerer now move to dismiss the Second Amended Complaint, arguing (1) Ms. Walker fails to state a claim or (2) they are entitled to qualified immunity for her claims under the Act.²²

II. Analysis²³

Messrs. Coffey and Zimmerer argue we should dismiss Ms. Walker’s claims because (1) she fails to state a claim under the Stored Communications Act, or (2) qualified immunity bars her claims because (a) it is not “clearly established” law enforcement should first assume opened emails in post-transmission storage on a private employer’s server are in “electronic storage”

covered by the Stored Communications Act and (b) it is not “clearly established” law enforcement must always obtain a warrant or valid subpoena even if the employer first requests a subpoena but then consents to a search of its emails. We find Ms. Walker has failed to state a claim under the Act as a citizen may turn over information to the government absent coercion regardless of the status of the subpoena. Even assuming she states a claim, qualified immunity shields Messrs. Coffey and Zimmerer from liability under the Act.

A. Ms. Walker fails to state a claim under the Stored Communications Act.

Messrs. Coffey and Zimmerer argue Ms. Walker failed to state a claim under the Act because Penn State authorized production of Ms. Walker’s emails. Ms. Walker argues Messrs. Coffey and Zimmerer fraudulently compelled production of the emails using an invalid subpoena. We agree with Messrs. Coffey and Zimmerer.

1. Ms. Walker fails to state a claim under Section 2701(a).

To state a claim under Section 2701(a) of the Stored Communications Act, Ms. Walker must allege Messrs. Coffey and Zimmerer “(1) intentionally accesse[d] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[ed] an authorization to access that facility; and thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it is in electronic storage in such system[.]”²⁴ Section 2701(a) does not apply if Messrs. Coffey and Zimmerer’s conduct was “authorized by the person or entity providing a wire or electronic communications service.”²⁵

The parties agree Penn State provides electronic communications services to its employees through its employee email system. Ms. Walker alleges Messrs. Coffey and Zimmerer initially requested Penn State voluntarily produce Ms. Walker’s emails from her work email account. Penn State officials demanded a subpoena. Ms. Walker alleges Messrs. Coffey and Zimmerer used a

“fraudulent and illegal subpoena to trick” Penn State into producing her emails. Mr. Zimmerer served the subpoena on Penn State’s Assistant General Counsel. The subpoena lacked a date, time, and place for Penn State officials to appear with the emails. Notwithstanding the subpoena’s deficiencies, the Assistant General Counsel did not contest the subpoena’s validity and assisted Messrs. Coffey and Zimmerer in obtaining Ms. Walker’s emails.

Ms. Walker fails to allege Messrs. Coffey and Zimmerer obtained Ms. Walker’s emails without authorization. Messrs. Coffey and Zimmerer cannot be liable under Section 2701(a) if their conduct was “authorized by the person or entity providing a wire or electronic communications service,” in this case, Penn State.²⁶

Ms. Walker argues Penn State could not have authorized production because the use of an invalid subpoena “negated” Penn State’s authorization. We disagree. Although the subpoena lacked critical information, Ms. Walker alleges Mr. Zimmerer presented the subpoena to Penn State’s Assistant General Counsel. Counsel did not contest the validity of the subpoena despite its clear lack of a date, time, and place to appear with the emails. Counsel further assisted Messrs. Coffey and Zimmerer in obtaining Ms. Walker’s emails. Ms. Walker fails to allege facts showing Penn State did not voluntarily authorize production of the emails.

While ruling under the Fourth Amendment, our Court of Appeals, analyzing the same facts, found Messrs. Coffey and Zimmerer did not coerce Penn State’s consent with the invalid subpoena.²⁷ Our Court of Appeals explained Penn State “was not merely a private party induced to perform a search; rather it was a third party with common authority over Walker’s emails and the independent ability to consent to a search.”²⁸ The court found “rather than contest the validity of the subpoena or otherwise limit any search,” Penn State’s Assistant General Counsel instructed Penn State’s employees to assist in the production of Ms. Walker’s emails.²⁹ The court held

“[u]nder these circumstances, despite the facial invalidity of the subpoena, we decline to find that the university’s conduct was coerced.”³⁰ We do not merely apply our Court of Appeals’ holding on Ms. Walker’s Fourth Amendment claim to her claim under the Act under the law of the case. Rather, we find our court of appeals’ reasoning persuasive in finding Messrs. Coffey and Zimmerer did not coerce Penn State’s authorization with respect to Ms. Walker’s emails.³¹

Because we find Ms. Walker failed to state a claim under Section 2701(a) of the Stored Communications Act, we dismiss Ms. Walker’s claim.

2. Ms. Walker fails to state a claim under Section 2703.

Messrs. Coffey and Zimmerer argue Ms. Walker fails to state a claim under Section 2703 of the Act. Section 2703(a) provides a procedure for the government to obtain emails in electronic storage for 180 days or less:

[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.

Section 2703(a) also provides a procedure for the government to obtain emails in electronic storage for more than 180 days:

A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.³²

Section 2703(b) identifies ways to obtain the contents of electronic communications:

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section[.]³³

Unlike Section 2701, Section 2703 does not except the defendant's conduct when he obtains the service provider's authorization. But we cannot find, as Ms. Walker's counsel argued, Congress intended to remove the government's ability to obtain emails through consent. The government can always obtain documents through a party's consent.³⁴ The statute provides the government "may require" disclosure under this section. As "may require" implies such procedures are not mandatory, this language only makes sense if the government can also obtain emails through a party's consent.

At oral argument, Ms. Walker's counsel argued because Penn State initially demanded a subpoena but ultimately produced her emails after Messrs. Coffey and Zimmerer presented an invalid subpoena, Messrs. Coffey and Zimmerer did "require" production and thus must obtain a warrant under Section 2703. But if we accept counsel's argument, we would remove a party's ability to consent even after the government "requires" production. We proposed a hypothetical: after Penn State demanded a subpoena, suppose Penn State's counsel called the Attorney General's Office and said Penn State would voluntarily produce Ms. Walker's emails regardless of the defective subpoena. Is there a reason Penn State cannot cooperate with prosecutors as to its own records? We cannot say, and counsel failed to argue, Messrs. Coffey and Zimmerer were still required to follow the procedures in Section 2703 after such consent.

Because we find Penn State consented to disclosure of Ms. Walker's emails, we find Ms. Walker fails to state a claim under Section 2703. We dismiss Ms. Walker's claim.

B. We may apply qualified immunity to claims under the Stored Communications Act.

Even assuming Ms. Walker states a claim under the Act, we find Messrs. Coffey and Zimmerer are entitled to qualified immunity for Ms. Walker's claims under the Act.

Before we determine whether qualified immunity applies, we must determine whether Messrs. Coffey and Zimmerer are able to invoke qualified immunity as a defense to claims under the Stored Communications Act. Messrs. Coffey and Zimmerer argue they may invoke qualified immunity to claims under the Act since Congress failed to abrogate qualified immunity. Ms. Walker argues they cannot invoke qualified immunity as a defense to claims under the Act because Congress provided a statutory good faith defense.

Our court of appeals has not determined whether a defendant can claim qualified immunity for violations of the Act. We look to other courts of appeals.

Ms. Walker relies on *Berry v. Funk* in arguing qualified immunity does not apply to Stored Communications Act violations. In *Berry*, the Court of Appeals for the District of Columbia Circuit held qualified immunity does not apply to violations of the Wiretap Act.³⁵ The court explained defendants usually invoked qualified immunity for *Bivens* and § 1983 suits.³⁶ The court found because Congress provided a complete "good faith" defense in the Wiretap Act for reliance on a warrant, the defendants could not invoke qualified immunity, explaining "[w]hen Congress itself provides for a defense to its own cause of action, it is hardly open to the federal court to graft common law defenses on top of those Congress creates."³⁷ The court did not determine whether qualified immunity applied to Stored Communications Act violations.

In *Schmitz*, a public policy advocacy group sued the district attorney and others for violating the Act when the district attorney's office obtained emails under an investigation into campaign misconduct.³⁸ While acknowledging Congress provided a "good faith" defense in the

Act for officers relying on a warrant, the Court of Appeals for the Seventh Circuit also held the defendants could invoke qualified immunity under the Act.³⁹ The court acknowledged the *Berry* decision but explained it has “consistently recognized qualified immunity for alleged Wiretap Act violations” and saw “no persuasive reason” to distinguish between the Wiretap Act and the Stored Communications Act.⁴⁰

Other courts of appeals disagree with the *Berry* decision. In *Blake v. Wright*, the Court of Appeals for the Sixth Circuit applied qualified immunity to Wiretap Act claims alleging a police chief monitored police department employees’ telephone calls.⁴¹ The court explained the Wiretap Act’s “good faith” defense applied to all citizens, not just public officials.⁴² The court further explained federal courts, in developing the qualified immunity doctrine, intended public officials “receive additional protection in responding to constitutional and statutory claims when ordinary citizens do not.”⁴³ Because it did not expressly abrogate qualified immunity, Congress did not intend through silence to remove the qualified immunity defense.⁴⁴

In *Tapley v. Collins*, the plaintiff alleged a police chief violated the Wiretap Act when he intercepted the plaintiff’s phone calls on his personal radio scanner.⁴⁵ The Court of Appeals for the Eleventh Circuit applied qualified immunity under the Wiretap Act despite a good faith defense in the statute.⁴⁶ The court found a defendant may invoke qualified immunity for a statutory violation, noting eleven court of appeals decisions holding qualified immunity available to claims under eight different federal statutes.⁴⁷ The court found Congress did not expressly abrogate qualified immunity in the Wiretap Act and explained “the Supreme Court has said that the defense of qualified immunity is so well established, that if Congress wishes to abrogate it, Congress should specifically say so.”⁴⁸ The court further explained qualified immunity and the good faith defense are not the same. The good faith defense is an affirmative defense to liability usually

proved later in the case. Since the Supreme Court instructs courts to determine qualified immunity at the earliest stage possible, the court found the qualified immunity defense protects public officials from extended litigation under the Act.⁴⁹

In an unpublished decision in *Diana v. Oliphant*, our Court of Appeals held qualified immunity bars liability Wiretap Act claims of two police officers recording his phone calls.⁵⁰ The court found the law was not “clearly established” the officers could not rely on an exception in the Wiretap Act when they recorded the phone calls.⁵¹

In *Cruz Lopez v. Pena*, the District Court for the Northern District of Texas applied qualified immunity for violations under the Stored Communications Act.⁵² The court held qualified immunity shielded defendants since it was not “clearly established” the defendants obtained emails in “electronic storage” under the Act.⁵³

We find qualified immunity is available for Stored Communications Act claims. While Congress provides a “good faith” defense in the statute, it did not abrogate the qualified immunity defense. We presume Congress was aware of qualified immunity when it passed the Stored Communications Act in 1986 and could have abrogated qualified immunity if it meant to remove it as a defense.⁵⁴ Since the Supreme Court provided for qualified immunity before 1986,⁵⁵ we will not interpret Congress’s silence as intent to remove the qualified immunity defense. Our Court of Appeals applied qualified immunity to a claim under the Wiretap Act, which also contains a statutory good faith defense. Our decision on qualified immunity may shield the public officials in this case from extended litigation whereas the defendants may not be able to prove the statutory good faith defense until a later stage.

Messrs. Coffey and Zimmerer can invoke qualified immunity as a defense to Ms. Walker’s claims under the Stored Communications Act.⁵⁶

C. Messrs. Coffey and Zimmerer are entitled to qualified immunity from Ms. Walker's Stored Communications Act claims.

As we hold Messrs. Coffey and Zimmerer may claim qualified immunity as defense to claims under the Act, we now determine whether qualified immunity bars Ms. Walker's claims. We apply a two-step qualified immunity analysis: "(1) whether the plaintiff sufficiently alleged the violation of a constitutional right, and (2) whether the right was 'clearly established' at the time of the official's conduct," here, in October 2015.⁵⁷ For purposes of deciding a motion to dismiss, qualified immunity "will be upheld on a 12(b)(6) motion only when the immunity is established on the face of the complaint."⁵⁸

To determine whether a right is clearly established, we first look to "applicable Supreme Court precedent."⁵⁹ If none exists, we see if "there is a case of controlling authority in our jurisdiction or a 'robust consensus of cases of persuasive authority' in the Courts of Appeals [that] could clearly establish a right for purposes of qualified immunity."⁶⁰ "[T]here must be sufficient precedent at the time of action, factually similar to the plaintiff's allegations, to put defendant on notice that his or her conduct is [statutorily] prohibited."⁶¹ "The authority need not be 'directly on point, but existing precedent must have placed the statutory or constitutional question beyond debate.'"⁶²

1. Ms. Walker fails to show it was "clearly established" her emails on Penn State's server were in "electronic storage" under the Act.

Messrs. Coffey and Zimmerer argue they did not violate a "clearly established right" because it is not "clearly established" law enforcement officers must presume emails on an employer's server are in "electronic storage" as the term is defined in the Act. Ms. Walker argues the law is "clearly established" emails on a non-public electronic communications service provider are in "electronic storage."

For us to find Messrs. Coffey and Zimmerer liable under the Act, they must have obtained emails in “electronic storage.” Both Sections 2701 and 2703 apply only to electronic communications held in “electronic storage.” Congress defined “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.”⁶³

The parties do not dispute Penn State provides non-public electronic communication services through its employee email system. The parties also agree Ms. Walker’s emails were not in “temporary, intermediate storage.” The parties dispute whether Ms. Walker’s emails are in storage “for purposes of backup protection.” Messrs. Coffey and Zimmerer argue our Court of Appeals has not “clearly established” emails on a non-public email service provider’s server are in “electronic storage” as defined in the Act. They further argue a non-public electronic communication services provider like Penn State does not store employees’ opened emails on its servers for “purposes of backup protection.”

Ms. Walker argues it is clearly established emails on her employer’s server are stored for “purposes of backup protection.” In other words, Ms. Walker argues an officer seeking to obtain emails from a non-public service provider’s server must presume every email is stored on the provider’s server for “purposes of backup protection” and thus the Stored Communications Act always governs the officer’s conduct. We cannot find the law is “clearly established” on this issue. To the contrary, there is significant debate over the contours of the term “for purposes of backup protection” under the Act.

Neither party directs our attention to Supreme Court precedent on this issue. Mr. Coffey cites *Fraser v. Nationwide Mutual Insurance Company* in support of his claim. In *Fraser*, a man

sued his former employer under the Stored Communications Act after the employer searched his emails in his employee email account on the company's central server without his consent.⁶⁴ The court distinguished amongst three types of email storage: (1) "intermediate storage," in which the employer's email system stores the message after the user sends the message; (2) "backup protection storage," in which the system stores a copy of a message for backup purposes in case the system crashes before it can complete transmission; (3) "post-transmission storage," where the system stores a message after the recipient logs on and retrieves the message.⁶⁵ The court found no liability against the employer under the Act as the employer obtained "post-transmission" emails.⁶⁶ The court explained opened messages in "post-transmission storage" are not protected under the Act because they are not in intermediate storage under Section 2510(17)(A) and they are not being stored for "purposes of backup protection" under Section 2510(17)(B).⁶⁷

Our Court of Appeals reversed the district court's decision on different grounds. Explaining it was "questionable that the transmissions were not in backup storage," the court determined for purposes of its ruling it was "assuming without deciding that the e-mail in question was in backup storage."⁶⁸ The court then held the employer exempt under a different section of the statute.⁶⁹

In *Bansal v. Russ*, the plaintiff sued the U.S. Attorneys' Office for violating the Act during an investigation into a drug conspiracy.⁷⁰ The plaintiff alleged the attorneys searched his university email account without a warrant and obtained "opened" emails.⁷¹ The court dismissed the claim, explaining "to the extent Plaintiff purports to assert claims for violation of the Stored Communications Act based on the government's obtaining of 'opened' e-mails, the claims must be dismissed because such conduct, even if proved, does not violate the Act."⁷²

Ms. Walker cites a handful of district court cases in our District to support her argument emails like the ones Messrs. Coffey and Zimmerer obtained are in "electronic storage;" but these

cases fail to show the issue with post-transmission emails is “beyond debate” as required to find a right “clearly established.”⁷³ In *Markert*, the plaintiff claimed his employer violated the Act when it accessed his personal email account from his work computer.⁷⁴ In response to the employer’s argument post-transmission emails are not in “electronic storage” under the Act, the district court explained “the Third Circuit has not yet directly held that this is the proper interpretation of the Act” but acknowledged the court of appeals’ “nod in that direction.”⁷⁵ In *Brooks*, the district court did not rule whether post-transmission emails fell within the definition of “electronic storage” since the parties agreed they did.⁷⁶ In *Integrated Waste*, the district court explained our court of appeals “suggested” post-transmission emails are in “electronic storage” under the Act but found it “need not join the debate over post-transmission storage” since the plaintiff plead access to both pre- and post-transmission emails.⁷⁷ In *Strategic Wealth*, the district court found persuasive “the Third Circuit’s assumption that an opened e-mail retained on a server is in the backup storage contemplated by the Act.”⁷⁸ The court also acknowledged the “debate over [the Act’s applicability to] post-transmission storage.”⁷⁹

These cases fail to satisfy the “clearly established” standard as the court in each case acknowledged the “debate” in this area of law. The parties do not cite authority, and we cannot find any, ending this debate.

Ms. Walker also relies on an oft-cited and widely disputed decision from the court of appeals for the Ninth Circuit.⁸⁰ In *Theofel*, an attorney issued an overbroad subpoena seeking copies of emails from an opposing company in litigation.⁸¹ After a judge in the underlying litigation found the subpoena “patently unlawful,” the company sued the attorney under the Stored Communications Act.⁸² The attorney argued because the emails remained on the server after the recipient opened the emails, the emails were not in “electronic storage” under the Act.⁸³ The court

disagreed. The court found emails stored on the server even after the recipient opens the emails are being stored “for purposes of backup protection.”⁸⁴ The court explained an internet service provider stores messages on its server 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. The ISP copy of the message functions as a ‘backup’ for the user.”⁸⁵

District courts in the Ninth Circuit bound by *Theofel* apply the rule very strictly. In *Gonzales*, the plaintiff brought a class action under the Act on behalf of Lyft drivers claiming Uber intercepted electronic communications showing the drivers’ locations.⁸⁶ The court dismissed the plaintiff’s claims because he did not allege facts showing Uber intercepted electronic communications stored “for purposes of backup protection.”⁸⁷ To do so, the court explained the plaintiff would have to allege Uber accessed “a *separate* copy . . . that exists outside of Lyft’s servers[.]”⁸⁸ In *Cline*, the court dismissed the plaintiff’s claims under the Act for failure to allege facts showing the opened emails were stored for the “purpose of backup protection.”⁸⁹ The court rejected the argument “that any emails stored on the server of an internet service provider (ISP) following delivery are necessarily stored for backup purposes.”⁹⁰

In *United States v. Warshak*, the court of appeals for the Sixth Circuit explained the decision in *Theofel* did not bind them and cited commentary on the Stored Communications Act explaining “*Theofel* is quite implausible and hard to square with the statutory test.”⁹¹ In the commentary, Professor Kerr explains Congress understood a “backup copy” to be a “copy made by the service provider for administrative purposes,” such as in the event of a server crash or similar problem. This understanding of a “backup” copy is inconsistent with an opened email on an employer’s server. He also cites legislative history showing Congress intended to keep opened emails covered under a different section of the statute with separate rules for obtaining these

emails.⁹² If opened, post-transmission emails fall under “electronic storage,” government officials would be subject to conflicting requirements.⁹³

District courts from other circuits disagree with *Theofel*. In *United States v. Weaver*, the district court for the Central District of Illinois explained the court’s reasoning in *Theofel* does not square with the legislative history of the Act.⁹⁴ The court found Congress considered what would happen if an email user left an opened email on the service provider’s server and decided another section of the statute governing electronic communications held “solely for the purpose of providing storage” would apply.⁹⁵ The court found it could not reconcile these two sections of the statute if it determined opened emails on a server were in “electronic storage.”

In *Lazette v. Mulmatycki*, the court disagreed with the *Theofel* reasoning. The court found the statutory definition of “electronic storage” is narrow:

E-mails which an intended recipient has opened may, when not deleted, be “stored,” in common parlance. But in light of the restriction of “storage” in § 2510(17)(B) solely for “backup protection,” e-mails which the intended recipient has opened, but not deleted (and thus which remain available for later re-opening) are not being kept “for the purposes of backup protection.”⁹⁶

The court further explained in light of the *Warshak* decision, the court of appeals for the Sixth Circuit would likely find opened, post-transmission emails are not in storage for “purposes of backup protection.”⁹⁷

In *Cruz Lopez v. Pena*, the plaintiff sued customs agents who detained the plaintiff, found his email login information in his wallet, and used the information to login to his email account and look at his emails.⁹⁸ The District Court for the Northern District of Texas applied qualified immunity to the plaintiff’s Stored Communications Act claim since it was “not clearly established” his previously opened, post-transmission emails were in “electronic storage” under the Act.⁹⁹ Citing *Theofel* and our court of appeals’ decision in *Fraser*, the court found “other courts are in

hot debate” over whether opened emails are in “electronic storage.”¹⁰⁰

We find no existing precedent places “beyond debate” the question of whether emails on an employer’s server are necessarily being stored for “purposes of backup protection” and thus are automatically in “electronic storage” and subject to the Act.¹⁰¹ An expert in communications technology may someday prove this point and obtain a robust consensus necessary to properly inform law enforcement. But we are faced with a complex computer storage issue far from settled.

Messrs. Coffey and Zimmerer requested Ms. Walker’s emails from Penn State and Penn State provided the emails. But they did not request emails stored for “purposes of backup protection.” If we deny Messrs. Coffey and Zimmerer qualified immunity, we would find law enforcement officers seeking to obtain emails on a non-public electronic communications service provider’s server presume every email sought is stored for “purposes of backup protection” and thus the Stored Communications Act governed their conduct. We cannot do so as there is no law clearly establishing this. The law is even unclear regarding what emails are in storage for purposes of backup protection. The courts in cases Ms. Walker cited acknowledge the law regarding whether emails are stored for “purposes of backup protection” is in debate. We cannot say the law is clearly established Messrs. Coffey and Zimmerer violated Ms. Walker’s rights under the Stored Communications Act when they accessed emails from her Penn State employee email account.

While we acknowledge our court of appeals has suggested opened emails stored on a provider’s server are in “electronic storage,” we cannot rely on dicta in our court of appeals’ decision to find the right clearly established. While Ms. Walker cited district court cases in our district, this is insufficient to show a “clearly established” right. As the cases cited demonstrate, we find the issue of whether emails are in “electronic storage” under the Act in debate.¹⁰² Messrs. Coffey and Zimmerer are entitled to qualified immunity because Ms. Walker has failed to show

Messrs. Coffey and Zimmerer violated clearly established law under the Act when they obtained her emails from Penn State.

2. Ms. Walker fails to show it was “clearly established” Messrs. Coffey and Zimmerer were required to obtain a warrant or valid subpoena under Section 2703.

Ms. Walker argues Messrs. Coffey and Zimmerer violated Section 2703 because they did not comply with its procedures, which include obtaining a warrant to access emails in electronic storage for less than 180 days.¹⁰³ At oral argument, counsel for Ms. Walker argued the government must always comply with these procedures when it seeks disclosure under Section 2703. Ms. Walker essentially argues the government cannot obtain emails under Section 2703 through consent; whenever law enforcement officers seek production of emails from an email service provider, Ms. Walker argues, those officers must comply with Section 2703. We cannot find this proposed blanket rule is “clearly established” law.

We found Penn State voluntarily authorized production of Ms. Walker’s emails. While Penn State initially demanded a subpoena, it later voluntarily authorized production of Ms. Walker’s emails. We cannot say the law is “clearly established” Messrs. Coffey and Zimmerer must obtain a warrant or valid subpoena under Section 2703 with this set of facts. Ms. Walker cites no caselaw from the Supreme Court or our court of appeals establishing this proposition.

At oral argument, counsel for Miss Walker cited *Freedman v. America Online, Inc.*, to support its claim the law is “clearly established” the government must follow the “specific legal processes” listed in Section 2703 when seeking electronic communications.¹⁰⁴ In *Freedman*, the district court for the District of Connecticut found two police officers violated the Act when they used an invalid warrant to obtain the plaintiff’s subscriber information from his internet service provider. The information included his “name, address, phone numbers, account status,

membership information, software information, billing and account information, and his other AOL screen names.”¹⁰⁵ In *Freedman*, the officers sought subscriber information, not emails. While the facts are somewhat similar to our case, we cannot find this district court case outside our circuit clearly establishes the government must obtain a warrant under Section 2703 to obtain emails from a service provider’s server, especially when the employer witness voluntarily produces information to which the employee does not enjoy an expectation of privacy.

Qualified immunity also protects Messrs. Coffey and Zimmerer from liability for Ms. Walker’s claims under Section 2703 of the Stored Communications Act since the law is not “clearly established” law enforcement officers must always obtain a warrant or valid subpoena to access emails from an electronic communications service provider’s server.

III. Conclusion

We grant Messrs. Coffey and Zimmerer’s motion to dismiss Ms. Walker’s Second Amended Complaint in the accompanying Order.

¹ Second Amended Complaint (ECF Doc. No. 29 ¶ 1).

² *Id.* at ¶ 15.

³ *Id.* at ¶ 1.

⁴ *Id.* at ¶¶ 6-7.

⁵ *Id.* at ¶ 10.

⁶ *Id.* at ¶¶ 8-9.

⁷ *Id.* at ¶ 12.

⁸ *Id.* at ¶¶ 25-26.

⁹ *Id.* at ¶ 32.

¹⁰ *Id.* at ¶ 34.

¹¹ *Id.* at ¶ 35.

¹² *Id.* at ¶ 31.

¹³ *Id.* at ¶ 28.

¹⁴ *Id.* at ¶¶ 28, 39; Ex. B.

¹⁵ *Id.* at ¶ 42.

¹⁶ ECF Doc. No. 5.

¹⁷ ECF Doc. No. 21.

¹⁸ ECF Doc. No. 22 (motion); ECF Doc. No. 22-2 (proposed Second Amended Complaint).

¹⁹ ECF Doc. No. 23.

²⁰ *Walker v. Coffey*, 905 F.3d 138, 150 (3d Cir. 2018).

²¹ *Id.*

²² ECF Doc. No. 30.

²³ When considering a motion to dismiss “[w]e accept as true all allegations in the plaintiff’s complaint as well as all reasonable inferences that can be drawn from them, and we construe them in a light most favorable to the non-movant.” *Tatis v. Allied Interstate, LLC*, 882 F.3d 422, 426 (3d Cir. 2018) (quoting *Sheridan v. NGK Metals Corp.*, 609 F.3d 239, 262 n.27 (3d Cir. 2010)). To survive dismissal, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Twombly*, 550 U.S. at 556). Our Court of Appeals requires us to apply a three-step analysis under a 12(b)(6) motion: (1) “it must ‘tak[e] note of the elements [the] plaintiff must plead to state a claim;” (2) “it should identify allegations that, ‘because they are no more than conclusions, are not entitled to the assumption of truth;” and, (3) “[w]hen there are well-pleaded factual allegations, [the] court should assume their veracity and then determine whether they plausibly give rise to an entitlement for relief.” *Connelly v. Lane Constr. Corp.*, 809 F.3d 780, 787 (3d Cir. 2016) (quoting *Iqbal*, 556 U.S. at 675, 679).

²⁴ 18 U.S.C. § 2701(a).

²⁵ *Id.* at § 2701(c).

²⁶ *Id.*

²⁷ *Walker*, 905 F.3d at 149.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ Neither party cited, and we cannot independently find, authority showing the consent standard under the Stored Communications Act is different than the consent standard under the Fourth Amendment.

³² 18 U.S.C. § 2703(a).

³³ *Id.* at § 2703(b).

³⁴ See *Fernandez v. California*, 571 U.S. 292, 298 (2014) (explaining consent is a long-recognized exception in Fourth Amendment doctrine); *United States v. Amon*, 669 F.2d 1351, 1358 (10th Cir. 1981) (explaining parties could not claim an expectation of privacy in documents voluntarily submitted to the government).

³⁵ *Berry v. Funk*, 146 F.3d 1003, 1013 (D.C. Cir. 1998).

³⁶ *Id.*

³⁷ *Id.*

³⁸ *John K. Maciver Inst. for Pub. Policy, Inc. v. Schmitz*, 885 F.3d 1004 (7th Cir. 2018).

³⁹ *Id.* at 1015.

⁴⁰ *Id.*

⁴¹ *Blake v. Wright*, 179 F.3d 1003, 1013 (6th Cir. 1999).

⁴² *Id.* at 1012.

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Tapley v. Collins*, 211 F.3d 1210, 1212-13 (11th Cir. 2000).

⁴⁶ *Id.* at 1216.

⁴⁷ *Id.* at 1215.

⁴⁸ *Id.* at 1214 (citing *Buckley v. Fitzsimmons*, 509 U.S. 259, 268 (1993)).

⁴⁹ *Id.* at 1215 (citing *Hunter v. Bryant*, 502 U.S. 224, 227 (1991) (“[B]ecause the entitlement is an immunity from suit rather than a mere defense to liability, we repeatedly have stressed the importance of resolving immunity questions at the earliest possible stage in litigation.”)).

⁵⁰ *Diana v. Oliphant*, 441 F. App’x 76 (3d Cir. 2011).

⁵¹ *Id.* at 80.

⁵² *Cruz Lopez v. Pena*, No. 12-165, 2013 WL 2250127, at *2 (N.D. Tex. May 22, 2013).

⁵³ *Id.* at *2-3.

⁵⁴ *Buckley*, 509 U.S. at 268 (explaining qualified immunity was so well established when Congress passed § 1983 in 1871 “that we presume that Congress would have specifically so provided had it wished to abolish” qualified immunity).

⁵⁵ *Harlow v. Fitzgerald*, 457 U.S. 800, 807 (1982).

⁵⁶ At oral argument, counsel for Ms. Walker argued *Hepting v. AT & T Corp.* is persuasive. 439 F. Supp. 2d 974 (N.D. Cal. 2006). The court found qualified immunity inappropriate when Congress enacts a statute with “comprehensive, free-standing liability schemes, complete with statutory defenses.” *Id.* at 1009. We do not find this argument persuasive. As qualified immunity is an old doctrine, Congress was aware of the doctrine when it passed the Stored Communications Act. We cannot say because Congress passed the Act with a statutory defense it meant to abrogate a well-established judicial doctrine.

⁵⁷ *L.R. v. Sch. Dist. of Philadelphia*, 836 F.3d 235, 241 (3d Cir. 2016) (quoting *Pearson v. Callahan*, 555 U.S. 223, 232 (2009)).

⁵⁸ *Leveto v. Lapina*, 258 F.3d 156, 161 (3d Cir. 2001).

⁵⁹ *Mammaro v. New Jersey Div. of Child Prot. & Permanency*, 814 F.3d 164, 169 (3d Cir.), *as amended* (Mar. 21, 2016).

⁶⁰ *Barna v. Bd. of Sch. Directors of Panther Valley Sch. Dist.*, 877 F.3d 136, 142 (quoting *Taylor v. Barkes*, 135 S. Ct. 2042, 2044 (2015)).

⁶¹ *Mammaro*, 814 F.3d at 169.

⁶² *Barna*, 877 F.3d at 142 (quoting *Ashcroft v. al-Kidd*, 563 U.S. 731, 741 (2011)).

⁶³ 18 U.S.C. § 2510(17).

⁶⁴ *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001), *aff'd in part, vacated in part, remanded*, 352 F.3d 107 (3d Cir. 2003), *as amended* (Jan. 20, 2004).

⁶⁵ *Id.* at 633-34.

⁶⁶ *Id.* at 636.

⁶⁷ *Id.*

⁶⁸ *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003), *as amended* (Jan. 20, 2004).

⁶⁹ *Id.* at 115 (citing 18 U.S.C. § 2701(c)) (finding no liability since the service provider also performed the search of the emails).

⁷⁰ *Bansal v. Russ*, 513 F. Supp. 2d 264 (E.D. Pa. 2007).

⁷¹ *Id.* at 271.

⁷² *Id.* at 276.

⁷³ *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331 (E.D. Pa. 2013); *Strategic Wealth Grp., LLC v. Canno*, No. 10-0321, 2011 WL 346592 (E.D. Pa. Feb. 4, 2011); *Integrated Waste Sols., Inc. v. Goverdhanam*, No. 10-2155, 2010 WL 4910176 (E.D. Pa. Nov. 30, 2010); *Markert v. Becker Tech. Staffing, Inc.*, No. 09-5774, 2010 WL 1856057 (E.D. Pa. May 7, 2010).

⁷⁴ *Markert*, 2010 WL 1856057, at *6.

⁷⁵ *Id.*

⁷⁶ *Brooks*, 954 F. Supp. 2d at 337.

⁷⁷ *Integrated Waste*, 2010 WL 4910176, at *7.

⁷⁸ *Strategic Wealth*, 2011 WL 346592, at *4.

⁷⁹ *Id.*

⁸⁰ *Theofel v. Farey-Jones*, 359 F.3d 1066, 1071 (9th Cir. 2004).

⁸¹ *Id.* at 1071-72.

⁸² *Id.* at 1072.

⁸³ *Id.* at 1075.

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Gonzales v. Uber Techs., Inc.*, No. 17-02264, 2018 WL 4616266, at *1 (N.D. Cal. Sept. 26, 2018).

⁸⁷ *Id.* at *5.

⁸⁸ *Id.* at *3.

⁸⁹ *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000 (N.D. Cal. 2018).

⁹⁰ *Id.* at 1044.

⁹¹ *United States v. Warshak*, 631 F.3d 266, 291 (6th Cir. 2010) (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1217 (2004)).

⁹² Kerr, *supra* note 91, at 1217 n.61.

⁹³ *Id.*

⁹⁴ *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009).

⁹⁵ *Id.*

⁹⁶ *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013).

⁹⁷ *Id.* at 758 n.13 (“[T]hat the Sixth Circuit would follow *Theofel* and extend SCA protection to opened but undeleted e-mails is doubtful.”).

⁹⁸ *Cruz Lopez v. Pena*, No. 12-165, 2013 WL 819373, at *4 (N.D. Tex. Mar. 5, 2013).

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Barna*, 877 F.3d at 142 (quoting *Ashcroft*, 563 U.S. at 741).

¹⁰² At oral argument, Ms. Walker’s counsel argued the state of the law need only give Messrs. Coffey and Zimmerer “fair warning” their conduct violated her rights. *Kane v. Barger*, 902 F.3d 185, 195 (3d Cir. 2018). In *Kane*, a police officer inappropriately touched and photographed a victim of sexual assault while purportedly interviewing her about the assault. The plaintiff alleged the officer violated her Fourteenth Amendment right to bodily integrity by touching and photographing her in violation of police policy. Our Court of Appeals found it “absurd” to analyze

whether the right to be free from a police officer's sexual assault was "clearly established" because the officer's actions clearly resembled a crime, specifically the crime of indecent assault under Pennsylvania law. We do not face a similar situation here. Ms. Walker has not alleged Messrs. Coffey and Zimmerer's actions resemble a crime. In the absence of such clearly criminal behavior of which there is a robust consensus, we find *Kane* inapplicable to requests for emails from a private employer.

¹⁰³ 18 U.S.C. § 2703(a).

¹⁰⁴ *Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121 (D. Conn. 2004).

¹⁰⁵ *Id.* at 123.