4-16-2020

Carol Walker v. Brian Coffey

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 19-1067

_____

CAROL LEE WALKER,
Appellant

v.

SENIOR DEPUTY BRIAN T. COFFEY, In His Individual Capacity;
SPECIAL AGENT PAUL ZIMMERER, In His Individual Capacity

_____

On Appeal from the United States District Court
for the Eastern District of Pennsylvania

(D.C. No. 2-17-cv-00040)

District Judge: Honorable Mark A. Kearney

_____

Argued September 12, 2019

Before: CHAGARES, JORDAN and RESTREPO,
Circuit Judges

(Opinion Filed: April 16, 2020)

Geoffrey Richard Johnson [ARGUED]
Stevens & Lee
1818 Market Street
29th Floor
Philadelphia, PA 19103

Counsel for Appellant

Claudia M. Tesoro [ARGUED]
Office of Attorney General of Pennsylvania
1600 Arch Street
Suite 300
Philadelphia, PA 19103

Counsel for Appellees

OPINION OF THE COURT

RESTREPO, *Circuit Judge*

Appellant Carol Lee Walker brought suit against a prosecutor and special agent from the Pennsylvania Office of the Attorney General (OAG) alleging they violated provisions of the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* (SCA), by inducing her employer, Pennsylvania State University (Penn State or University), to disclose her work emails with a facially invalid subpoena. Because the Appellees' actions, although improper, did not violate the SCA, we will affirm the dismissal of Walker's claims.

I.

In July 2015, the OAG brought charges of forgery and computer crimes against Walker in Pennsylvania state court. The charges arose from a criminal investigation involving Walker's husband and his trucking company. The OAG assigned Senior Deputy Attorney General Brian Coffey as the prosecutor and Special Agent Paul Zimmerer as the lead investigator to her case. Some charges against Walker were dropped after an August 2015 preliminary hearing, but four counts of conspiracy to commit forgery remained pending trial.

In October 2015, Coffey and Zimmerer requested that Penn State aid their investigation by producing Walker's emails from her employee account. Rather than disclose

Walker's emails, however, Penn State officials requested the government agents produce a subpoena. Coffey and Zimmerer obtained a subpoena form from the Centre County Court of Common Pleas but only partially completed the required fields. The subpoena listed the case caption, the intended recipient, and the request for "any & all emails/computer files/documents/attachments to or from Carol Lee Walker" at her Penn State email address. Missing from the subpoena was information regarding the date, time or place where the testimony or evidence would be produced, or which party was requesting the evidence. The OAG concedes that the subpoena was incomplete and therefore unenforceable.

On October 21, 2015, Zimmerer offered the facially invalid subpoena to Katherine Allen, Assistant General Counsel for Penn State. Allen thereafter instructed a Penn State employee to assist Zimmerer with the production of the requested emails. Sometime after the OAG obtained Walker's emails, the pending criminal charges against her were dismissed with prejudice.

Walker filed an action under 42 U.S.C. § 1983, alleging that Coffey and Zimmerer conducted an unreasonable search in violation of the Fourth Amendment by inducing Penn State to produce the emails with an invalid subpoena. The District Court granted the Appellees' motion to dismiss after concluding Coffey and Zimmerer were entitled to qualified immunity because Walker did not have a clearly established right to privacy in her work emails.

On appeal, a panel of this Court affirmed the District Court's dismissal on qualified immunity grounds. The panel held there was "no dispute" that the confiscated emails were sent or received by Walker's work e-mail address, and the emails themselves were a "part of an email system controlled and operated by Penn State." *Walker v. Coffey*, 905 F.3d 138, 149 (3d Cir. 2018). Because the "emails were subject to the common authority of [her] employer," Walker "did not enjoy any reasonable expectation of privacy vis-à-vis Penn State." *Id.* Thus, Fourth Amendment protection did not attach.

Given that Penn State exercised this dominion over its employees' electronic communications, the panel held that the University had the authority to produce Walker's work emails.

Significantly, the panel also concluded that Penn State acted through its attorney and produced the emails voluntarily, rather than under coercion resulting from the invalid subpoena. Rather than finding Coffey and Zimmerer "evade[d] the limitations of the Fourth Amendment by inducing [Penn State] to do what [it] cannot," the panel held that Penn State was a private party that exercised its "independent ability to consent to a search." *Id*. In reaching this conclusion, the panel emphasized that it did not condone Coffey and Zimmerer's improper use of an invalid subpoena. While noting the impropriety of the OAG's actions, it determined that under the circumstances—Penn State acting within its legal authority and through its own counsel—the University's compliance with the government's request for the emails was voluntary "despite the facial invalidity of the subpoena." *Id.* at 150.

Because Coffey and Zimmerer did not violate Walker's right to privacy, the panel agreed with the District Court that they were entitled to qualified immunity and affirmed the dismissal of her § 1983 claim. However, it vacated the District Court's order denying Walker leave to file a second amended complaint to address a new claim under the SCA. *Id.* at 150-51.

Walker filed an amended complaint alleging that Coffey and Zimmerer violated sections 2701(a), 2703(a) and 2703(b) of the SCA. In granting the Appellees' motion to dismiss, the District Court found that Walker had not alleged a violation. It further found that qualified immunity was available for claims raised under the SCA and that Coffey and Zimmerer were again entitled to immunity. The District Court reasoned that, even if an SCA violation had been alleged, qualified immunity would be appropriate because the applicable law was unclear when the emails were procured. Walker appeals the District Court's dismissal of her claim.

II.

The District Court exercised jurisdiction under 28 U.S.C. § 1331. We have jurisdiction under 28 U.S.C. § 1291 to review the District Court's order of dismissal. We exercise plenary review over a decision to dismiss claims under Federal Rule of Civil Procedure 12(b)(6). *In re Nickelodeon Consumer*

Privacy Litig., 827 F.3d 262, 271 (3d Cir. 2016). To survive a motion to dismiss, a plaintiff must allege "enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary element[s]" of a cause of action. *Phillips v. County of Allegheny*, 515 F.3d 224, 234 (3d Cir. 2008) (internal quotations omitted).

III.

This Court, in reviewing the dismissal of Walker's first complaint, held that it was not clearly established that the Fourth Amendment afforded her the right "to have the contents of her work emails remain free from a law enforcement search, absent a warrant or valid exception to the warrant requirement." *Walker*, 905 F.3d at 144. The primary question before us now is whether the SCA provided Walker with heightened privacy rights to her work emails and a cause of action resulting from the government's use of an invalid subpoena.

For the reasons that follow, we conclude that the SCA does not provide Walker with viable grounds for relief. The SCA is inapplicable because Penn State does not provide electronic communication services to the public, and the University acted within its rights as Walker's employer in voluntarily disclosing her work emails. Our holding is a narrow one: we are not deciding whether, if the invalid subpoena had induced Penn State to disclose Walker's emails, Coffey and Zimmer would have liability under the SCA. We hold only that, given the record before us, the dismissal of the claims was proper.

The Stored Communications Act is Title II of the Electronic Communications Privacy Act, codified at 18 U.S.C. §§ 2701 *et seq*. Passed by Congress in 1986, "the SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900 (9th Cir. 2008), *rev'd on other grounds sub nom. Ontario v. Quon*, 560 U.S. 746 (2010). Historically, the Fourth Amendment has not protected personal information revealed to third parties. *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 443 (1976) ("The Fourth Amendment does not prohibit the

obtaining of information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). Providers of electronic communications act as third parties that store and process their users' private files, meaning the provider-maintained files fall outside Fourth Amendment protection. Because most electronic communication providers serve the public but are themselves private actors, they could potentially search files held under their control and disclose their users' information to the government without violating the Fourth Amendment. *See* 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, 1210-11 (2004).

To address this vulnerability, Congress crafted the SCA to protect information held by centralized communication providers. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 147 (3d Cir. 2015). The SCA "creates a set of Fourth Amendment-like privacy protections by statute [by] regulating the relationship between government investigators and service providers in possession of users' private information." Kerr, *supra*, at 1212. It provides this enhanced privacy protection by limiting the government's ability to compel providers to disclose their users' information, 18 U.S.C. § 2703, and by limiting the providers' ability to disclose such information to the government, 18 U.S.C. § 2702.

In addition to enhancing privacy rights, the SCA also prohibits certain forms of electronic trespass. Whereas sections 2702 and 2703 set forth procedural rules for acquiring or disclosing a user's information, section 2701 prohibits intentionally accessing without authorization, or accessing beyond authorization, a service provider in order to obtain, alter, or prevent authorized access to an electronic communication. 18 U.S.C. § 2701(a). Unlike other sections of the SCA, liability for violating section 2701 could be damages or a fine and imprisonment, depending on the intention of the violator. While sections 2702 and 2703 regulate the information given to the government, section 2701 was "primarily designed to provide a cause of action against

computer hackers." *State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995).

Aside from the criminal prohibitions unique to section 2701, violators of the SCA face civil liability pursuant to section 2707. The section enables service providers, subscribers or any "other person aggrieved" to bring a civil action against anyone who knowingly and intentionally violates the SCA. 18 U.S.C. § 2707(a). Government entities are included in those potentially liable where it is established that their agents willfully violated the SCA's provisions. *Organizacion JD Ltda. v. U.S. Dep't of Justice*, 18 F.3d 91, 95 (2d Cir. 1994); 18 U.S.C. § 2707(d). A violation of the Act is not enough to satisfy the requirement for Article III standing; a plaintiff must allege the SCA violations caused a "sufficiently concrete and particularized" injury-in-fact in order to have standing to sue. *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019) (citing *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)). If a sufficiently particularized injury is alleged but the SCA is found not to apply, the plaintiff may have standing but no civil recourse. *See In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d at 273-74, 277.

It is in this context that we determine whether the District Court erred in finding that Coffey and Zimmerer did not violate sections 2701 or 2703 of the SCA. Walker claims the OAG officials violated section 2701(a) by gaining unauthorized access to Penn State's electronic communications through the use of an invalid subpoena. She claims they violated section 2703, either paragraph (a) or (b), by using the invalid subpoena to coerce Penn State to disclose her work emails. Because we conclude Penn State's consensual search of its own server and its voluntary disclosure of Walker's emails to the government did not violate the SCA, we affirm the District Court's dismissal of Walker's second amended complaint.

IV.

Section 2701 of the SCA creates liability for one who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to

access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a).

While the SCA does not define "facility," it does define "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1)). This Court has concluded that "facilities" under the SCA are network service providers, which include "telephone companies, internet or e-mail service providers, and bulletin board services." *In re Google Inc.*, 806 F.3d at 146 (quoting *Garcia v. City of Laredo*, 702 F.3d 788, 792 (5th Cir. 2012)). We agree with the District Court, therefore, that Penn State qualifies as a facility that provides electronic communication services to its employees under the terms of the SCA.

The question becomes, therefore, whether Coffey and Zimmerer intentionally "accessed" Penn State's server under the terms of section 2701. We conclude they did not.[1] The

---

[1] We are assuming here, without deciding, that sections 2701 and 2703 apply to the emails in question, though there is a serious argument that they do not. By their terms, those sections apply only to communications "in electronic storage[.]" *See* 18 U.S.C. §§ 2701(a), 2703(a). "Electronic storage" is a term of art under the SCA. A message can be in electronic storage in one of two ways – the "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof[,]" or the "storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]" *Id*. § 2510(17). The parties agree that the first definition is inapplicable here. Indeed, they must, because we have previously held that e-mails, once they have been read by the recipient, are no longer in temporary, intermediate storage. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003), *as amended* (Jan. 20, 2004) (holding that e-mails stored on a server were no longer in temporary, intermediate storage after they had been read by the recipient). Thus the only way that Walker's e-mails could be held to be in electronic storage is if they were being stored "for

SCA does not define "access," but a dictionary definition of the verb is "to get at" or "gain access to." *See United States v. Smith*, 155 F.3d 1051, 1058 n.13 (9th Cir. 1998) (citing *Webster's Ninth New Collegiate Dictionary* 49 (1986)) (noting that "access" as a verb "came into being in the so-called 'computer age'"). Accessing a facility as defined by section 2701 requires an intrusion into an electronic communication system. Even assuming Coffey and Zimmerer coerced Penn State's Assistant General Counsel with the invalid subpoena to acquire Walker's emails, they themselves did not gain access to Penn State's electronic communications facility. They instead only accessed Walker's emails, through the assistance of a Penn State employee.

Designed to prohibit "hacking" into electronic communication facilities, section 2701 does not cover nonintrusive procurements of electronic communications. Walker's argument encourages us to find that the OAG's use of the illegal subpoena rendered Penn State's search of its own facility unauthorized. But section 2701(c)(1) explicitly excepts from liability conduct authorized "by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1); *see Fraser*, 352 F.3d at 114-15 (noting

---

purposes of backup protection[.]" 18 U.S.C. § 2510(17). And that is where Walker might run into difficulty, since it is arguable that versions of already-read emails that are left on a service provider's server do not qualify as being stored for backup protection. *See Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 & n.13 (N.D. Ohio 2013) (concluding opened e-mails are not in storage for backup protection); *United States v. Weaver*, 636 F. Supp. 2d 769, 771-73 (C.D. Ill. July 15, 2009) (rejecting reasoning that opened emails on a service provider's server are covered by the SCA); *Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that accessing to opened e-mail did not violate the SCA). *But see Theofel v. Farley-Jones*, 359 F.3d 1066 (9th Cir. 2004) (stating that "[a]n obvious purpose for storing a message on an [internet service provider's] server after delivery is to provide a second copy of the message in the event that the user needs to download it again[,]" and so concluding that "[t]he ISP copy of the message functions as a 'backup' for the user."). We do not need to address this issue now and therefore do not.

the liability exception in section 2701(c)(1) extends to employers searching their own electronic communications server). Penn State's search of its own server to produce Walker's emails is not prohibited by section 2701, regardless of whether its counsel was induced by deceit or knowingly cooperative. Because no proscribed intrusion occurred in this instance, we deny the claim and turn to Walker's next ground for relief.[2]

V.

Walker argues the District Court erred in finding that Coffey and Zimmerer's use of the invalid subpoena did not violate section 2703, titled "Required disclosure of customer communications or records." Given the circumstances of Penn State's disclosure of her emails, we again agree with the District Court that this provision of the SCA does not provide Walker a viable cause of action.[3]

Section 2703 mandates that electronic communication providers disclose a user's information to the government if the

---

[2] Walker claims the disclosure of her emails to the OAG was contrary to Penn State's privacy policy, which recognized that she had an expectation of privacy in her emails. However, this argument again misinterprets the applicability of section 2701. Penn State had the authority to search and cull her work emails. In citing Penn State's privacy policy, Walker is "relying on a theory of unauthorized *disclosure* of information," not of one of unauthorized access, and disclosures are not covered by section 2701. *In re Am. Airlines, Inc. Privacy Litig.*, 370 F. Supp. 2d 552, 558-59 (N.D. Tex. 2005) ("Section 2701 does not proscribe unauthorized use or disclosure of information obtained from authorized access to a facility.").

[3] Although section 2703's title is "Required disclosure of customer communications or records," the section also addresses the disclosure of a *subscriber's* information. Walker subscribed to Penn State's email service as an employee.

government meets certain procedural requirements.[4] Walker argues Coffey and Zimmerer failed to abide by the

---

[4] The relevant parts of 18 U.S.C. § 2703(a) and (b) are as follows:

> **(a) Contents of wire or electronic communications in electronic storage**. 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[.] . . . 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.
>
> **(b) Contents of wire or electronic communications in a remote computing service.—**
>
> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant . . .; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

requirements when they used a facially invalid subpoena to obtain her emails. She acknowledges, however, that the District Court's ruling that Penn State consented to disclosing the emails independently of the illegal subpoena is fatal to her claim. Walker's argument on appeal, therefore, amounts to an attack on the District Court's conclusion that Penn State voluntarily "agreed to produce" her emails. App. 3.

Walker fails to recognize that this Court, in affirming the dismissal of her first complaint, also concluded that Penn State's Assistant General Counsel "instructed an employee in her office to assist with the production of [her] emails," choosing to cooperate "rather than contest the validity of the subpoena or otherwise limit any search." *Walker*, 905 F.3d at 149-50. Thus, we have previously decided the issue of whether Penn State acted voluntarily, and that decision is the law of the case. The law of the case doctrine dictates that "one panel of an appellate court generally will not reconsider questions that another panel has decided on a prior appeal in the same case." *In re City of Phila. Litig.*, 158 F.3d 711, 717 (3d Cir. 1998). The precept fosters "the finality and efficiency of the judicial process by protecting against the agitation of settled issues." *In re Cont'l. Airlines, Inc.*, 279 F.3d 226, 233-34 (3d Cir. 2002) (internal quotations omitted) (quoting *Christianson v. Colt Indus. Operating Corp.*, 486 U.S. 800, 816 (1988)). The law of the case governs our exercise of discretion; we can reconsider previously decided issues under "extraordinary circumstances," such as if new evidence becomes available, a supervening law has been introduced, or the prior decision was "clearly erroneous and would create manifest injustice." *In re City of Phila. Litig.*, 158 F.3d at 718 (citing *Pub. Interest Research Grp. of N.J., Inc. v. Magnesium Elektron, Inc.*, 123 F.3d 111, 116 (3d Cir. 1997)).

> (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[.]

Walker does not allege, much less establish, that extraordinary circumstances exist to justify reconsidering whether Penn State acted voluntarily in cooperating with the government agents. Because it is the law of the case that Penn State consented to disclosing Walker's emails, we conclude that she failed to allege a violation of section 2703.

Given that Penn State acted voluntarily, we note that the disclosure of Walker's emails is governed by section 2702 of the SCA, aptly titled "Voluntary disclosure of customer communications or records."[5] Section 2702 requires electronic communication service providers to keep communications confidential unless a court order, warrant, or subpoena is produced. However, these restrictions apply only to providers offering services "*to the public*." 18 U.S.C. § 2702(a)(1) (emphasis added). Penn State offers electronic communication services to its employees, not to the community at large. Walker's work emails, therefore, fall outside of the scope of the SCA's protection. *See, e.g.*, *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (holding that contract employer did not provide electronic communication services to the public and therefore could not be sued under the SCA for divulging emails from its server to third parties). Because the Act did not restrict Penn State from voluntarily providing Coffey and Zimmerer with the requested emails from its server, we will affirm the District Court's finding that Walker failed to state a cause of action under the SCA.

---

[5] 18 U.S.C. § 2702 provides in relevant part:

> (a) Prohibitions.--Except as provided in subsection (b) or (c)--
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service[.]

VI.

In light of our holding that no violation of the SCA occurred, we need not reach the issue of whether Coffey and Zimmerer are entitled to qualified immunity. We decline to review the holding of the District Court because such a decision is not necessary to resolve the case. We join the prior panel of this Court in condemning the OAG's use of an invalid subpoena to obtain evidence and similarly emphasize that our holding denying Walker relief should not be interpreted as excusing its failure to prepare an enforceable subpoena. *Walker*, 905 F.3d at 150 ("We emphasize that nothing in this opinion should be taken as condoning the actions of Appellees in this case.").

For the foregoing reasons, we hold that the Appellees cannot be found liable under the Stored Communications Act and will therefore affirm the District Court's dismissal of Walker's second amended complaint.