9-20-2018

Carol Walker v. Brian Coffey

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 17-2172

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. Civil Action No. 2-17-cv-00040)
District Judge: Honorable Mark A. Kearney

Argued on January 8, 2018

Before: JORDAN, ROTH, Circuit Judges and STEARNS*, District Judge

(Opinion filed: September 20, 2018)

Geoffrey R. Johnson, Esq. (**ARGUED**)
1110 Wellington Road
Jenkintown, PA 19046

Counsel for Appellant

John G. Knorr, III, Esq. (**ARGUED**)
J. Bart DeLone, Esq.
Office of Attorney General of Pennsylvania
Strawberry Square
15th Floor
Harrisburg, PA 17120

Counsel for Appellees

OPINION

ROTH, Circuit Judge

---

* The Honorable Richard G. Stearns, District Judge of the Massachusetts District Court, sitting by designation

Appellant Carol Lee Walker commenced this action under 42 U.S.C. § 1983. She alleges that Appellees—a prosecutor and a special agent employed by the Pennsylvania Office of the Attorney General (OAG)—violated her Fourth Amendment right to be free from an unreasonable search when they used an invalid subpoena to induce Walker's employer, Pennsylvania State University (Penn State), to produce her work emails. The District Court granted Appellees' motion to dismiss, concluding that they were entitled to qualified immunity because Walker did not have a clearly established right to privacy in the content of her work emails. For the reasons stated below, we will affirm the dismissal of Walker's § 1983 claim. We will vacate the District Court's denial of Walker's subsequent motion for leave to file a second amended complaint, asserting claims under the Stored Communications Act (SCA),[1] and remand for further proceedings consistent with this opinion.

I.

This case stems from a criminal prosecution brought against Walker by the OAG. In July 2015, the OAG filed criminal charges against Walker in state court, which included numerous counts of forgery and various computer crime offenses. These charges were joined with prior charges that had been filed against Walker's husband, Ray Allen Walker, Jr., and his trucking company. Appellee Brian Coffey, a senior deputy attorney general, was the prosecutor assigned to the case, and Appellee Paul Zimmerer, an OAG

[1] 18 U.S.C. § 2701 *et seq*. Throughout her filings, Walker sometimes erroneously refers to the SCA as the "Secured" Communications Act.

special agent, served as the lead investigator. Following a preliminary hearing in August 2015, some of the charges against Walker were dismissed, but four counts of conspiracy to commit forgery remained pending.

In October 2015, before her trial had been scheduled, Coffey and Zimmerer sought to obtain Walker's work emails from her employer, Penn State, as part of their investigation. Coffey and Zimmerer initially asked Penn State to produce Walker's work emails voluntarily, but Penn State officials requested formal documentation, saying, "We just need something formal, a subpoena."[2] Coffey and Zimmerer then obtained a blank subpoena form from the Centre County Court of Common Pleas, which they filled out in part. The subpoena includes the case caption, is addressed to "John Corro, PSU General Counsel & Senior Security / Systems Analyst," and requests production of "any & all emails/computer files/documents/attachments to or from Carol Lee Walker at her email address, to or from the following email addresses: . . .."[3] The seven listed email addresses appear to belong to either Walker's husband or his business. The subpoena is blank as to the date, time, and place of production and the party on behalf of whom testimony is required. As such, Appellees concede that the subpoena was, on its face, incomplete and unenforceable. On October 21, 2015, Zimmerer presented the unenforceable subpoena to Katherine Allen, Assistant General Counsel at Penn State. Under Allen's direction, Penn State employees searched for the requested emails and turned them over to Zimmerer. At some point after Penn State produced the

[2] App. at 150-51.
[3] App. at 49.

emails, the remaining criminal charges against Walker were dismissed with prejudice, *nolle prosequi*.

Walker then filed this § 1983 action against Zimmerer and Coffey, alleging that their use of an invalid subpoena to obtain Walker's work emails violated her right to be free from unreasonable search under the Fourth Amendment of the U.S. Constitution.[4] Zimmerer and Coffey both moved to dismiss, arguing, in part, that they were entitled to qualified immunity because Walker did not have a reasonable expectation of privacy in her work emails or, if she did, that right was not clearly established.

The District Court granted the motion to dismiss, agreeing that Zimmerer and Coffey were entitled to qualified immunity. The court concluded that Walker could not show a clearly established right to privacy in the content of her work emails.[5] Following the dismissal of her case, Walker filed a motion for reconsideration of the District Court's ruling and for leave to file a second amended complaint. Walker's proposed second amended complaint was filed as an attachment to her motion. The proposed complaint included a new claim for violation of the SCA and pleaded additional

---

[4] Walker's complaint also alleged a violation of Article I, section 8 of the Pennsylvania Constitution. The District Court dismissed this claim on the grounds that Pennsylvania law does not provide a private right of action allowing plaintiffs to seek money damages for violations of the Pennsylvania Constitution. App. at 20. Walker does not challenge that ruling on appeal.

[5] *Walker v. Coffey*, No. 17-40, 2017 WL 1477144, at *6-*9 (E.D. Pa. Apr. 24, 2017).

facts regarding Penn State's role as both Walker's employer and Walker's internet service provider (ISP), the measures Walker took to protect the privacy of her work email account, and the Penn State internet privacy policy applicable at the time of the search. In a short memorandum order, the District Court denied Walker's motion. Ignoring the SCA claim, the court simply concluded that, even if it were to allow Walker to file her proposed second amended complaint, the additional factual allegations therein would not alter the court's prior conclusion that the Defendants were entitled to qualified immunity.

Walker now appeals both the District Court's dismissal of her complaint on qualified immunity grounds and the District Court's denial of her motion for reconsideration and leave to file a second amended complaint.

II.

The District Court exercised subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1343. We have appellate jurisdiction over the District Court's final orders pursuant to 28 U.S.C. § 1291.

"We review a motion to dismiss based on the defense of qualified immunity *de novo* as it involves a pure question of law."[6] We review a district court's denial of a motion for

[6] *McLaughlin v. Watson*, 271 F.3d 566, 570 (3d Cir. 2001).

reconsideration and denial of leave to amend for abuse of discretion.[7]

III.

A.

"Qualified immunity shields government officials from civil damages liability unless the official violated a statutory or constitutional right that was clearly established at the time of the challenged conduct."[8] Qualified immunity is a strong shield and protects "all but the plainly incompetent or those who knowingly violate the law."[9] "To resolve a claim of qualified immunity, courts engage in a two-pronged inquiry: (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."[10] A court may address either of these questions first, "in light of the circumstances in the particular case at hand,"[11] and the Supreme Court has "repeatedly . . . stressed the importance of

[7] *Budhun v. Reading Hosp. & Med. Ctr.*, 765 F.3d 245, 259 (3d Cir. 2014); *Caver v. City of Trenton*, 420 F.3d 243, 258 (3d Cir. 2005).

[8] *Taylor v. Barkes*, 135 S. Ct. 2042, 2044 (2015) (internal quotation marks omitted).

[9] *Mullenix v. Luna*, 136 S. Ct. 305, 308 (2015) (internal quotation marks omitted).

[10] *L.R. v. Sch. Dist. of Phila.*, 836 F.3d 235, 241 (3d Cir. 2016).

[11] *Pearson v. Callahan*, 555 U.S. 223, 236 (2009).

resolving qualified immunity questions at the earliest possible stage in litigation."[12]

When considering whether a right is clearly established for purposes of qualified immunity, a court must, as a threshold matter, identify the scope of the right at issue. The Supreme Court has emphasized that, for purposes of this inquiry, a court must define or identify the right at a particularized level.[13] "A Government official's conduct violates clearly established law when, at the time of the challenged conduct, '[t]he contours of [a] right [are] sufficiently clear' that every 'reasonable official would have understood that what he is doing violates that right.'"[14] Although the Supreme Court "do[es] not require a case directly on point, . . . existing precedent must have placed the statutory or constitutional question beyond debate."[15] A plaintiff must identify either "controlling authority in the[] jurisdiction" or a "consensus of cases of persuasive authority."[16]

B.

Consistent with the Supreme Court's precedent, we begin our analysis by identifying the constitutional right at

---

[12] *Id*. at 232 (quoting *Hunter v. Bryant*, 502 U.S. 224, 227 (1991) (*per curiam*)).
[13] *See, e.g.*, *Anderson v. Creighton*, 483 U.S. 635, 640 (1987).
[14] *Ashcroft v. al-Kidd*, 563 U.S. 731, 741 (2011) (quoting *Anderson*, 483 U.S. at 640).
[15] *Id*.
[16] *Wilson v. Layne*, 526 U.S. 603, 617 (1999).

issue, as "particularized to the facts of the case."[17] Thus, for purposes of qualified immunity, we must consider, at a minimum, whether it is clearly established that the Fourth Amendment affords an employee, such as Walker, 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. Because we conclude that such a right is not clearly established—especially where, as here, the employer ultimately produces the emails to law enforcement—we hold that Appellees are entitled to qualified immunity.

1.

"The touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'"[18] Courts answer this question through a two-part test, examining both subjective and objective expectations of privacy. First, a court considers whether an individual has "manifested a subjective expectation of privacy in the object of the challenged search."[19] Second, a court considers whether "society [is] willing to recognize that expectation as reasonable."[20]

---

[17] *White v. Pauly*, 137 S. Ct. 548, 552 (2017) (*per curiam*).

[18] *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

[19] *Id*.

[20] *Id.*; *see also United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (noting that a "search," for Fourth Amendment purposes, "occurs when an expectation of privacy that society is prepared to consider reasonable is infringed").

Throughout this litigation, Walker's subjective expectation of privacy in her work emails has not been contested. Thus, our analysis focuses on whether Walker enjoyed an objectively reasonable expectation of privacy in the content of her work emails.

When conducting such analysis, the Supreme Court has historically expressed sensitivity to advances in technology,[21] though in recent years the Court has also exercised caution in this area.[22] In addition, although the Fourth Amendment "protects people not places,"[23] the caselaw consistently recognizes that objective expectations of privacy in the workplace are distinct from those in other contexts.[24] In analyzing Walker's claim, we are therefore mindful of this delicate balance.

The Supreme Court's early decisions addressing the Fourth Amendment's application to telephone calls provide our initial foundation. In *United States v. Katz*, the Court first

---

[21] *See, e.g.*, *Katz*, 389 U.S. at 352 (holding that failure to recognize a reasonable expectation of privacy in a telephone booth would "ignore the vital role that the public telephone has come to play in private communication").

[22] *See City of Ontario v. Quon*, 560 U.S. 746, 759 (2010) ("The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . .. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

[23] *Katz*, 389 U.S. at 351.

[24] *See, e.g.*, *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968).

recognized a reasonable expectation of privacy in the content of a telephone call made from a public phone booth.[25] The Court concluded that the government's use of an electronic listening device to record the call constituted a search that, absent a warrant or valid exception to the warrant requirement, violated the Fourth Amendment.[26] Next, in *Smith v. Maryland*, the Court addressed the government's use of a pen register to record the number dialed from an individual's home telephone.[27] After reaffirming *Katz*'s holding that the content of a phone call is protected by the Fourth Amendment, the Court concluded that telephone users do not have a legitimate expectation of privacy in the numbers that they dial.[28] Whereas the holding of *Katz* reflected widely-held expectations that the words spoken into the mouthpiece of a phone will remain private, the *Smith* Court reasoned that no such expectation existed for the numbers a user dials, because the numbers, unlike the content of the calls, are voluntarily turned over to the phone company.[29]

The core holding of *Smith* rested upon the established rule that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[30] This principle—the third-party doctrine—has arisen in a variety of contexts. With regard to communications, the third-party doctrine often dictates distinct treatment for the content of

---

[25] *Katz*, 389 U.S. at 351-52.
[26] *Id*.
[27] *Smith*, 442 U.S. at 737.
[28] *Id*. at 743.
[29] *Id*. at 742-44.
[30] *Id*. at 743-44.

communications as opposed to surface-level identifying information or metadata. Notably, the rules established for telephone calls in *Katz* and *Smith* align with prior and subsequent Supreme Court caselaw applying the Fourth Amendment to physical mail: Senders enjoy a reasonable expectation of privacy in the content of their letters and packages, but not in information readily discernable from the surface of a mailed item, such as the address.[31]

Content, however, is not categorically protected; content that is turned over to a third party is not subject to a reasonable expectation of privacy. *Smith* drew upon the Court's prior decision in *United States v. Miller*, which addressed an account holder's reasonable expectation of privacy in checks and bank records.[32] The *Miller* Court concluded that because the documents "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," the account holder had "no legitimate 'expectation of privacy' in their contents."[33]

---

[31] *See, e.g.*, *Jacobsen*, 466 U.S. at 114 ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

[32] *United States v. Miller*, 425 U.S. 435, 438-39 (1976).

[33] *Id*. at 442.

As technology has advanced, courts have grappled with defining objective expectations of privacy in the content of electronic communications. And those expectations can be even harder to define in the workplace context. *City of Ontario v. Quon* posed the question whether a police officer enjoyed a reasonable expectation of privacy in the content of text messages sent from his City-issued pager.[34] The Supreme Court declined to resolve the question definitively. Instead, after noting the risk of "elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear,"[35] the Court assumed *arguendo* that "Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City" and that a search had occurred for purposes of the Fourth Amendment.[36] The Court nevertheless concluded that the search was reasonable because, pursuant to an established Fourth Amendment exception, it was conducted by Quon's employer for a legitimate work-related purpose.[37]

Only months after *Quon* was decided, the Eleventh Circuit, in *Rehberg v. Paulk*,[38] confronted a set of facts similar to those of our present case. The defendants in that case—a state prosecutor and law enforcement investigator—had been investigating Rehberg and issued an allegedly defective subpoena to Rehberg's ISP in order to obtain emails

---

[34] 560 U.S. 746, 750 (2010).
[35] *Id*. at 759.
[36] *Id*. at 760.
[37] *Id*. at 764-65.
[38] 611 F.3d 828 (11th Cir. 2010).

sent and received from Rehberg's personal computer.[39] Rehberg later filed a § 1983 action alleging, among other claims, that the subpoena violated his Fourth Amendment rights. After noting the paucity of caselaw addressing Fourth Amendment protection of email content and the "marked lack of clarity in what privacy expectations as to content of electronic communications are reasonable,"[40] the Eleventh Circuit, relying on *Quon*, concluded that the case presented "'far-reaching' legal issues that [the court] should be cautious about resolving too broadly."[41] Rather than attempting to resolve those issues, the Eleventh Circuit simply concluded that a right to privacy in the content of email communications was not clearly established.[42] Notably, the Eleventh Circuit acknowledged the apparent relevance of the Supreme Court's precedents governing telephone communications, but found those cases were not dispositive. As the court explained, "The Supreme Court's decisions in *Katz* and *Smith* clearly established an objectively reasonable privacy right in telephone conversation content, but, as the modern Internet did not exist at the time of those decisions, whether the analytical framework, much less the rationale, of those decisions transfers to privacy rights in Internet email is questionable and far from clearly established."[43]

Several months later, the Sixth Circuit took a different approach in *United States v. Warshak*.[44] In *Warshak*, law

---

[39] *Id*. at 835.
[40] *Id*. at 843-44.
[41] *Id*. at 846.
[42] *Id*. at 847.
[43] *Id*.
[44] 631 F.3d 266 (6th Cir. 2010).

enforcement agents, relying on section 2703(b) of the SCA,[45] had obtained a subpoena compelling Warshak's ISP to produce the contents of approximately 27,000 emails sent or received from Warshak's account. Warshak moved to suppress, arguing that the government's warrantless search and seizure of his emails violated his Fourth Amendment rights.[46] After reviewing the case law discussed above, the Sixth Circuit concluded that, "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[47] The court found that an ISP is "the functional equivalent of a post office or telephone company," and, as a result, "the government cannot compel a commercial ISP to turn over the contents of email without triggering the Fourth Amendment."[48] Addressing the potential applicability of the third-party doctrine, the Sixth Circuit, drawing on *Katz* and *Smith*, held that the "mere *ability*" of an ISP to access the content of emails is not "sufficient to extinguish a reasonable expectation of privacy."[49] The Sixth Circuit distinguished *Miller* on the grounds that Warshak's ISP, unlike the bank in *Miller*, was an intermediary rather than the intended recipient of the material in question.

Walker argues, in short, that *Warshak* should carry the day. She characterizes the Sixth Circuit's decision as a straightforward and modest application of the Supreme

---

[45] 18 U.S.C. § 2703(b).
[46] *Warshak*, 631 F.3d at 282.
[47] *Id*. at 285-86.
[48] *Id*. at 286.
[49] *Id*. at 286-87.

Court's precedents on mail and telephone communications to the field of electronic communications. But Walker has failed to identify, nor can we, a "robust consensus of cases of persuasive authority"[50] supporting the position she advances. To the contrary, at present *Warshak* remains closer to a lonely outlier than to a representation of consensus. Although *Warshak* arguably tracks a longstanding distinction in Fourth Amendment law between content and metadata, that distinction is not dispositive, as content is not uniformly protected.[51] As *Quon* and *Rehberg* recognized, electronic communications present new considerations, and perhaps distinguishing features, that may counsel caution rather than a rote application of older precedents addressing other forms of communication. Moreover, the Fourth Amendment issues in *Warshak* arose in the context of suppression of evidence. Thus, the Sixth Circuit did not face the question that we must answer: whether the particular Fourth Amendment right was clearly established.

As such, we would be hard put to find that Walker enjoyed a clearly established right to privacy in the content of her work emails. But because this case involves Walker's *work* emails, which were produced to law enforcement by her employer, Penn State, our inquiry does not end there. As explained below, those facts remove any doubt that Walker has failed to allege a violation of a clearly established constitutional right.

2.

---

[50] *L.R. v. Sch. Dist. of Phila.*, 836 F.3d at 248 (internal quotation marks omitted).

[51] *See, e.g.*, *Miller*, 425 U.S. at 442.

Most of the cases discussed above address the reasonable expectation of privacy in *personal* communications. Here, it is undisputed that the communications in question were sent or received from Walker's work email account. And although the Fourth Amendment affords employees a reasonable expectation of privacy in the content of certain work-related communications and files, an employee's Fourth Amendment rights in the workplace are subject to additional exceptions and limitations.

The Supreme Court has recognized that employees may be entitled to a reasonable expectation of privacy in the contents of documents stored in the workplace, both in the private[52] and public[53] sectors. At the same time, public employers remain free to conduct a warrantless search of an employee's files or communications if the search is "conducted for a 'noninvestigatory, work-related purpos[e]' or for the 'investigatio[n] of work-related misconduct.'"[54] This rule is consistent with the nature of an employer-employee relationship and reflects an understanding that, although employees may have certain privacy interests in their work-related documents and communications vis-à-vis outsiders, their privacy interests vis-à-vis their employer are far more circumscribed.

---

[52] *Mancusi v. DeForte*, 392 U.S. 364, 368-70 (1968).

[53] *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (extending the holding of *Mancusi* to public sector employees).

[54] *Quon*, 560 U.S. at 761 (quoting *O'Connor*, 480 U.S. at 725-26).

In a similar vein, courts have long recognized that employers, as third parties who possess common authority over the workplace, may independently consent to a search of an employee's workplace documents or communications.[55] This rule is a logical application, in the workplace context, of general principles governing third-party consent. An individual or entity exercising common authority over the place or thing to be searched may independently consent to a search.[56]

More recently, the Ninth Circuit addressed the application of this principle to modern workplace technology. *United States v. Ziegler*[57] involved an investigation into an employee who, law enforcement believed, had been accessing child pornography on his work computer. Following several conversations with an FBI agent, employees from the company's IT department made a copy of the suspect-employee's hard drive and produced it to the FBI. After finding, pursuant to *Mancusi* and *O'Connor*, that the suspect-employee enjoyed a reasonable expectation of privacy in the

---

[55] *See, e.g.*, *Mancusi*, 392 U.S. at 369 (holding that an employee could reasonably have expected that documents stored in a shared office "would not be touched except with the[] permission [of co-occupants of the office] or that of [workplace supervisors]").

[56] *See, e.g.*, *United States v. Matlock*, 415 U.S. 164, 171 (1974) (holding that the government "may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected").

[57] 474 F.3d 1184 (9th Cir. 2007).

contents of his work computer, the Ninth Circuit nevertheless concluded that the search of the computer was permissible because the FBI had obtained consent from the employer, who exercised common authority over the workplace computer at issue.[58]

We reach the same conclusion here. There is no dispute that the emails in question were sent or received via Walker's work email address, as part of an email system controlled and operated by Penn State. Thus, for purposes of the Fourth Amendment, the emails were subject to the common authority of Walker's employer. Walker did not enjoy any reasonable expectation of privacy vis-à-vis Penn State, and Penn State could independently consent to a search of Walker's work emails. Upon receipt of the subpoena, Penn State exercised its independent authority to consent to a search and produced Walker's work emails.[59]

Walker argues that we should find Penn State's consent invalid because it was procured through fraud or coercion, via the invalid subpoena. She notes that a law enforcement officer cannot evade the limitations of the Fourth Amendment by inducing private parties to do what they cannot. With that proposition, we agree. But Walker fails to recognize that 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. As alleged in Walker's

---

[58] *Id*. at 1190-91.

[59] In holding that Penn State had joint control over Walker's work emails, we need not address the government's argument that the third party doctrine applies.

complaint, Appellees presented the subpoena to Penn State's Assistant General Counsel.[60] Rather than contest the validity of the subpoena or otherwise limit any search, the Assistant General Counsel instructed an employee in her office to assist with the production of Walker's emails.[61] That decision was within the authority of Penn State—acting through its attorney—as Walker's employer. Under these circumstances, despite the facial invalidity of the subpoena, we decline to find that the university's consent was coerced.[62]

We emphasize that nothing in this opinion should be taken as condoning the actions of Appellees in this case. On the contrary we are dismayed by their reliance on an invalid subpoena to procure the documents that they sought. And we add a note of caution that, under slightly difference circumstances, similar actions might well lead us to a conclusion opposite from the one we reach today. But improper conduct alone does not result in a forfeiture of qualified immunity.[63] Rather, the relevant question is whether, under the particular circumstances of this case, Appellees' conduct violated Walker's clearly established

---

[60] App. at 39.

[61] App. at 39.

[62] *Cf. Schneckloth v. Bustamonte*, 412 U.S. 218, 227 (1973) ("[T]he question whether a consent to a search was in fact 'voluntary' or was the product of duress or coercion, express or implied, is a question of fact to be determined from the totality of all the circumstances.").

[63] *See Davis v. Scherer*, 468 U.S. 183, 194 (1984) ("Officials sued for constitutional violations do not lose their qualified immunity merely because their conduct violates some statutory or administrative provision.").

constitutional rights. Because we conclude that it did not, Appellees are entitled to qualified immunity. We will therefore affirm the District Court's dismissal of Walker's § 1983 claim.

C.

Walker also appeals the denial of her subsequent motion for reconsideration and for leave to file a second amended complaint. Attached to Walker's motion was a proposed second amended complaint, which included a new claim alleging violation of the SCA.[64] The District Court denied Walker's motion in a brief memorandum order that focused solely on reconsideration of Walker's § 1983 claim and made no mention of Walker's attempt to assert a new claim under the SCA.[65]

For the reasons stated at length above, we agree that Appellees are entitled to qualified immunity as to Walker's § 1983 claim, and the District Court therefore did not err in denying reconsideration. At present, however, we have insufficient information to determine whether Walker could plead a valid claim under the SCA. We therefore conclude that, as to Walker's attempt to assert a new claim under the SCA, the District Court abused its discretion by denying out of hand Walker's motion for leave to file a second amended complaint. We will therefore vacate in part the District

[64] App. at 105.
[65] App. at 28-30.

Court's order of May 17, 2017, and remand this matter to the District Court to address the SCA issue in the first instance.[66]

IV.

For the reasons stated above, we will affirm the District Court's dismissal of Walker's § 1983 claim, because we find that Appellees are entitled to qualified immunity. We will vacate in part the District Court's subsequent order denying Walker leave to file a second amended complaint, so that the District Court may address in the first instance Walker's attempt to assert a new claim under the SCA.

[66] Post-argument, the Supreme Court decided *Carpenter v. United States*, 585 U.S. ___, 138 S.Ct. 2206 (2018). As *Carpenter* post-dates the events in question, it has no bearing on the state of the law pertinent to the qualified immunity analysis. Any impact of *Carpenter* on the SCA claim is in the first instance for the District Court on remand.