UNPUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 22-1139

AMANDA CARSON, f/k/a Amanda Leche,

Plaintiff, Appellant,

v.

EMERGENCYMD, LLC; DAVID BRANCATI; JOHANNA CALGIE,

Defendants, Appellees.

Appeal from the United States District Court for the South Carolina, at Greenville. Joseph Dawson, III, District Judge. (6:20–cv–01946–JD)

Submitted: October 11, 2022 Decided: February 9, 2023

Before GREGORY, Chief Judge, and HARRIS and QUATTLEBAUM, Circuit Judges.

Vacated and remanded by unpublished per curiam opinion.

ON BRIEF: Wesley D. Few, WESLEY D. FEW, LLC, Greenville, South Carolina, for Appellant. R. Mills Ariail, Jr., LAW OFFICE OF R. MILLS ARIAIL, JR., Greenville, South Carolina, for Appellees.

Unpublished opinions are not binding precedent in this circuit.

PER CURIAM:

Amanda Carson appeals an order granting summary judgment to the defendants EmergencyMD, David Brancati and Johanna Calgie on her Stored Communications Act[1] claim. Because we find there are genuine disputes of material fact related to Carson's claim that the defendants violated the Stored Communications Act, we vacate the district court's order granting summary judgment and remand for further proceedings.

I.

Carson, a physician's assistant, worked at EmergencyMD, LLC as an independent contractor from February 2014 until May 1, 2017. In accepting this position, she agreed to be bound by the company handbook and all company policies, including EmergencyMD's Electronic Communication Policy.

Carson had the opportunity to use a work-email while at EmergencyMD but elected, with the company's approval, to use her personal Gmail account for work duties. When at work, she used a shared desktop computer to access her Gmail account. Other EmergencyMD employees and affiliates also used the same shared desktop computer.

EmergencyMD terminated Carson's employment for an inappropriate relationship with a subordinate employee in violation of the company's code of conduct. Carson then went to work with her ex-husband's company. Litigation between that company and EmergencyMD, as well as related parties, ensued. This litigation generally involved

[1] 18 U.S.C. § 2701, et. seq.

competing claims of unfair competition and misappropriation of trade secrets.[2] During this litigation, EmergencyMD published emails that it obtained from Carson's Gmail account. The emails contained communications between Carson and her new company. In some emails, Carson discussed joining the company and bringing EmergencyMD information and employees. Some of the communications were dated during the time Carson still worked at EmergencyMD, but others were dated after she had been terminated.

The publication of these emails in the state court litigation led to this lawsuit. Here, Carson asserts a claim against the defendants for violating the Stored Communications Act as well as state law claims for violating the South Carolina Homeland Security Act[3] and for invasion of privacy. In all these claims, Carson contends that the defendants intentionally, and without authorization, accessed her private Gmail account and printed emails for use in the state court litigation.

Discovery revealed that several weeks after EmergencyMD terminated Carson, someone associated with EmergencyMD logged on to the shared desktop computer and discovered Carson's private email account open on the web browser. Exactly how that occurred is not clear.

Megan Montagano was an employee of EmergencyMD Staffing, LLC—a separate but affiliated company—while Carson was working for EmergencyMD. Montagano

[2] The state court litigation involves multiple cases. Some cases have been stayed due to the bankruptcy of certain parties.

[3] S.C. Code Ann. § 17-30-10, et seq.

testified that she was the person who accessed Carson's account. She said that she regularly used the same shared work computer. Montagano testified that she woke the computer to check her Gmail account several weeks after Carson was terminated. When she did, she found that a Gmail inbox page was already open in the web browser. According to Montagano, the discovery of her open inbox caused her to suspect that, when previously using the computer, she neglected to log out of her Gmail account on that computer. But when she noticed several emails that she did not recognize, she claims to have worried that someone might have hacked her account. She then printed out over one hundred pages of emails and the corresponding attachments.

Montagano says she took the documents, without knowing their contents, to her supervisor, Dr. Jason Blasenak.[4] According to Montagano, after Dr. Blasenak looked over the printed pages, he told her that the emails were from Carson's email account. Montagano said she then logged out of that account and had nothing further to do with the emails.

Dr. David Brancati, also a supervisor at EmergencyMD, represented the company during a Federal Rule of Civil Procedure 30(b)(6) deposition. His testimony generally conforms to Montagano's.

Dr. Blasenak, however, tells a different story. He testified that he accessed the computer and immediately noticed that Carson's Gmail account was open on the web browser. According to Dr. Blasenak, he then told Dr. Brancati and Montagano that

[4] Jason Blasenak was also an original defendant in the lawsuit, but he settled and was dismissed before the district court order ruling on the motions for summary judgment.

Carson's private email account was open on the web browser. He claims to have no information about what they did with the emails. He does not remember Montagano bringing him the printed emails or telling her they were Carson's emails. He claims that he did not open or print any of the emails from Carson's account.

After discovery, the parties filed cross-motions for summary judgment on Carson's Stored Communications Act claim. The district court granted the defendants' motion. It determined that Carson failed to produce evidence that created a genuine dispute of material fact as to whether one of the defendants accessed the emails; whether such access was unintentional; and whether Carson authorized such access by agreeing to the EmergencyMD Electronic Communication Policy and by leaving her Gmail account open on EmergencyMD's computer.[5]

This appeal followed.[6]

[5] Additionally, the defendants moved for summary judgment on Carson's South Carolina Homeland Security Act and invasion of privacy claims. The district court granted the motion as to the South Carolina Homeland Security Act claim and declined to exercise supplemental jurisdiction over the state law claim for invasion of privacy as well Carson's motion for spoliation of evidence. Carson does not appeal the district court order granting defendants' summary judgment motion on the South Carolina Homeland Security Act violation claim. Carson included the spoliation motion in her appeal but, because the district court did not rule on the motion in the order—remanding it as a related motion to state court with the state law privacy claim—it is not properly before us. Thus, the only issue properly before us is the Stored Communications Act claim.

[6] We have jurisdiction under 28 U.S.C. § 1291.

II.

A.

We review de novo an award of summary judgment. In doing so, we "must review the facts in the light most favorable to [the non-movant], drawing all reasonable inferences in [her] favor." *Dean v. Jones*, 984 F.3d 295, 301 (4th Cir. 2021). Summary judgment may only be granted if "no material facts are disputed and the moving party is entitled to judgment as a matter of law." *Id.* (citing *Ausherman v. Bank of Am. Corp.*, 352 F.3d 896, 899 (4th Cir. 2003)).

B.

> Under the Stored Communications Act
>
> whoever --
>
> > (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> >
> > (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2701. Section 2707, in turn, provides a civil cause of action for violations of § 2701. 18 U.S.C. § 2707(a) (any "other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity… engaged in that violation such relief as may be appropriate."); *see Van Alstyne v. Elec. Scriptorium, Ltd.*, 50 F.3d 199, 204 (4th Cir. 2009) (citing 18 U.S.C. § 2701).

So, the question before us is whether there is a genuine dispute of material fact as to whether the defendants violated § 2701. Referring back to the requirement of establishing a violation of that provision, there is no question that the defendants obtained Carson's emails and that the emails are electronic communications. But under § 2701, Carson must still show that the defendants intentionally, and without authorization, accessed a facility through which electronic communication service was provided. The defendants insist that we should affirm the district court because Carson has not presented evidence that creates a genuine dispute of material fact on those requirements to establish a violation of § 2701. We disagree.

1.

First, as to whether one of the defendants intentionally accessed Carson's emails, the defendants point out that Carson conceded in her deposition that she has no proof that the defendants printed the emails. They add that Montagano, who is not an employee of EmergencyMD, nor a defendant in the lawsuit, testified that she discovered and printed the emails. And they also emphasize that Montagano said she had no idea the emails were from Carson and printed them only because she thought her account had been hacked.

But there is conflicting testimony on this. Dr. Blasenak testified that he, not Montagano, discovered the emails and then told Montagano and Dr. Brancati about Carson's Gmail account being open on the shared work computer. Construing the evidence and reasonable inferences from it in the light most favorable to Carson, a jury could reasonably believe that Dr. Blasenak, an employee of EmergencyMD, initially discovered the emails and, using information that they received from him, Dr. Brancati and Montagano

then intentionally reviewed Carson's emails and printed out the ones that provided evidence of her wrongdoing.

What's more, a reasonable jury might reject Montagano's testimony. Keep in mind that when the emails were discovered, the litigation between EmergencyMD and its competitor had begun. In that litigation, EmergencyMD claimed that Carson planned to recruit its employees and use its trade secrets to unfairly compete against EmergencyMD. Given that, a jury might not find Montagano's testimony credible. For example, a jury might find it is suspicious that, of all the information on Carson's private Gmail account, Montagano happened to print over 100 pages of emails that showed Carson's misconduct and took them to Dr. Blasenak without any knowledge that they were Carson's. Said differently, a jury might not accept Montagano's testimony that she coincidentally printed those emails because she thought her account might have been hacked. Thus, there is a genuine dispute of material fact as to whether the defendants accessed Carson's emails.

2.

Next, the defendants emphasize that there is no evidence in the record that the initial discovery of Carson's open and accessible Gmail account on EmergencyMD's computer—whether by Dr. Blasenak or Montagano—was intentional. There does not seem to be any dispute about this. But after that initial discovery, someone reviewed and printed emails showing Carson's interactions with a competing company, which were later used in litigation. So, the question that remains is whether the unintentional initial discovery of Carson's emails shields the subsequent decision to review and print certain emails from liability under the Act. We have not previously addressed this question, nor have we

delineated the contours of what it means to intentionally access electronic communications under the Act. But in our view, the evidence of the defendants' conduct after the initial discovery that Carson's account was open creates a question of fact as to whether the defendants intentionally accessed Carson's emails.

3.

Finally, as to whether Carson authorized EmergencyMD to obtain and disclose the emails, we consider first the defendants' argument that she did so by leaving her Gmail account open on the shared computer she used at EmergencyMD. The Act does not define "authorization." Nor have we had occasion to interpret that term. But the term is commonly understood to involve knowing, intentional action.[7] Unintentionally failing to log out of a computer seems at odds with the meaning of authorization. Perhaps it was careless. But did it authorize EmergencyMD to review her private emails? There is at least a question of fact on this issue.

Next, we consider the defendants' argument that Carson authorized the defendants' obtaining and disclosing her emails by agreeing to EmergencyMD's Electronic Communication Policy. To assess that argument, we must review the actual language of the Policy:

> All information created, sent, received, or stored on the company's electronic resources is company property. Such information is not the private property of any employee and employees should have no expectation of privacy in the

[7] For example, Webster's Ninth New Collegiate Dictionary (1986)—published in the same year Congress passed the Stored Communications Act—defines authorize as "to establish by or as if by authority," "to invest with legal authority," to "empower" or to "justify." These definitions all connote knowing and intentional conduct.

> use or contents of the company's electronic resources. Passwords do not confer any right of privacy upon any employee of the company. Employees should understand that the company may monitor the usage of its electronic resources and may access, review, and disclose information stored on its electronic resources, including messages, personal e-mail communications sent and received on the employer's computers but using private email accounts, and other data, at any time, with or without advance notice to the user or the user's consent.

J.A. 124.

At the outset, there is a genuine dispute of material fact as to whether the Policy authorized EmergencyMD to review emails sent or received after it terminated Carson's employment. We see nothing in the Policy that suggests an employee's use of the company's shared computer to access her Gmail account for work purposes authorizes EmergencyMD to access and use emails created on a private Gmail account after the employee has been terminated.

And even for emails sent or received while Carson was still employed at EmergencyMD, the Policy allowed it to access, review and disclose electronic information sent and received on the employer's computers. But the record does not establish that Carson's emails at issue here were created or sent on EmergencyMD's computers. Since Carson used her Gmail account for company business, the emails could have been sent from and received on her personal computer. Perhaps data from the emails or some other information will reveal whether Carson sent or received the emails from EmergencyMD's computers. But we cannot tell that from the record before us.

Also, the Policy allows EmergencyMD to access and disclose personal electronic information stored on its electronic resources. But emails from a Gmail account are not

stored on EmergencyMD's electronic resources. Gmail uses a web-based host for emails. *Hately v. Watts*, 917 F.3d 770, 773 (4th Cir. 2019). Google hosts and stores all emails so that an account holder can access the copies if they are not deleted by the user. *See id.* at 773, n. 1 (noting that when emails are stored using a web-based server, like the Google cloud system, then the user's "computer or mobile device merely serves as a conduit to access the [host's] server."). Using EmergencyMD computers to access electronic communications stored on a cloud storage system is not the same as storing electronic communications on EmergencyMD's electronic resources.

That is not to say that agreements with employees or company policies could not be crafted to allow an employer to access, review and disclose some or all of the emails at issue here. But there is at least a question of fact as to whether what Carson agreed to under EmergencyMD's Policy applies to the emails on her private Gmail account, even if she used that account in doing her job.

III.

Our decision here has nothing to do with the content of Carson's emails or whether she violated duties of loyalty owed to EmergencyMD. Those are matters for the state court litigation. Likewise, our decision does not mean that EmergencyMD did not have a right to seek the emails in the state court litigation under the South Carolina Rules of Civil Procedure or to request that steps be taken to ensure that the emails were not deleted or otherwise destroyed. Almost certainly it did. But there is at least a question of fact as to whether the defendants ignored those options and took steps prohibited by the Stored

Communications Act. A jury could reasonably conclude that the defendants intentionally, and without authorization, accessed Carson's emails on her private Gmail account. Accordingly, the order granting summary judgment for the defendants on Carson's Stored Communications Act claim is

VACATED AND REMANDED.