961 F.Supp.2d 659 (2013)

Deborah EHLING, Plaintiff,
v.
MONMOUTH-OCEAN HOSPITAL SERVICE CORP., et al., Defendants.

United States District Court, D. New Jersey.

August 20, 2013.WILLIAM J. MARTINI, District Judge:

Plaintiff Deborah Ehling filed this action against Monmouth-Ocean Hospital Service Corp. ("MONOC"), Vincent Robbins, and Stacy Quagliana (collectively "Defendants"). This matter comes before the Court on Defendants' motion for summary judgment under Federal Rule of Civil Procedure 56. There was no oral argument. Fed.R.Civ.P. 78(b). For the reasons set forth below, Defendants' motion for summary judgment is GRANTED.

## I. BACKGROUND

Plaintiff Deborah Ehling is a registered nurse and paramedic. Defendant MONOC is a non-profit hospital service corporation dedicated to providing emergency medical services to the citizens of the State of New Jersey. Defendant Vincent Robbins is the President and CEO of MONOC. Defendant Stacy Quagliana is the Executive Director of Administration at MONOC.

Plaintiff was hired by MONOC in 2004 as a registered nurse and paramedic. In July of 2008, Plaintiff took over as President of the Professional Emergency Medical Services Association—New Jersey (the "Union"). As President of the Union, Plaintiff was regularly involved in actions intended to protect MONOC employees. For example, Plaintiff filed complaints with the Environmental Protection Agency ("EPA") and the New Jersey Department of Environmental Protection ("NJDEP"), reporting that MONOC's use of a disinfectant called Zimek was creating health problems for employees. In response, the EPA issued a removal order requiring MONOC to stop using Zimek. Plaintiff also testified in the wage and hour lawsuit of another MONOC employee.

Plaintiff's claims in this case arise out of: (1) an incident involving Plaintiff's Facebook account, and (2) Plaintiff's disciplinary record and medical leave. The Court will summarize the pertinent facts relating to each issue.

### A. The Facebook Incident

Facebook is a widely-used social-networking website. The website provides a digital medium that allows users to connect and communicate with each other. Every Facebook user must create a Profile Page, which is a webpage that is intended to convey information about the user. The Profile Page can include the user's contact information; pictures; biographical information, such as the user's birthday, hometown, educational background, work history, family members, and relationship status; and lists of places, musicians, movies, books, businesses, and products that the user likes. A Facebook user can connect with other users by adding them as "Facebook friends." Facebook users can have dozens, hundreds, or even thousands of Facebook friends. In addition to having a Profile Page, each user has a webpage called a News Feed. The News Feed

aggregates information that has recently been shared by the user's Facebook friends. By default, Facebook pages are public. However, Facebook has customizable privacy settings that allow users to restrict access to their Facebook content. Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user.

Facebook provides users with several means of communicating with one another. Users can send private messages to one or more users. Users can also communicate by posting information to their Facebook "wall," which is part of each user's Profile Page. A Facebook "wall post" can include written comments, photographs, digital images, videos, and content from other websites. To create a Facebook wall post, users upload data from their computers or mobile devices directly to the Facebook website. Facebook then saves that data onto its computers (called "servers"). New wall posts are typically distributed to a user's Facebook friends using the News Feed feature. Users' most recent wall posts also appear at the top of their Profile Pages. A user's Facebook friends can comment on the wall posts, indicate that they "like" the wall posts, or share the posts with other users. Facebook users typically do not post information to their Facebook walls with the intent to delete it later. Instead, Facebook designed its website so that its servers would save this data indefinitely. As more and more wall posts are added, earlier wall posts move lower and lower down on the user's Profile Page, and are eventually archived on separate pages that are accessible, but not displayed.

During the 2008-2009 timeframe, Plaintiff maintained a Facebook account and had approximately 300 Facebook friends. Plaintiff selected privacy settings for her account that limited access to her Facebook wall to only her Facebook friends. Plaintiff did not add any MONOC managers as Facebook friends. However, Plaintiff added many of her MONOC coworkers as friends, including a paramedic named Tim Ronco. Plaintiff posted on Ronco's Facebook wall, and Ronco had access to Plaintiff's Facebook wall. Unbeknownst to Plaintiff, Ronco was taking screenshots of Plaintiff's Facebook wall and printing them or emailing them to MONOC manager Andrew Caruso. Ronco and Caruso became friends while working together at a previous job, but Ronco never worked in Caruso's division at MONOC. The evidence reflects that Ronco independently came up with the idea to provide Plaintiff's Facebook posts to Caruso. Caruso never asked Ronco for any information about Plaintiff, and never requested that Ronco keep him apprised of Plaintiff's Facebook activity. In fact, Caruso was surprised that Ronco showed him Plaintiff's Facebook posts. Caruso never had the password to Ronco's Facebook account, Plaintiff's Facebook account, or any other employee's Facebook account. Once Caruso received copies of Plaintiff's Facebook posts, he passed them on to Quagliana, MONOC's Executive Director of Administration.

On June 8, 2009, Plaintiff posted the following statement to her Facebook wall:

An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards. . . . go to target practice.

After MONOC management was alerted to the post, Plaintiff was temporarily suspended *with* pay, and received a memo stating that MONOC management was concerned that Plaintiff's comment reflected a "deliberate disregard for patient safety." In response, Plaintiff filed a complaint with the National Labor Relations Board ("NLRB"). After reviewing the evidence, the NLRB found that MONOC did not violate the National Labor Relations Act. The NLRB also found that there was no privacy violation because the post was sent, unsolicited, to MONOC management.

*****

A. Count 1: Federal Stored Communications Act

In Count 1, Plaintiff asserts a claim for violation of the Federal Stored Communications Act (or "SCA"), 18 U.S.C. §§ 2701-11. Plaintiff argues that Defendants violated the SCA by improperly accessing her Facebook wall post about the museum shooting. Plaintiff argues that her Facebook wall posts are covered by the SCA because she selected privacy settings limiting access to her Facebook page to her Facebook friends. Defendants disagree and argue that, even if the SCA applies, the facts in this case fall under one of the SCA's statutory exceptions. For the reasons set forth below, the Court finds that non-public Facebook wall posts are covered by the SCA, and that one of the exceptions to the SCA applies. The Court will address each issue in turn.

i. The SCA Covers Non-Public Facebook Wall Posts

The first issue before the Court is whether the SCA applies to Facebook wall posts. Very few courts have addressed this issue. *See* Catherine Crane, *Social Networking v. the Employment-at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking*, 89 Wash. U.L.Rev. 639, 668 (2012) ("Very few courts, however, have ruled on whether other unique features found within social networking sites—such as wall posts, status updates, notes, pictures, etc.—could also be protected against employer intrusion under the SCA"). For the reasons set forth below, the Court finds that Facebook wall posts fall within the purview of the SCA.

In 1986, Congress passed the Electronic Communications Privacy Act, which was intended to afford privacy protection to electronic communications. *See* Pub.L. No. 99-508, 100 Stat. 1848; *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir.2002). Title II of the Electronic Communications Privacy Act contains the SCA, which was designed to "address[] access to stored wire and electronic communications and transactional records." S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. "The legislative history of the [SCA] suggests that Congress wanted to protect electronic communications that are configured to be private." *Konop*, 302 F.3d at 875; *see also* S.Rep. No. 99-541, at 35-36, 1986 U.S.C.C.A.N. at 3599 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public."); H.R.Rep. No. 99-647 at 41, 62-63 (1986) (describing the Committee's understanding that the configuration of an electronic communications system would determine whether an electronic communication was accessible to the public).

******

The SCA provides that 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 the authorized access to a wire or electronic communication while in electronic storage in such a system" shall be liable for damages. 18 U.S.C. § 2701(a); 18 U.S.C. § 2707 (providing for civil liability under the statute). The statute further provides that "[i]t shall not be unlawful . . . [to] access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). In other words, the SCA covers: (1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) that are not public. Facebook wall posts that are configured to be private meet all four criteria.

*******

*Fourth,* Facebook wall posts that are configured to be private are, by definition, not accessible to the general public. The touchstone of the Electronic Communications Privacy Act is that it protects private information. The language of the statute makes clear that the statute's purpose is to protect information that the communicator took steps to keep private. *See* 18 U.S.C. § 2511(2)(g)(i) (there is no protection for information that is "configured [to be] readily accessible to the general public"); *see also* *Konop*, 302 F.3d at 875 ("The legislative history of the [Electronic Communications Privacy Act] suggests that Congress wanted to protect electronic communications that are configured to be private"). Cases interpreting the SCA confirm that information is protectable as long as the communicator actively restricts the public from accessing the information. *See* *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y.2008) (holding that SCA prevented Viacom from accessing YouTube "videos that [users] have designated as private and chosen to share only with specified recipients"); *Crispin*,717 F.Supp.2d at 991 (finding that SCA protection for Facebook wall posts depends on plaintiff's use of privacy settings); *cf.* *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir.2006) ("an express warning, on an otherwise publicly accessible webpage" is insufficient to give rise to SCA protection).

Facebook allows users to select privacy settings for their Facebook walls. Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user. The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are "configured to be private" for purposes of the SCA. The Court notes that when it comes to privacy protection, the critical inquiry is whether Facebook users took steps to limit access to the information on their Facebook walls. Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has. "Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing" and would be legally unworkable. *Crispin*, 717 F.Supp.2d at 990; *see also* Crane, 89 Wash. U.L.Rev. at 641 ("The fulcrum in [the privacy] balancing act exists as one, seemingly obvious, factor: privacy settings.").

******

Accordingly, the Court finds that non-public Facebook wall posts are covered by the SCA. Because Plaintiff in this case chose privacy settings that limited access to her Facebook wall to only her Facebook friends, the Court finds that Plaintiff's Facebook wall posts are covered by the SCA.

ii. The SCA's Authorized User Exception Applies in this Case

Having concluded that the SCA applies to the type of communication at issue in this case, the Court next evaluates whether either of the SCA's statutory exceptions apply. The SCA "does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c); *see also* *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754, 2009 WL 3128420, at *2 (D.N.J. Sept. 25, 2009) ("According to the SCA, if access to [a restricted website] was authorized by a user of that service with respect to a communication of or intended for that user, there is no statutory violation") (internal quotations omitted). For the reasons set forth below, the Court finds that the authorized user exception (the second exception) applies in this case.

The authorized user exception applies where (1) access to the communication was "authorized," (2) "by a user of that service," (3) "with respect to a communication. . . intended for that user." 18 U.S.C. § 2701(c)(2). Access is not authorized if the "purported `authorization' was coerced or provided under pressure." *Pietrylo*, 2009 WL 3128420, at *3. In this case, all three elements of the authorized user exception are present.

*First*, access to Plaintiff's Facebook wall post was "authorized." 18 U.S.C. § 2701(c)(2). The undisputed evidence establishes that Ronco voluntarily provided Plaintiff's Facebook posts to MONOC management without any coercion or pressure. Caruso testified at his deposition that Plaintiff's Facebook friend Ronco voluntarily took screenshots of Plaintiff's Facebook page and either emailed those screenshots to Caruso or printed them out for him. Certification of M. Elizabeth Duffy Ex. C 42:20-43:3, 45:11-22, ECF No. 36-1. This information was completely unsolicited. Caruso never asked Ronco for any information about Plaintiff and never requested that Ronco keep him apprised of Plaintiff's Facebook activity; in fact, Caruso was surprised that Ronco showed him Plaintiff's Facebook postings. Ex. C 43:6-8, 44:23-45:1, 52:11-17, 53:4-8, 62:19-21, 87:18-88:1. Caruso never had the password to Ronco's Facebook account, Plaintiff's Facebook account, or any other employee's Facebook account. Ex. C 44:7-9, 88:13-21. Caruso's deposition testimony is supported by additional evidence, including a copy of a May 10, 2009 email from Ronco to Caruso attaching copies of Plaintiff's Facebook posts, Quagliana's testimony that she never asked Caruso or anyone else to provide her with a copy of Plaintiff's Facebook page, and Caruso's NLRB affidavit. Ex. H, D 619; Ex. E 47:9-49:6; Ex. H, D 425.

Plaintiff provided no evidence to support her theory that access to her Facebook page was unauthorized. In the Amended Complaint, Plaintiff alleged that Defendants gained access to her Facebook page because a "member of upper management summoned a MONOC employee, who was also one of Ms. Ehling's Facebook friends, into his office" and "coerced, strong-armed, and/or threatened this employee into accessing his Facebook account on the work computer in the supervisor's presence." Am. Compl. ¶ 20. After discovery, it became clear that this was not

the case. Instead, the evidence reflected that Ronco voluntarily shared this information with Caruso. Plaintiff now surmises that Ronco must have shared the information for "compensation or privileged treatment or a really good deal." Ex. B 139:5-11. But this theory does not make sense in light of MONOC's management structure. Ronco never worked in a division that Caruso oversaw, and Caruso never had control over Ronco's pay or bonuses, so Caruso was not in a position to offer Ronco any sort of benefit. Ex. C 53:11-19, 86:3-10. Furthermore, Plaintiff's theory is pure speculation. Plaintiff did not depose Ronco because Ronco was "traveling in an RV" and no longer worked for MONOC. Ex. C 62:2-3. And Plaintiff produced no other evidence that Ronco provided information in exchange for compensation (or some other benefit). Thus, the undisputed evidence shows that access to Plaintiff's Facebook wall post was authorized.

*Second*, access to Plaintiff's Facebook wall post was authorized "by a user of that service." 18 U.S.C. § 2701(c)(2). A "user" is "any person or entity who (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13). It is undisputed that Ronco was a Facebook user: Plaintiff acknowledged that she added Ronco as a Facebook friend and posted on Ronco's Facebook wall. Ex. B 150:17-152:16.

*Third*, Plaintiff's Facebook wall post was "intended for that user." 18 U.S.C. § 2701(c)(2). Based on the privacy settings that Plaintiff selected for her Facebook page, Plaintiff's wall posts were visible to, and intended to be viewed by, Plaintiff's Facebook friends. Am. Compl. ¶ 11. On June 8, 2009, when Plaintiff posted the comment about the museum shooting, Ronco was one of Plaintiff's Facebook friends. Ehling Cert. Ex. A 155:8-21, ECF No. 38. Thus, the post was intended for Ronco.

In conclusion, access to Plaintiff's Facebook wall post was authorized by a Facebook user with respect to a communication intended for that user. Therefore, the authorized user exception applies and Defendants are not liable under the SCA. Accordingly, the motion for summary judgment on Count 1 is GRANTED.

*****

E. Count 6: Invasion of Privacy

In Count 6, Plaintiff asserts a claim for common law invasion of privacy. Plaintiff's claim is premised on Defendants' alleged unauthorized "accessing of her private Facebook postings" regarding the museum shooting. Am. Compl. ¶ 78. Defendants argue that they are entitled to summary judgment on the privacy claim because Plaintiff's friend "freely chose to share the information" with Defendants. Mot. Summ. J. at 11. The Court finds that summary judgment should be granted on Count 6.

A claim for invasion of privacy under New Jersey law will succeed if a plaintiff brings forth evidence showing that (1) there was an intentional intrusion "upon the solitude or seclusion of another or his private affairs," and that (2) this intrusion would highly offend the reasonable person. *Bisbee v. John C. Conover Agency, Inc.*, 186 N.J.Super. 335, 339, 452 A.2d 689 (App.Div.1982). Under the first prong, a defendant must commit an intrusive act. *See*

Restatement (Second) of Torts § 652B (1977) ("The intrusion itself makes the defendant subject to liability"); *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir.1989) (according to the Restatement, an actor must "commit [an] intrusive act" to be liable for invasion of privacy). "The converse of this principle is, however, of course, that there is no wrong where defendant did not actually delve into plaintiff's concerns." *Bisbee*, 186 N.J.Super. at 340, 452 A.2d 689. Plaintiff faces a high burden in asserting a cause of action based on intrusion of seclusion. *Stengart v. Loving Care Agency, Inc.*,201 N.J. 300, 316-17, 990 A.2d 650 (2010).

In this case, Plaintiff failed to show that there was an intentional intrusion by any of the Defendants. In the Amended Complaint, Plaintiff alleged that Defendants gained access to her Facebook page because a "member of upper management summoned a MONOC employee . . . into his office" and "threatened this employee into accessing his Facebook account." Am. Compl. ¶ 20. Now that discovery is complete, it is clear that there is no evidentiary support for these allegations. The evidence does not show that Defendants obtained access to Plaintiff's Facebook page by, say, logging into her account, logging into another employee's account, or asking another employee to log into Facebook. Instead, the evidence shows that Defendants were the passive recipients of information that they did not seek out or ask for. Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else. *See* Ex. C 43:6-8, 44:23-45:1, 52:11-17, 53:4-8, 62:19-21, 87:18-88:1; Ex. E 47:9-49:6; Ex. H, D 425, D 619. This may have been a violation of trust, but it was not a violation of privacy.

Accordingly, the motion for summary judgment on Count 6 is GRANTED.

******