UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DEBORAH EHLING, **Plaintiff,** **v.** **MONMOUTH-OCEAN HOSPITAL SERVICE CORP., *et al.*,** **Defendants.**	Civ. No. 2:11-cv-03305 (WJM) **OPINION**

WILLIAM J. MARTINI, U.S.D.J.:

Plaintiff Deborah Ehling brings this action against Monmouth-Ocean Hospital Service Corp. ("MONOC"), Vincent Robbins, and Stacy Quagliana (collectively "Defendants"), alleging violations of the Electronic Communications Privacy Act, the Family Medical Leave Act, and various state laws. This matter comes before the Court on Defendants' motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief may be granted. There was no oral argument. Fed. R. Civ. P. 78(b). For the reasons set forth below, Defendants' Rule 12(b)(6) motion is **GRANTED in part, and DENIED in part**.

I. BACKGROUND

The following facts are drawn from the Amended Complaint and the documents that form the basis of Plaintiff's claims.

Plaintiff Deborah Ehling is a registered nurse and paramedic. Defendant Monmouth-Ocean Hospital Service Corporation ("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 the Acting President of the local union for Professional Emergency Medical Services Association – New Jersey (the "Union"). As President, Plaintiff was "very proactive in attempting to protect the rights and safety of her union members" and filed numerous complaints and charges against MONOC to that end. Am. Compl. 8. Plaintiff alleges that, as soon as she became President of the Union, Defendants began engaging in a pattern of retaliatory conduct against her, eventually culminating in her termination in July 2011. Although the Amended Complaint contains allegations regarding a wide range of conduct, the Court will discuss only those allegations that are relevant to the motion to dismiss.

During the 2008-2009 timeframe, Plaintiff maintained an account on Facebook, a social networking website. According to Plaintiff, if someone was not invited to be her Facebook "friend," he or she could not access and view postings on Plaintiff's Facebook "wall." Many of Plaintiff's coworkers were invited to be Plaintiff's Facebook friends. Plaintiff did not invite any members of MONOC management as friends.

Plaintiff alleges that MONOC "[s]ubsequently . . . gained access to Ms. Ehling's Facebook account by having a supervisor(s) summon a MONOC employee, who was also one of Ms. Ehling's Facebook friends, into an office" and "coerc[ing], strong-arrn[ing], and/or threaten[ing] the employee into accessing his Facebook account on the work computer in the supervisor's presence." Am. Compl. 20. Plaintiff claims that the supervisor viewed and copied Plaintiff's Facebook postings. One such posting was a comment that Plaintiff made regarding a shooting that took place at the Holocaust Museum in Washington, DC, stating:

> 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.

Certification of Elizabeth Duffy ("Duffy Cert.") Ex. C, ECF No. 11.[1] On June 17, 2009, MONOC sent letters regarding Plaintiff's Facebook posting to the New Jersey Board of

[1] The Court relies on the screenshot of Plaintiff's Facebook page attached to the motion to dismiss, as Plaintiff's Facebook posting is integral to Plaintiff's Amended Complaint. *See* Am. Compl. ¶¶ 11-13, 18, 20-23; *see also In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997) ("a document integral to or explicitly relied upon in the complaint may be considered without converting the motion to dismiss into one for summary judgment") (internal citations omitted); *Pryor v. Nat'l Coll. Athletic Ass'n*, 288 F.3d 548, 560 (3d Cir. 2002) ("documents whose contents are alleged in the complaint and whose authenticity no party

Nursing and the New Jersey Department of Health, Office of Emergency Medical Services. The letters state that MONOC was concerned that Plaintiff's Facebook posting showed a disregard for patient safety. *See* Duffy Cert. Ex. A, ECF No. 11. Plaintiff alleges that these letters were sent in a "malicious" attempt to attack Plaintiff, damage her reputation and employment opportunities, and potentially risk losing her nursing license and paramedic certification status. Am. Compl. 21-22.

II. LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(6) provides for the dismissal of a complaint, in whole or in part, if the plaintiff fails to state a claim upon which relief can be granted. The moving party bears the burden of showing that no claim has been stated. *Hedges v. United States*, 404 F.3d 744, 750 (3d Cir. 2005). In deciding a motion to dismiss under Rule 12(b)(6), a court must take all allegations in the complaint as true and view them in the light most favorable to the plaintiff. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975); *Trump Hotels & Casino Resorts, Inc. v. Mirage Resorts Inc.*, 140 F.3d 478, 483 (3d Cir. 1998).

Although a complaint need not contain detailed factual allegations, "a plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Thus, the factual allegations must be sufficient to raise a plaintiff's right to relief above a speculative level, such that it is "plausible on its face." *See id.* at 570; *see also Umland v. PLANCO Fin. Serv., Inc.*, 542 F.3d 59, 64 (3d Cir. 2008). A claim has "facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009) (citing *Twombly*, 550 U.S. at 556). While "[t]he plausibility standard is not akin to a 'probability requirement' . . . it asks for more than a sheer possibility." *Iqbal*, 129 S.Ct. at 1949 (2009).

III. DISCUSSION

Defendants move to dismiss two of the nine counts in the Amended Complaint: (1) Count II, alleging a violation of the New Jersey Wiretapping and Electronic Surveillance Control Act; and (2) Count IV, alleging common law invasion of privacy. Each issue will be addressed in turn.

---

questions, but which are not physically attached to the pleading, may be considered" on a motion to dismiss).

a. N.J. WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT (COUNT II)

In Count II of the Amended Complaint, Plaintiff alleges that Defendants violated the a. New Jersey Wiretapping and Electronic Surveillance Control Act ("NJ Wiretap Act"), N.J.S.A. 2A:156A-27, "by accessing without permission and improperly monitoring the electronic communications being stored on the plaintiffs Facebook account." Am. Compl. 59. Defendants move to dismiss Count II on the ground that the communication was not accessed in the course of transmission. The Court finds that Count II should be dismissed.

The NJ Wiretap Act provides that: "A person is guilty of a crime of the fourth degree if he (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and (2) thereby obtains, alters, or prevents authorized access to a wire or electronic communication while that communication is in electronic storage." N.J.S.A. 2A:156A-27(a). "Electronic storage," as used in the NJ Wiretap Act, is defined as: "(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) Any storage of such communication by an electronic communication service for purpose of backup protection of the communication." N.J.S.A. 2A:l56A-2(q).

Based on the definition of "electronic storage," New Jersey courts have held that the NJ Wiretap Act "protects only those electronic communications, which are in the course of transmission or are backup to that course of transmission." *White v. White*, 344 N.J. Super. 211, 220 (Ch. Div. 2001). Thus, in *White*, the court concluded that the NJ Wiretap Act "does not apply to electronic communications received by the recipient, placed in post-transmission storage, and then accessed by another without authorization[,]" because "the 'strong expectation of privacy with respect to communication in the course of transmission significantly diminishes once transmission is complete.'" *Id.* at 220. This is consistent with federal courts' interpretation of similar provisions of the federal Wiretap Act (18 U.S.C. § 2510 et seq.). *See Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission."); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (dismissing claim for violation of the Wiretap Act in a case where employer gained access to restricted employee website because the electronic communication was not acquired "during transmission").

In this case, Plaintiff clearly failed to state a claim under the NJ Wiretap Act. The Amended Complaint does not allege that Plaintiff's Facebook posting was in the course of transmission when Defendants viewed it. To the contrary, the Amended Complaint clearly states that the posting was live on the Facebook website for all of Plaintiff's

Facebook friends to "access and view." Am. Compl. 11. Because the posting was in post-transmission storage when Defendants accessed it, this communication does not fall under the purview of the NJ Wiretap Act.

Accordingly, the motion to dismiss Count II of the Amended Complaint is granted.

b. COMMON LAW INVASION OF PRIVACY (COUNT VI)

In Count VI of the Amended Complaint, 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 Holocaust Museum shooter. Am. Compl. 78; Duffy Cert. Ex. C. Defendants move to dismiss Count VI, arguing that Plaintiff did not have a reasonable expectation of privacy in her Facebook posting. The Court finds that the motion to dismiss Count VI should be denied.

Under New Jersey law, to state a claim for intrusion upon one's seclusion or private affairs, a plaintiff must allege sufficient facts to demonstrate that (1) her solitude, seclusion, or private affairs were intentionally infringed upon, and that (2) this infringement would highly offend a reasonable person. *See Bisbee v. John C. Conover Agency Inc.*, 186 N.J. Super. 335, 339 (App. Div. 1982). "[E]xpectations of privacy are established by general social norms" and must be objectively reasonable – a plaintiff's subjective belief that something is private is irrelevant. *White*, 344 N.J. Super. 211, 223 (Ch. Div. 2001).

Privacy in social networking is an emerging, but underdeveloped, area of case law. *See* Robert Sprague, *Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship*, 50 U. Louisville L. Rev. 1, 13 (2011) (discussing the undefined legal boundary between public and private communications on social networking websites). There appears to be some consistency in the case law on the two ends of the privacy spectrum. On one end of the spectrum, there are cases holding that there is ***no*** reasonable expectation of privacy for material posted to an unprotected website that anyone can view. *See, e.g., United States v. Gines-Perez*, 214 F.Supp.2d 205, 225 (D.P.R. 2002), *rev'd on other grounds*, 90 F. App'x 3 (1st Cir. 2004) ("[I]t it strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any measures to protect the information"); *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 44 (Minn. Ct. App. 2009) (holding that privacy was lost when private information was posted on a publicly accessible Internet website and "[a]ccess to the publication was not restricted"). On the other end of the spectrum, there are cases holding that there ***is*** a reasonable expectation of privacy for individual, password-protected online communications. *See, e.g., Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (N.J. 2010) (employee could have reasonably expected that e-mail communications with her

lawyer through her personal, password-protected, web-based e-mail account would remain private); *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (employee had a reasonable expectation of privacy in personal, password-protected e-mail messages stored on a third party's server, although the employee had accessed that outside server while at work).

Courts, however, have not yet developed a coherent approach to communications falling between these two extremes. Although most courts hold that a communication is not necessarily public just because it is accessible to a number of people, courts differ dramatically in how far they think this theory extends. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. Chi. L. Rev. 919, 939, 973 (2005) (explaining that most courts have adopted the concept of "limited privacy," which is "the idea that when an individual reveals private information about herself to one or more persons, she may retain a reasonable expectation that the recipients of the information will not disseminate it further."); *compare Multimedia Wmaz v. Kubach*, 212 Ga. App. 707, 709 & n.1 (Ga. Ct. App. 1994) (plaintiff's disclosure of facts to sixty people did not render them public) *with Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 878 (8th Cir. 2000) (plaintiff's disclosure of facts to two coworkers deprived her of a reasonable expectation of privacy). What is clear is that privacy determinations are made on a case-by-case basis, in light of all the facts presented. *See Pietrylo v. Hillstone Rest. Group*, No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *20 (D.N.J. July 24, 2008).

In this case, Plaintiff argues that she had a reasonable expectation of privacy in her Facebook posting because her comment was disclosed to a limited number of people who she had individually invited to view a restricted access webpage. Defendants argue that Plaintiff cannot have a reasonable expectation of privacy because the comment was disclosed to dozens, if not hundreds, of people.[2] The Amended Complaint and underlying documents do not indicate how many Facebook friends Plaintiff had at the time the comment was made; thus, there is no indication of how many people could permissibly view Plaintiff's posting.

The Court finds that Plaintiff has stated a plausible claim for invasion of privacy, especially given the open-ended nature of the case law. Plaintiff may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing. More importantly, however, reasonableness (and offensiveness) are highly fact-sensitive inquiries. As such, these issues are not properly resolved on a motion to dismiss. *See*

[2] The parties did not cite any relevant case law in support of their arguments. Instead, they each cited to a single, non-analogous case. Plaintiff cited a case in which the Court held that there was ***no*** reasonable expectation of privacy in communications sent over the company e-mail system. *See Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996). Defendants cited a case in which the person accused of invading the plaintiff's privacy had direct, authorized access to the communications at issue. *See White*, 344 N.J. Super. at 223.

Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *20 (D.N.J. July 24, 2008) ("[T]he question of the reasonableness of the Plaintiffs' expectations of privacy is a question of fact for the jury to decide.").

Accordingly, the motion to dismiss Count VI of the Amended Complaint is denied.

IV. CONCLUSION

For the reasons stated above, Defendants' motion to dismiss is **GRANTED in part, and DENIED in part**. Specifically, the motion to dismiss Count II of the Amended Complaint is granted, and Count II is dismissed with prejudice. The motion to dismiss Count VI is denied. An appropriate order follows.

/s/ William J. Martini
WILLIAM J. MARTINI, U.S.D.J.

Date: May 30, 2012.