UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 2 Article 6

2014

The Thirty-Third Annual John Marshall Law School International Moot Court Competition in Information Technology and Privacy Law: Brief for the Respondent, 31 J. Marshall J. Computer & Info. L. 285 (2014)

Sara Schroeder

Austin Hoffman

Becky Fey

BRIEF FOR RESPONDENT

NO. 2014-CV-1234

IN THE

SUPREME COURT OF THE STATE OF MARSHALL

FALL TERM 2014

JANE SHAPIRO, AN INDIVIDUAL,
Petitioner,

V.

U.S. APPAREL, A CORPORATION,
Respondent.

ON APPEAL TO THE SUPREME COURT OF THE STATE OF MARSHALL

SARA SCHROEDER

AUSTIN HOFFMAN

BECKY FEY

QUESTIONS PRESENTED

I. Whether the Circuit Court of Nashville County properly dismissed Petitioner's claim of intrusion upon seclusion?

II. Whether the Circuit Court of Nashville County properly dismissed Petitioner's claim of a violation of the State of Marshall Computer Fraud and Abuse Act?

III. Whether the Circuit Court of Nashville County properly dismissed Petitioner's claim of conversion?

OPINIONS BELOW

The Nashville County Circuit Court granted U.S. Apparel's motion to dismiss the three counts of intrusion upon seclusion, a violation of the Computer Fraud and Abuse Act, and conversion. Jane Shapiro appealed this decision to the Third District of the Appellate Court ofthe State of Marshall. The Marshall Court of Appeals certified the three questions raised by Shapiro to the Supreme Court of the State of Marshall. The Supreme Court accepted the case for review.

STATEMENT OF JURISDICTION

A formal Statement of Jurisdiction has been omitted pursuant to §1020 of the Rules for the 33rd Annual John Marshall Law School Moot Court Competition in Information Technology and Privacy Law.

STANDARD OF REVIEW

When reviewing a district court's dismissal of an action for failure to state a claim, the decision is reviewed de novo. *Vesely v. Armslist LLC*, 13-3505, 2014 WL 3907114, at *2 (7th Cir. Aug. 12, 2014). All well-pleaded facts will be construed in the light most favorable to the nonmoving party. *Id.*

STATEMENT OF THE FACTS

I. FACTUAL BACKGROUND

U.S. Apparel ("Respondent"), an American clothing designer, manufactures and sells clothing targeted toward pre-teens and teens. (R. at 1). Respondent is known in the industry as a responsible and wholesome producer. *Id.* Jane Shapiro ("Petitioner"), Respondent's former chief executive officer, developed business strategy, operation plans, marketing proposals, promotion material, and company policy. *Id*. Peti-

tioner frequently traveled on behalf of Respondent and utilized a personal tablet and cell phone, which both automatically synced to a desktop located within Respondent's place of business. *Id.* Petitioner could access Respondent's detailed business plans, written policies, and contact information from all three devices. *Id.*

Sharon Bennett ("Bennett"), an employee of Respondent, created two social media accounts while acting as Petitioner's administrative assistant. *Id.* Bennett created a Twitter account titled "@U.S.Apparel_Shapiro" and a LinkedIn account using the name Jane Shapiro. *Id.* These social media accounts were used for promoting and communicating with the public on behalf of Respondent's business. *Id.* Petitioner gave Bennett the passwords to these accounts, despite Respondent's policy to the contrary. *Id.* Petitioner advised Bennett that Petitioner's authorization was necessary to access these accounts. *Id*. In addition to company business,

Petitioner also used these social media accounts to build her reputation, connect with family, friends and colleagues, and to sustain professional relationships. (R. at 2). Following a decline in business, Respondent's board of directors voted for a change in leadership. *Id.* An effort to reinvent the company's image and change its marketing strategy ultimately led to Petitioner's forced termination. *Id*. Petitioner was replaced by Victor Valentini ("Valentini"), who was well known in the clothing industry. *Id*. Upon termination, Petitioner kept her personal tablet and cell phone. *Id.*

Valentini instructed Bennett to access files located on Petitioner's former office desktop computer. Id. Bennett located a folder titled, "Personal" in which she found files labelled "Threads Business Plan" and "Hanoi Labor, Co." *Id*. These files detailed Petitioner's business

plans and a personal agreement with Hanoi Labor, Co. for a possible new clothing company. *Id.*

Bennett relayed this information to Valentini, who informed Respondent's Chairman of the Board. *Id.* Although Respondent did not do business with Hanoi Labor, Co., the Chairman of the Board directed Valentini to examine Hanoi Labor, Co.'s business practices. *Id*. After the month-long independent investigation, Respondent learned that Hanoi Labor, Co. employed young children under dire working conditions, which included 14-hour days in poorly lit, crowed, and unsanitary facilities for less than $25.00 a month. *Id*. The Chairman of the Board disclosed Petitioner's possible business plans to the public, along with Hanoi Labor, Co.'s dismal working conditions and use of child labor. (R. at 3).

Subsequently, Valentini instructed Bennett to sign in to Petitioner's company LinkedIn and Twitter accounts and substitute Petitioner's information for Valentini's. *Id*. Bennett changed Petitioner's name, photo, personal information, and updated the handle from

"@U.S.Apparel_Shapiro" to "@U.S.Apparel_Valentini." *Id.* Bennett modified the passwords, preventing Petitioner from signing in to these account. *Id.* All other posts, connections, and followers associated with these accounts remained the same. *Id.*

II. PROCEDURAL BACKGROUND

Petitioner filed suit against Respondent by filing a three-count complaint alleging (1) intrusion upon seclusion; (2) a violation of the State of Marshall Computer Fraud and Abuse Act; and (3) conversion. (R. at 3-5). Respondent moved to dismiss all three counts alleged by Petitioner. (R. at 5). The Circuit Court of Nashville County granted Respondent's motion, finding that Petitioner had failed to state a claim upon which relief can be granted, under State of Marshall Rules of Civil Procedure, § 12(b)(6). Id.

Petitioner appealed to the Third District of the Appellate Court of the State of Marshall. *Id*. The Appellate Court certified Petitioner's questions to the Supreme Court of the State of Marshall. *Id.* The Supreme Court accepted the case for review. *Id.*

SUMMARY OF THE ARGUMENT

In order to sustain a claim of intrusion upon seclusion, Petitioner must establish that (1) an intentional, unauthorized intrusion occurred into a matter in which he had a reasonable expectation of privacy; (2) that the intrusion occurred in a manner highly offensive to a reasonable person; and (3) that the intrusion caused anguish and suffering. Respondent had a diminished expectation of privacy because Respondent believed it was authorized to search the desktop computer that was owned by Respondent and located on company property. Thus, any expectation of privacy was not objectively reasonable. Further, any intrusion was not highly offensive to a reasonable person because the alleged intrusion was minimal. Respondent owned the computer and no password was needed to access the files. Also, such conduct would not be highly offensive to a reasonable person because under the circumstances, Respondent acted with a legitimate business objective in viewing documents on a computer used by a former employee. Finally, Petitioner fails to state a claim for intrusion upon seclusion because any damage suffered must result from the intrusion. Here, the alleged damage resulted from the publication of information, not the viewing of files on the desktop computer. Thus, Petitioner cannot sustain a claim for intrusion upon seclusion.

To assert a successful claim under the Computer Fraud and Abuse Act ("CFAA"), Petitioner must show that Respondent accessed the social media accounts "without authorization" or "exceeded authorized access." If this requirement is met, Petitioner must establish damage or

loss as a result of the alleged violation. Respondent did not act without authorization because Petitioner provided Respondent with passwords to the social media accounts. Additionally, Respondent did not exceed authorized access because Respondent was still acting within the scope of her employment when interacting with the social media accounts.

Finally, Petitioner failed to satisfy the loss or damage requirement of a CFAA claim. Petitioner did not assert any damage or loss as a result of an inoperable computer, money spent to fix equipment, or any financial burden as a result of a forensic investigation of equipment damage. Additionally, any damage or loss asserted in relationship to lost business opportunities is not compensable under the CFAA. Therefore, Petitioner cannot sustain a claim for a violation of the CFAA.

For Petitioner to assert a successful conversion claim, the property must be tangible or connected to something tangible, and any act must be so serious as to interfere with the right of another to control the chattel. Because Petitioner's social media accounts are not tangible property, nor are they connected to tangible property, they are not subject to a conversion claim. Additionally, Respondent had a good faith belief when it changed the names on the accounts after Petitioner's termination and exit from the company. Petitioner also failed to show any harm was done to her when the name, photo, and personal information was changed. Petitioner also failed to show she incurred any expense when the changes were made to the social media accounts. For these reasons, Petitioner's conversion claim fails.

ARGUMENT

I. THE CIRCUIT COURT PROPERLY DISMISSED PETITIONER'S CLAIM OF INTRUSION UPON SECLUSION BECAUSE PETITIONER HAD A DIMINISHED EXPECATION OF PRIVACY, ANY INTRUSION WAS NOT HIGHLY OFFENSIVE TO A REASONABLE PERSON, AND PETITIONER DID NOT SUFFER UNREASONBLE DAMAGE

The law protects several privacy interests, but there is no absolute right to privacy. *Bank of Ind. v. Tremunde*, 365 N.E.2d 295, 298 (Ill. App. Ct. 1977). As privacy jurisprudence has developed, four distinct causes of action have been recognized that protect one's privacy rights: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness. William Prosser, *Privacy*, 48 Calif. L. Rev. 381, 389 (1960). Petitioner has brought this claim against Respondent, her private employer, under the theory of intrusion upon seclusion.

The rights of private employees within the private employment setting should be carefully outlined. *See Bradley v. Cowles Mag., Inc.*, 168 N.E.2d 64, 65 (Ill. App. Ct. 1960). "Although privacy has been identified

as an interest worthy of some legal protection, courts generally did not give privacy a privileged place or undue weight in the balancing process." *Hill v. Nat'l Collegiate Athletic Assn.*, 865 P.2d 633, 648 (Cal. 1994) (quoting J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 Pepp. L. Rev. 327, 376 (1992)). Under the common law, "intrusion upon seclusion is limited by principles in order to prevent the tort from becoming an all-encompassing, constantly-litigated assertion of an individual right." Robert C. Post, *The Social Foundations of Privacy*, 77 Calif. L. Rev. 957, 1008 (1989). The full context of an employee and employer's relationship must be wholly analyzed before an employee can demand an expectation of privacy. *Acosta v. Scott Labor LLC*, 377 F. Supp. 2d 647, 651 (N.D.Ill. 2005) (citing *O'Connor v. Ortega*, 480 U.S. 709 (1987)).

The State of Marshall has adopted the Restatement (Second) of Torts § 652B (1977) for the tort of intrusion upon seclusion. While Respondent need only refute one element of the claim to prevail, Petitioner's claim fails because she cannot establish:

> (1) that an intentional, unauthorized intrusion occurred into a matter in which he had a reasonable expectation of privacy;
>
> (2) that the intrusion occurred in a manner highly offensive to a reasonable person; and (3)that the intrusion caused anguish and suffering.

Restatement (Second) of Torts § 652B (1977); *See e.g., Cooney v. Chi. Pub. Sch.*, 943 N.E.2d 23, 32 (Ill. App. Ct. 2010). The plaintiff bears the burden to establish each element of intrusion upon seclusion. *Mauri v. Smith*, 929 P.2d 307, 311 (Or. 1996). Plaintiff also bears the burden in proving a defendant's state of mind. *Id.* Because Petitioner failed to establish every element of intrusion upon seclusion, the Circuit Court correctly dismissed Petitioner's claim.

A. Petitioner Had a Diminished Expectation of Privacy Because the Alleged Intrusion Was Authorized

Petitioner had a diminished expectation of privacy concerning files contained on her desktop work computer because Respondent believed its conduct was authorized in order to protect business interests. A claim for intrusion upon seclusion must fail without proof of an intentional and unauthorized invasion. Restatement (Second) of Torts § 652B. An "intentional intrusion" may only be found when an actor "desires to cause an unauthorized intrusion or believes that an unauthorized intrusion is substantially certain to result from committing the invasive act in question." *Mauri*, 929 P.2d at 311. Further, in order for the law to protect an interest in seclusion, the plaintiff must have an actual expectation of seclusion or solitude, and that expectation must be objectively reasonable. *PETA v. Bobby Bersoni, Ltd.*, 895 P.2d 1269, 1279

(Nev. 1995).

1. Respondent believed its conduct was authorized

Petitioner failed to establish the first element because Respondent believed its conduct was authorized. "[A]n actor commits an intentional intrusion only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989). Even when a court finds an intrusion was intentional, if a defendant can demonstrate he subjectively believed he had legal or personal permission, a claim for intrusion upon seclusion must fail. *Id.*

In *Sitton v. Print Direction, Inc.*, an employee's personal laptop, that was used at work, was searched by his employer. 718 S.E.2d 532 (Ga. Ct. App. 2011). The employer suspected the employee of running a competing business using customer information from the employer's files. *Id.* at 537. The employer accessed the employee's laptop in order to search his e-mails, which proved the suspicions were true. *Id.* at 535. The *Sitton* Court held that the employer's review of the employee's email on his personal laptop was not an unreasonable intrusion into the employee's seclusion or solitude. *Id.* at 537. The court stated the employer's activity was "reasonable in light of the situation" because the employee's personal computer was used at work, contained company owned records, and brought onto company property. *Id.*

As the owner of the desktop computer and all of the company information it contains, Respondent reasonably believed that it had the legal or personal permission to view files found on the desktop computer after Petitioner was terminated. Like *Sitton*, the desktop computer was not only used at work, it remained on company property. (R. at 1). Furthermore, Petitioner herself synced company information from mobile devices to the desktop computer. *Id.* Thus, Respondent's actions were reasonable in light of the situation.

2. Petitioner had a diminished expectation of privacy that was not objectively reasonable

Petitioner's subjective expectation of privacy alone, under the circumstances of this case, is insufficient to sustain a claim of intrusion upon seclusion. Even if Petitioner had a subjective expectation of privacy in her desktop work computer, this belief was not objectively reasonable. "No community could function if every intrusion into the realm of private action, no matter how trivial or slight gave rise to a cause of action for invasion of privacy." *Hill*, 865 P.2d at 660.

Petitioner knew that her laptop was synced to her company owned desktop computer at Respondent's office; thus, Petitioner should have taken reasonable measures to protect such information upon her termi-

nation. Consequently, any subjective expectation of privacy Petitioner held was not objectively reasonable. Further, to sustain a claim for intrusion upon seclusion, Petitioner must allege an invasion of privacy. *Busse v. Motorola, Inc*., 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004). Courts have recognized that "the right of privacy is not an absolute right, but a right that is qualified by the circumstances and the rights of others." *Wilcher v. City of Wilmington*, 60 F. Supp. 2d 298, 302 (D. Del. 1999). A private employee's professed expectation of privacy must be "assessed in the context of the particular employment relationship." *O'Connor*, 480 U.S. at 717.

Two requirements are necessary in making a determination of a reasonable expectation of privacy: (1) "'whether the individual, by conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private;'" and (2) "'whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable.'" *Clements-Jeffrey v. City of Springfield, Ohio*, 810 F. Supp. 2d 857, 865 (S.D. Ohio 2011) (quoting *United States v. King*, 227 F.3d 732, 743–44 (6th Cir. 2000)). While the "first factor is subjective and involves a question of fact; the second factor is objective and involves a question of law." *Clements-Jeffrey*, 810 F. Supp. 2d at 865 (citing *United States v. Welliver*, 976 F.2d 1148, 1151 (8th Cir. 1992)). Without proof of an objectively reasonable expectation of privacy, a claim of intrusion upon seclusion cannot succeed.

In *United States v. Angevine*, the Tenth Circuit rejected an employee's claim that he had a reasonable expectation of privacy in an office computer, after his company-owned computer was searched. 281 F.3d 1130 (10th Cir. 2002). The Court highlighted the fact that "[a]lthough ownership of the item[s] seized is not determinative, it is an important consideration in determining the existence and extent of a defendant's Fourth Amendment interests." *Id.* at 1134 (quoting *United States v. Erwin*, 875 F.2d 268, 270–71 (10th Cir.1989)).

Factors that contributed to the Court's finding that the employee had no reasonable expectation of privacy included the employer's ownership of the equipment, the lack of immediate control the employee had of his data, and the employee's failure to take any steps to maintain privacy in his computer. *Id.* Analogous to *Angevine*, Respondent owned the equipment allegedly intruded upon. After Petitioner's termination, Petitioner took her personal cell phone and tablet, leaving the desktop computer; thus, Petitioner lacked immediate control of the data in her desktop. (R. at 2). Petitioner further made no attempt to remove the data from her desktop upon her termination knowing personal information was located on the computer. Therefore, Petitioner had no reasonable expectation of privacy in the desktop computer.

B. The Alleged Intrusion was Not Highly Offensive to a Reasonable Person Because the Any Intrusion was Minimal, Respondent's Act was Reasonable Under the Circumstances, and Respondent Acted with a Legitimate Objective

Even if the court determines that Petitioner's expectation of privacy was reasonable, Petitioner is still required to prove that the alleged intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B. "The law of privacy is not intended for the protection of any shrinking soul who is abnormally sensitive about such publicity." William Prosser, *Privacy*, 48 Cal. L. Rev. 381, 397 (1960).

An offensive intrusion requires an unreasonable manner of intrusion or an intrusion for an unwarranted purpose. *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1069 (Colo. App. 1998). It is the degree of intrusion that determines whether such intrusion is offensive. See *Werner v. Kliewer*, 710 P.2d 1250 (Kan. 1985). Liability "depends upon some type of highly offensive prying into the physical boundaries or affairs of another person." *Lovgren v. Citizens First Nat'l Bank*, 534 N.E.2d 987, 989 (Ill. 1989).

> While what is 'highly offensive to a reasonable person' suggests a standard upon which a jury would properly be instructed, there is a preliminary determination of 'offensiveness' which must be made by the court in discerning the existence of a cause of action of intrusion.

Bauer v. Ford Motor Credit Co., 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001) (quoting *Miller v. Nat'l Broad. Co.*, 232 Cal.Rptr. 668, 678 (Cal. Ct. App. 1986)); *see Froelich v. Werbin*, 548 P.2d 482, 482-83 (Kan. 1976) (evidence was insufficient as a matter of law to establish that an invasion of the plaintiff's right of privacy would be highly offensive to a reasonable person); *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 877 (8th Cir. 2000) (concluding as a matter of law that revealing medical information did not rise to the level of highly offensive conduct).

Factors for the court to consider include, "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." *Bauer*, 149 F. Supp. 2d at 1109. Petitioner failed to assert sufficient facts to support a claim that Respondent's conduct was highly offensive.

1. The alleged intrusion was minimal

Respondent's conduct was not highly offensive because the alleged intrusion was *de Minimis*, when a court finds that the degree of the intrusion was minimal, a claim of intrusion upon seclusion must fail. *Id.* Liability for a claim of intrusion upon seclusion occurs as a result of the

"particular method of obtaining information, not the content of the information obtained, or even the use put to the information by the intruder following the intrusion." *Koeppel v. Speirs*, 808 N.W.2d 177, 180 (Iowa 2011).

The degree of intrusion into the desktop computer was minimal for several reasons. First, the files were accessed after Petitioner's termination and exodus from the company. (R. at 2-3). Additionally, the method of intrusion was minimal because the record does not indicate that a password was necessary to access the files. Finally, Petitioner took no steps to remove or protect the information. Therefore, any intrusion was minimal.

2. The context, conduct, and circumstance of the alleged intrusion were not "highly offensive"

Respondent's conduct was not an exceptional kind of prying and, therefore, is not "highly offensive." The illustrations in the comments to the Restatement (Second) of Torts § 652B suggest that the conduct must be an exceptional kind of prying into another's private affairs. *See* Restatement (Second) of Torts § 652B cmt. b. (offering the following examples: (1) taking the photograph of a woman in the hospital with a "rare disease that arouses public curiosity" over her objection, and (2) using a telescope to look into someone's upstairs bedroom window for two weeks and taking "intimate pictures" with a telescopic lens).

Further, release of information does not constitute highly offensive conduct when that information could otherwise have been obtained by proper means. *Fletcher*, 220 F.3d at 876. For example, in *Fletcher v. Price*, the defendant corporate manager could have employed proper means to discover whether plaintiff actually had an infection when she was fired. *Id.* However, the manager's decision to bypass proper channels in obtaining information from plaintiff's doctor was not highly offensive conduct. *Id.*

Examining the context, conduct, and circumstances, Respondent's actions were not highly offensive, because Respondent did not utilize exceptional types of prying. Respondent accessed a computer, located on company property, not a private residence. (R. at 1). The record does not indicate that Respondent utilized any tactics for circumventing a password on the desktop computer. Upon termination, Petitioner gave no indication to Respondent that the desktop computer was off limits. Moreover, it is unreasonable to suggest that an employer cannot interact with a company owned computer utilized by a former employee.

Despite the fact that the information was accessed from a file labeled "personal" on the desktop computer, this information was supplemented through an individual's private investigation. (R. at 2). The information shared to the public regarding Hanoi Labor, Co.'s use of

child labor and dismal work practices was found pursuant to an independent investigation, not the information found on the desktop computer. Additionally, upon Petitioner's launch of the Threads clothing company, details of her suppliers would have been discoverable by the public. Even if Respondent did in fact bypass proper channels for discovering information, that alone does not make the conduct highly offensive.

3. Respondent had a legitimate objective

If a "justification is apparent and is plausible on its face, a complainant who hopes to survive a motion to dismiss must do more than suggest conclusory that the [defendant] has an improper or insufficient motivation." *Berner v. Delahanty*, 129 F.3d 20, 26 (1st Cir. 1997).

Petitioner's assertion that Respondent's search of the desktop computer involved insidious motivation is not sufficient to support a claim for intrusion upon seclusion. It is apparent and plausible that Respondent had a reasonable business motivation to access a computer that was not only owned by Respondent but was located on company property. Further, Petitioner's assertion that Respondent's disclosure was out of competition is flawed. It is plausible that the revelation of Hanoi Labor, Co.'s practice of utilizing child labor may have been motivated by an overarching desire to improve social welfare. According to the record, Respondent has a longstanding reputation in the industry as a responsible company, not one utilizing insidious business practices. (R. at 1). Thus, Petitioner's conclusory suggestion that Respondent had an ill motive for disclosing the business plans with Hanoi Labor, Co. cannot support a claim for intrusion upon seclusion.

C. Petitioner's Allegations of Anguish and Suffering Did Not Result from the Alleged Intrusion.

Petitioner's alleged damage to her reputation after it was revealed to the public of Petitioner's involvement with Hanoi Labor, Co. was not the result of Respondent's viewing of Petitioner's files located on her desktop work computer. "The basis of the tort is not publication or publicity. Rather, the core of this tort is the offensive prying into the private domain of another." *Lovgren*, 534 N.E.2d at 989; Restatement (Second) of Torts § 625B cmt. a, b.

A plaintiff must prove the actual intrusion caused anguish and suffering, because "injury is not presumed." *Schmidt v. Ameritech Illinois*, 768 N.E.2d 303, 316 (Ill. App. Ct. 2002) (quoting Restatement (Second) of Torts § 652H(b)). A plaintiff cannot sustain a claim for intrusion where the resulting anguish and suffering flow from publication or some other act rather than from the intrusion. *Doe*, 972 P.2d at 1066. The dissemination of what is learned in an intrusion is not itself an in-

trusion upon seclusion. *Barker v. Manti Telephone Co*., No. 2:06-CV-00812TCSA, 2009 WL 47110, *4 (D. Utah Jan. 6, 2009). Injury that results from the publication of private information should be brought under the tort of public disclosure of private facts, or false light, not intrusion upon seclusion. See *Lovgren*, 534 N.E.2d at 989.

In *Thomas v. Pearl*, the employer secretly recorded employee's phone conversation while at work. 998 F.2d 447, 451 (7th Cir. 1993). The Court found that although this was an intrusion, it did not cause the employee harm. *Id*. at 452. It was only after the conversation was published to the public that the employee experienced any harm. *Id*. Thus, the employee's harm resulted from the publication, not the intrusion, and could not sustain a claim for intrusion upon seclusion *Id*.

Here, Petitioner cannot prove that her anguish and suffering resulted from the intrusion itself. Like *Thomas*, any damage to Petitioner's reputation did not occur simply from Respondent's conduct of viewing files found on her desktop computer. Rather, the harm Petitioner alleges was the result of having such information published. Petitioner cannot point to any facts in the record in order to demonstrate that anguish and suffering occurred from the intrusion; thus, Petitioner cannot sustain her claim for intrusion upon seclusion. As a matter of law, Petitioner's claim must fail because Petitioner had a diminished expectation of privacy, the alleged intrusion was not highly offensive to a reasonable person, and Petitioner did not plead sufficient facts to suggest she suffered unreasonable damage.

II. THE CIRCUIT COURT PROPERLY DISMISSED PETITIONER'S CLAIM OF A VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT BECAUSE RESPONDENT NEITHER ACCESSED A COMPUTER WITHOUT AUTHORIZATION NOR EXCEEDED AUTHORIZED ACCESS, PETITIONER DID NOT SUFFER ANY COGNIZABLE DAMAGE OR LOSS, AND IF THE COURT FINDS THE STATUTE TO BE AMBIGUOUS, THE RULE OF LENITY APPLIES

The Computer Fraud and Abuse Act ("CFAA") was passed in 1984 as a means to protect classified information, financial records, and credit information primarily on governmental and financial institution computers. Samantha Jensen, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 Hamline L. Rev. 81, 88 (2013). Historically, the CFAA has its origins as a criminal statute, with the goal of protecting against computer hackers. *Poller v. BioScrip, Inc*., 974 F. Supp. 2d 204, 232 (S.D.N.Y. 2013); *see also Dresser- Rand Co. v. Jones*, 957 F. Supp. 2d 610, 613 (E.D. Pa. 2013). According to the 1984 House Committee Report, "the conduct prohibited is analogous to that of breaking and entering rather than using a computer (similar to the use of a gun) in committing the offense." *Dresser-Rand*, 957 F.Supp.2d

at 613. Through the years, however, the statute has been expanded to include a limited private right of action. *Poller*, 974 F.Supp.2d at 232.

To assert a successful claim under the CFAA, several elements must be satisfied. The Act provides:

> [w]hoever knowingly accesses a computer without authorization or exceeding authorized access and by means of such conduct obtains personal information commits the offense of a fraud and related activity in connection with computers.

State of Marshall Computer Fraud and Abuse Act, ¶ 1030(a) (2008). The statute continues by stating, "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages or injunctive relief or other equitable relief." *Id.*

Petitioner failed to state a claim under the CFAA because Respondent did not access a computer "without authorization" or "exceeding authorized access." Additionally, Petitioner did not suffer any "damage" or "loss" as a result of Respondent's conduct. Finally, because the CFAA is both a criminal and civil statute, the rule of lenity applies protecting the public from unreasonable and unwarranted criminal sanctions.

A. Respondent Neither Accessed a Computer Without Authorization nor did Respondent Exceed Authorized Access

The case law involving a CFAA claim revolves around interpretations of the phrases "without authorization" and "exceeding authorized access." When engaging in statutory interpretation, courts look no further than the plain language contained in unambiguous statutes. *Robinson v. Shell Oil, Co*., 519 U.S. 337 (1997). Certain courts have chosen to adopt a narrow view of these phrases, reasoning that any other interpretation is unpersuasive and inappropriate. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-1135 (9th Cir. 2009). Therefore, applying a narrow interpretation of these phrases Respondent did not access the accounts without authorization or exceeding authorized access.

1. Petitioner gave respondent passwords to the accounts

While the CFAA contains no definition for "without authorization" several courts have translated the phrase to mean "without any permission." *Amphenol Corp. v. Paul*, 993 F. Supp. 2d 100, 109 (D. Conn. 2014) (citing *LVRC Holdings LLC*, 581 F.3d at 1130-1131). Therefore, a person who accesses a computer without authorization has no rights to use the computer. *LVRC Holdings LLC*, 581 F.3d at 1133. Specifically, courts have held that, "a person uses a computer 'without authoriza-

tion'… when the person has not received permission to use the computer for any purpose … or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* This illustrates that an employee who is given authorization, albeit limited, does not access a computer without authorization.

In *LVRC Holdings, LLC v. Brekka*, an employee, Brekka, was hired as a consultant for a residential treatment center. *Id.* at 1129. Brekka often traveled for the business and utilized a work computer provided by the company. *Id.* Brekka was given a login and password for the company email in order to access work files remotely. *Id.* After unsuccessful business negotiations, Brekka ceased working for LVRC. *Id.* at 1130. Upon leaving, Brekka left his work computer at LVRC. *Id.* Subsequently, LVRC discovered that Brekka continued to access company statistics and information remotely. *Id.* LVRC brought a CFAA action alleging that Brekka was in violation when he emailed documents to his personal account and continued to access the account post-employment. *Id.* The Court held that no CFAA violation occurred because Brekka had been given the initial authorization to access files remotely. *Id.* The Court highlighted the fact that when a person is given authorization to use a computer, subject to certain limitations, the person remains authorized even if they violate the limitations. *Id.*

Like Brekka, Respondent was given initial authorization to access the social media accounts. (R. at 1). Petitioner's verbal limitation of authorization is irrelevant because Petitioner gave Respondent a password for the accounts. Not only did Respondent receive permission to use the account, Respondent created the account for Petitioner. (R. at 1). Finally, at no point did Petitioner attempt to rescind permission to access the accounts. Petitioner's contention that Respondent did not have authorization is contradicted by the fact that Petitioner utilized Respondent's efforts and labor to maintain the accounts. Thus, Respondent did not act without authorization in violation of the CFAA.

2. Respondent was entitled to obtain and alter the social media accounts as a part of employment

The phrase "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter." *Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc.*, 953 F. Supp. 2d 1290, 1295 (S.D. Ga. 2013). A potential violation of the CFAA occurs when a person accesses a computer with permission, but goes on to access information that "falls outside the bounds of [their] approved access." *Dresser-Rand Co.*, 957 F.Supp.2d at 617. However, improper use of information that is validly accessed falls outside the scope of the CFAA. *Id.*

In *Dresser-Rand Co. v. Jones*, an employee, Jones, worked as a manager for a technology corporation. *Id.* at 611. Jones began performing work for another company and eventually resigned from his position at Dresser-Rand. *Id.* Dresser-Rand's forensic computer expert found that Jones downloaded Dresser-Rand files onto external storage devices prior to resignation. *Id.* Additionally, Jones deleted everything stored on his work computer. *Id.* at 612. The Court found that no CFAA violation occurred because Jones was given a password and login to access the deleted files. *Id.* at 620. The Court highlights the fact that Jones alleged misuse of files may have remedies under other laws, but application of the CFAA is improper. *Id.*

Like in *Dresser-Rand*, Respondent had been given a password to log in to the social media accounts. (R. at 1). Furthermore, the administrative assistant who altered the social media accounts was still acting within the scope of her employment, at the direction of her new boss. (R. at 2). The social media accounts were changed because of the instruction from Petitioner's replacement, Valentini. *Id*. The record does not indicate that Petitioner provided the administrative assistant any instruction regarding the social media accounts upon her termination. Since the administrative assistant was still acting within the scope of her employment she did not exceed authorized access as defined by the CFAA.

B. Petitioner Failed to Assert any Cognizable "Damage" or "Loss" as a Result of Respondent's Interaction with the Desktop Computer or Social Media Accounts.

To recover compensatory damages under the CFAA, a plaintiff must show either damage or loss as a result of the violation. State of Marshall Computer Fraud and Abuse Act, ¶ 1030(a). This provision of the CFAA is meant to protect against damage to data, not an employee who attains confidential information. *SBS Worldwide, Inc. v. Potts*, No. 13 C 6557, 2014 WL 499001, at *8 (N.D. Ill. Feb. 7, 2014).

Under the CFAA, "damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." *Id*. Courts have determined that damage may include the "destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any 'diminution in the completeness or usability of the data on a computer system.'" *Id*. However, copying, emailing, or printing electronic files from a computer is not sufficient to assert a CFAA claim. *Id*.

Alternatively, "loss" is defined in the CFAA as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost

incurred, or other consequential damages incurred because of interruption of service." *Eagle v. Morgan*, No. CIV.A. 11-4303, 2012 WL 4739436, at *8 (E.D. Pa. Oct. 4, 2012). Future lost revenue, however, is not compensable under the CFAA. *Id.* For instance, a plaintiff alleging a loss of business will not qualify as a "loss" under the CFAA. *Id.* Certain courts have allowed a plaintiff to satisfy the "loss" portion of the statute simply by alleging costs reasonably incurred in response to an alleged CFAA offense, even if it is ultimately found that no damage occurred. Other courts require that there be damage to a computer or computer system before a plaintiff can show a "loss" under the CFAA. *SBS Worldwide*, No. 13 C 6557, 2014 WL 499001, at *9.

In *Eagle v. Morgan*, the plaintiff, Eagle, worked for Edcomm, a banking education company. No. CIV.A. 11-4303, 2012 WL 4739436, at *1. While employed with Edcomm, Eagle created a LinkedIn account. *Id.* Eagle utilized the account to "promote [her employer's] banking education services; foster her reputation as a businesswoman; reconnect with family, friends, and colleagues; and build social and professional relationships." *Id.* Another individual, Elizabeth Sweeney, helped Eagle maintain the account and had access to the account password. *Id.* After Eagle was terminated from employment, she was no longer able to access her LinkedIn account. *Id.* Edcomm utilized Eagle's login credentials, changed the password, and changed Eagle's account to display a new employee's name and photograph. *Id.* Eagle brought a claim under the CFAA alleging that she had suffered damages trying to regain control over the account, she incurred legal fees trying to regain control of the account, that her reputation was harmed by Edcomm's conduct, that the value of the account decreased, and that Eagle missed out on professional business opportunities as a result of her impeded access. *Id.*

The Court held that none of Eagle's allegations were sufficient to create a "genuine issue of material fact as to the existence of cognizable damages under the CFAA." *Id.* at *5. The Court highlighted the fact that the plaintiff did not claim any lost money because of an inoperable computer or because she spent money to fix a computer. *Id.* The Court found that Eagle's alleged "loss of business opportunities" were "simply not compensable under the CFAA." *Id.* Additionally, the Court noted that Eagle provided no effort to quantify such "damage" and as result any conclusion on this point would have the court "rely on pure conjecture." *Id.* at *6. Ultimately, the Court declined to do so, finding that Eagle failed to assert a CFAA claim. *Id.*

Like the plaintiff in *Eagle*, Petitioner failed to claim any damage or loss because of an inoperable computer. The desktop at issue belonged to Respondent and has suffered no damage as a result of Respondent's conduct. Additionally, Petitioner has not asserted any facts stating that money was spent trying to fix the social media accounts. While the Peti-

tioner may assert a loss of business contacts associated with the social media accounts, this "loss of business opportunities" is not compensable under the CFAA. Finally, Petitioner has not provided any quantification for the alleged loss or damage. Therefore, Petitioner has failed to assert any loss or damage cognizable under the CFAA.

C. The Application of the Rule of Lenity is Necessary to Avoid Exposing the Public to Unreasonable Criminal Liability Without Notice.

If the statute contains ambiguous language, courts may consider information beyond the text of the statute. *De Buono v. NYSA-ILA Med. & Clinical Servs. Fund*, 520 U.S. 806, 813-814 (1997). It is important to note that the CFAA is primarily a criminal statute, creating criminal liability as a result of violations. *LVRC Holdings LLC*, 581 F.3d at 1134. Despite the CFAA's civil application, decisions stemming from a civil violation are equally applicable in the criminal context. *Id.* Courts must apply the rule of lenity to ambiguous criminal statutes. *Id.*

The rule of lenity requires that ambiguous criminal statutes be resolved in favor of lenience, so as to not impose unexpected burdens on defendants. *Id.* A "court confronted with two rational readings of a criminal statute, one harsher than the other, [must] choose the harsher only when Congress has spoken in clear and definite language." *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008); *Pasquantino v. United States*, 544 U.S. 349, 383 (2005).

> Applying the rule of lenity, [courts have] warned that the broader statutory interpretation would delegate to prosecutors and juries the inherently legislative task of determining what type of ... activities are so morally reprehensible that they should be punished as crimes and would subject individuals to the risk of arbitrary or discriminatory prosecution and conviction. By giving that much power to prosecutors, we're inviting discriminatory and arbitrary enforcement.

United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012). This rule stems from the principle that "no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *LVRC Holdings LLC*, 581 F.3d at 1135. At its core, the rule of lenity is rooted in the requirement of providing the public with notice before being subject to criminal sanctions. *Id.*

In *Matot v. CH*, the plaintiff brought a CFAA action after several students allegedly created social media accounts with the plaintiff's name and likeness. 975 F. Supp. 2d 1191 (D. Or. 2013). The plaintiff also alleged that the students invited other students to communicate with the false accounts. *Id.* The Court noted that the CFAA is focused on hacking rather than creating a "sweeping internet-policing mandate." *Id.* at 1195. Additionally, the Court stated that lying, duplicate ac-

counts, and fake accounts are common on social media websites. *Id.* at 1196. The Court held that a CFAA claim was precluded because imposing liability in such a situation involving social media would expose millions of unsuspecting individuals to criminal liability; thus, the rule of lenity applied. *Id.*

As was highlighted in *Matot*, imposing liability on Respondent would expose the general public to criminal sanctions without notice. While this case involves civil liability, the result of litigation can be applied in the criminal context. If Respondent is found to be civilly liable, Respondent will be potentially exposed to unreasonable and unwarranted criminal sanctions. Such an application of the CFAA is precluded by the rule of lenity so as to protect unwarned citizens, like Respondent.

As a matter of law, Petitioner's claim must fail because Respondent neither accessed a computer without authorization nor did Respondent exceed authorized access, Petitioner failed to assert any cognizable damage or loss as a result of Respondent's actions, and the rule of lenity applies protecting the public from unreasonable criminal sanctions.

III. THE CIRCUIT COURT PROPERLY DISMISSED PETITIONER'S CLAIM OF CONVERSION BECAUSE SOCIAL MEDIA ACCOUNTS ARE INTANGIBLE PROPERTY AND RESPONDENT DID NOT EXERT AN INTENTIONAL EXCERICSE OF DOMINION OR CONTROL OVER THE SOCIAL MEDIA ACCOUNTS WHICH SO SERIOUSLY INTERFERED WITH A RIGHT TO CONTROL THE ACCOUNTS.

The common law tort of conversion began as a remedy for the "wrongful taking of another's lost goods." *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003). Traditionally, conversion only applied to tangible property. *Id*. However, some courts now recognize the conversion of intangible property, only if the property is connected with a tangible object. *Id*. Even if a plaintiff meets the threshold requirement that property is tangible, a plaintiff must still demonstrate the necessary elements of a conversion claim. Because social media accounts are not tangible property, nor are they connected with tangible property and Petitioner failed to establish every element of conversion, the Circuit Court properly dismissed Petitioner's claim.

A. There is No Basis for a Conversion Claim Because Social Media Accounts are Not Tangible Property Nor Are They Connected With Tangible Property.

Several cases have held that "an action for conversion lies only for personal property which is tangible, or at least represented by or con-

nected with something tangible." *Joe Hand Promotions, Inc. v. Lynch*, 822 F. Supp. 2d 803, 806 (N.D. Ill. 2011); *See generally Michael v. Bell*, No. 11-CV-4484, 2012 WL 3307222 (N.D. Ill. Aug. 13, 2012); *Film & Tape Works, Inc. v. Junetwenty Films, Inc*., 856 N.E.2d 612, 624 (Ill. App. Ct. 2006). Social media accounts, such as LinkedIn, are not tangible property, "but rather an intangible right to access a specific page on a computer." *Eagle*, No. CIV.A. 11-4303, 2013 WL 943350, at *10.

In limited circumstances, intangible property may be the subject of a conversion claim if connected with something tangible.

> [I]ntangible rights can be converted when connected with something tangible by establishing that the connection must be to a tangible document, such as 'promissory notes, bonds, bills of exchange, share certificates, and warehouse receipts.

Joe Hand Promotions, Inc., 822 F. Supp. 2d at 808 (quoting *Film and Tape Works, Inc*., 856 N.E.2d at 624). To convert intangible property into tangible property, it "must have some value in terms of confidentiality, trade secrets, proprietary business information or the like." *Rubloff Dev. Grp., Inc. v. SuperValu, Inc*., 863 F. Supp. 2d 732, 751 (N.D. Ill. 2012). Some courts have held that intangible interest, such as customer lists, can be the basis of a conversion claim. *Welco Electronics, Inc. v. Mora*, 166 Cal. Rptr. 3d 877, 885 (Cal. Ct. App. 2014), reh'g denied (Feb. 19, 2014). However, social media accounts are a type of intangible property that is inappropriate for a conversion claim. *Eagle*, No. CIV.A. 11-4303, 2013 WL 943350, at *10.

As previously discussed in *Eagle*, the plaintiff, created a LinkedIn account for herself using her company e-mail address, gave the password to an unknown number of employees, and was fired roughly two years after she created the account. *Id*. at 1-3. Upon Eagle's termination, employees changed the password to her LinkedIn account, blocking her access. *Id* at 3. The Court held that Eagle was unable to state a claim of conversion. *Id*. at 10. The Court stated, "items such as software, domain names, and satellite signals are intangible property not subject to a conversion claim." *Id*. *See, e.g., Apparel Bus. Sys. v. Tom James Co*., No. Civ.A. 06-1092, 2008 WL 858754, at *18–19 (E.D. Pa. Mar. 28, 2008) ("Software is not the kind of property subject to a conversion claim"); *DirecTV, Inc. v. Frick*, No. Civ.A. 03–6045, 2004 WL438663, at *2–3 (E.D. Pa. Mar. 2, 2004) (finding that satellite signals constitute intangible property which cannot be converted under Pennsylvania law); *Famology.com Inc. v. Perot Sys. Corp*., 158 F. Supp. 2d 589, 591 (E.D. Pa. 2001) (holding that domain names are not the type of tangible property that may be converted).

Like the social media account in *Eagle*, LinkedIn and Twitter cannot be the basis for Petitioner's conversion claim, because social media is intangible property. Petitioner has not asserted that the social media accounts are in any way connected to tangible property such as bills of

exchange, bonds, or promissory notes. Additionally, both the LinkedIn and Twitter page were created by administrative assistant, Bennett, for Petitioner's use in promoting and communicating with the public for U.S. Apparel. R. at 1.

Petitioner provided Bennett with the account passwords. *Id.* Since the two accounts were created to interact with the public, and because Bennett had the passwords, these accounts did not have value in terms of confidentiality, trade secrets, proprietary business information or the like. Petitioner did use the Twitter account to interact with customers. R. at 1-2. However, these were U.S. Apparel customers, not exclusive customers of Petitioner; therefore, this would not qualify as Petitioner's "customer list." Because these social media accounts are intangible property, and have not been converted into tangible property, Petitioner failed to state a claim of conversion.

B. Respondent Did Not Interfere with Any Right to Control the Social Media Accounts, Nor Was any Alleged Interference So Serious As to Warrant a Claim for Conversion

Even if the court finds that the Twitter and LinkedIn Accounts are the type of intangible property subject to a conversation claim, Petitioner fails to meet the necessary conditions for a conversion claim. According to the State of Marshall's adoption of the Restatement (Second) of Torts, to assert a successful conversion claim there must be an "intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel." Restatement (Second) of Torts § 222A (1965).If the court determines that a person exercised dominion or control over property, the court must then examine several factors to measure the seriousness of such conduct. *Id.* Plaintiff bears the burden of proving the necessary elements for a successful conversion claim. *First Fin. Co. v. Ross*, 221 N.E.2d 37, 39 (Ill. App. Ct. 1966). Petitioner failed to provide facts necessary to assert a conversion claim because Petitioner held no right to the social media accounts and did not demonstrate that the alleged interference was so serious as to require Respondent to pay for the property.

1. Petitioner held no property rights to the social media accounts

While Petitioner accessed company information using her personal cell phone and tablet, she did not have specific property rights because these accounts were Respondent's property. Certain courts have stated that a company may have property rights in social media accounts with their name attached thereto. *See PhoneDog v. Kravitz*, No. C 11-03474 MEJ, 2011 WL 5415612, at *1 (N.D. Cal. Nov. 8, 2011). Therefore, because these accounts were the property of Respondent, Petitioner had

no legal right to them.

In *PhoneDog v. Kravitz*, the defendant, Kravitz, began working for PhoneDog as a product reviewer and blogger. No. C 11-03474 MEJ, 2011 WL 5415612, at *1. Kravitz maintained a Twitter account named "@PhoneDog_Noah." *Id.* Using this account, Kravitz posted information promoting PhoneDog's services. *Id.* Kravitz subsequently ended his employment with PhoneDog. *Id.* PhoneDog requested that Kravitz relinquish the account, but he instead changed the account name to "@noahkravitz" and continued to use the account. *Id*. As a result, PhoneDog brought an action for conversion against Kravitz. *Id*. Kravitz urged the Court to dismiss the conversion claim reasoning that PhoneDog did not have any right to possess the account. *Id*. at *9. The Court held that PhoneDog adequately alleged a right to possess the social media account. *Id.*

Like *PhoneDog*, Respondent, rather than Petitioner, maintains a right to possess the social media accounts. The social media accounts utilized by Petitioner were used to post information related to Respondent's business activities and contained Respondent's name. R. at 1-2. Furthermore, similar to *PhoneDog*, Petitioner did not create the social media accounts. Instead, this task was given to an administrative assistant. R. at 1. As a result, any property rights to the social media accounts lie with Respondent, not Petitioner.

2. Respondent acted in good faith, did no harm to the social media accounts, and caused no expense to petitioner

Even if the court finds that Petitioner did have property rights in the social media accounts, the Respondent did not so seriously interfere with these rights so as to constitute a claim for conversion. To determine the seriousness of the interference and the justice of requiring the actor to pay the full value, the court must examine:

> (a) the extent and duration of the actor's exercise of dominion or control;
>
> (b) the actor's intent to assert a right in fact inconsistent with the other's right of control; (c) the actor's good faith;
>
> (d) the extent and duration of the resulting interference with the other's right of control; (e) the harm done to the chattel;
>
> (f) the inconvenience and expense caused to other.

Restatement (Second) of Torts § 222A (1965).Here, Respondent acted in good faith, did no harm to the accounts, and caused no expense to Petitioner. Respondent acted in good faith when changing the names associated with the LinkedIn and Twitter accounts. The social media accounts were changed only after Petitioner's termination and exit from the company. R. at 2-3. The administrative assistant who changed the

accounts did so specifically as a task given on the job. R. at 3. The administrative assistant did not change the accounts on her own volition; rather, she acted with permission from Petitioner's direct replacement. *Id.* The Petitioner fails to allege any facts demonstrating that the administrative assistant acted out of spite or in bad faith when modifying the social media accounts to reflect a change in leadership.

Respondent did no harm to the Twitter and LinkedIn accounts by changing the name attached thereto. Since the only information removed from the accounts was a name, photo, and personal information, Petitioner failed to show that any harm was done. R. at 3. Petitioner likely has access to her photo and personal information; therefore none of this information was lost. Since the other information contained in the accounts remained unchanged, the accounts suffered no harm.

Since the information contained in the social media accounts remains unchanged, Petitioner has failed to show that Respondent caused Petitioner any expense. Due to the public nature of social media, the posts, connections, and followers attached to these accounts are likely viewable by anyone, Petitioner included. Petitioner can still view the accounts and find any past connections or followers for future business opportunities. Furthermore, Petitioner failed to allege any facts suggesting that she was forced to pay for any sort of damage mitigation or investigation as a result of Respondent's actions. Therefore, Petitioner has failed to assert any facts indicating that Respondent caused Petitioner any expense.

As a matter of law, Petitioner's claim for conversion must fail because social media accounts are intangible property and Respondent did not exert an intentional exercise of dominion or control over the social media accounts that so seriously interfered with a right of control.

CONCLUSION

Respondent respectfully requests the judgment of the Circuit Court of Nashville County be affirmed granting Respondent's motion to dismiss the claims of intrusion upon seclusion, a violation of the CFAA, and conversion.

Dated: October 1, 2014.

Respectfully submitted,

/s/_____
Attorneys for the Respondent