UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 2 Article 5

2014

The Thirty-Third Annual John Marshall Law School International Moot Court Competition in Information Technology and Privacy Law: Brief for the Petitioner, 31 J. Marshall J. Computer & Info. L. 251 (2014)

Amany Awad

Kelly O'Neill

Arlo Walsman

BRIEF FOR PETITIONER

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

AMANY AWAD

KELLY O'NEILL

ARLO WALSMAN

QUESTIONS PRESENTED

I. Whether Shapiro states a valid claim for intrusion upon seclusion against U.S. Apparel where Bennett, as U.S. Apparel's agent, accessed personal files within Shapiro's workplace computer that was located in her private office, and where U.S. Apparel then held a press conference revealing the contents of Shapiro's personal files to the public.

II. Whether Shapiro states a valid claim for violation of the State of Marshall Computer Fraud and Abuse Act where Respondent instructed Bennett to access Shapiro's personal files and subsequently broadcast that personal information and where Respondent instructed Bennett to access and alter Shapiro's social media accounts, all without Shapiro's authorization or by exceeding authorized access.

III. Whether Shapiro states a valid claim for conversion where her accounts constitute valuable, convertible property that she establishes she owned and with which the Respondent intentionally interfered when the Respondent had Bennett change the passwords, effectively locking Shapiro out of her social media accounts.

STATUTORY PROVISIONS

The Restatement (Second) of Torts § 652B (1977) provides:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The Restatement (Second) of Torts § 222A (1965) provides:

> (1) Conversion is 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.
>
> (2) In determining the seriousness of the interference and the justice of requiring the actor to pay the full value, the following factors are important:
>
> > (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 the other.

The State of Marshall's Computer Fraud and Abuse Act, ¶ 1030(a) (2008), provides in part:

> 1. Whoever 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.
>
> 2. Any 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 dam-ages or injunctive relief or other equitable relief.

STANDARD OF REVIEW

To survive a Rule 12(b)(6) motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). "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." *Id*. Determining whether a complaint states a plausible claim is a context-specific task that "requires the reviewing court to draw on its judicial experience and common sense." *Id*. at 679. "When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." *Id*.

A trial court's grant of a 12(b)(6) motion to dismiss is a question of law that is reviewed de novo. *Herring v. United States*, 424 F.3d 384, 389 (3d Cir. 2005); *Kane Enterprises v. MacGregor (USA) Inc*., 322 F.3d 371, 374 (5th Cir. 2003).

STATEMENT OF THE CASE

Jane Shapiro ("Shapiro") founded U.S. Apparel, a pre-teen and teen clothing company. R. at 1. She served as its chief executive officer ("CEO") for ten years. R. at 1. She often worked remotely while traveling and attending meetings on behalf of U.S. Apparel. R. at 1. When traveling, Shapiro used her personal tablet and personal cell phone to do work, which were both automatically synced to her desktop computer at U.S. Apparel. R. at 1. Syncing enabled her to access all of U.S. Apparel's business plans, written policies, and contract information from any of her three devices. R. at 1. After all, as U.S. Apparel's founder, she was responsible for developing the company's business strategy, operations, marketing, promotion, and policy. R. at 1.

Jane Shapiro's administrative assistant, Sharon Bennett ("Bennett"), created a Twitter ™ account for Shapiro, @U.S.Apparel_Shapiro,

and a LinkedIn ™ account for Shapiro as well ("accounts"). R. at 1. Shapiro used the accounts to promote U.S. Apparel as well as to connect with her family, friends and colleagues, maintaining social as well as professional relationships. R. at 1. Shapiro gave Bennett the passwords for these accounts, but Shapiro instructed Bennett that she could not access either account without Shapiro's authorization. R. at 1. Moreover, giving Bennett access to these accounts through the passwords ran contrary to U.S. Apparel's policy. R. at 1.

In an attempt to reinvent the company image, U.S. Apparel's board of directors voted for a change in leadership and forced Shapiro into termination. R. at 2. Post termination, Shapiro took her personal tablet and her personal cell phone with her. R. at 2. It is unclear whether she was able to go back to her office before being forced to leave the company. The board replaced her with Victor Valentini ("Valentini"). R. at 2.

After Shapiro left, Valentini instructed Bennett to go into Shapiro's desktop computer and search for files. R. at 2. While it is unclear whether Shapiro's desktop computer was pass- word protected, once Bennett gained access to Shapiro's desktop computer, she found a folder labeled, "personal" and opened it, read the documents inside and reported to Valentini. R. at 2. One such document Bennett read from Shapiro's personal folder was labeled "Threads Business Plan," a business plan for Shapiro's new start-up teen clothing company. R. at 2. Bennett opened another document called "Hanoi Labor, Co.," again from Shapiro's personal folder, which contained the agreement between Shapiro and Hanoi Labor, Co. stating that Hanoi Labor would manufacture clothing for Threads. R. at 2. Bennett gave these files from Shapiro's folder marked "personal" to Valentini, who in turn reported them to U.S. Apparel's Chairman of the Board,

Thomas Stephan ("Stephan"). R. at 2. After Stephan directed Valentini to investigate the company, Valentini found that many of Hanoi Labor's workers worked in dire conditions, and that the company used child labor. R. at 2-3. After learning this, Stephan called a press conference, disclosed Shapiro's plans to start the new clothing company, her plan to work with Hanoi Labor, Co., and the details on Hanoi Labor, Co. gleaned from U.S. Apparel's investigation. R. at 3. As a result of U.S. Apparel's press conference damaging Shapiro's new business before it even began.

Bennett also accessed Shapiro's social media accounts, even though she did not have Shapiro's authorization to do so, and deleted Shapiro's name and photo from the accounts. R. at 3. At Valentini's direction, Bennett replaced them with Valentini's name and photo, but the rest of the accounts—both Shapiro's tweets and her LinkedIn ™ listing of associations, honors and awards— stayed the same. R. at 2-3. Lastly, Bennett changed the passwords, denying Shapiro from accessing the accounts altogether. R. at 3.

Due to U.S Apparel's interferences with Shapiro's business and accounts, Shapiro took legal action against the company. She filed a three-count complaint in the Nashville County Circuit Court, in the State of Marshall. R. at 3. First, Shapiro alleged that U.S. Apparel intentionally intruded upon her seclusion by accessing her desktop computer files and disclosing the private information about her business dealings with Hanoi Labor, Co. to the public, damaging both her business and her personal reputation. R. at 3. Second, Shapiro alleged that Bennett, as an agent of U.S. Apparel, committed computer fraud in violation of the State of Marshall's Computer Fraud and Abuse Act ("MCFAA"), where Bennett—without Shapiro's authorization— knowingly accessed Shapiro's clearly labeled "personal" folder within the desktop computer. R. at 4.

Shapiro also alleged that Bennett violated the MCFAA where she: (1) knowingly and without authorization accessed Shapiro's accounts; (2) replaced Shapiro's name and photo with Valentini's information as well as the Twitter™ handle from @U.S.Apparel_Shapiro to @U.S.Apparel_Valentini; and (3) most importantly, changed Shapiro's account passwords, effectively locking Shapiro out of the accounts. R. at 4. Lastly, Shapiro brought a common law conversion claim, alleging that Bennett, as U.S. Apparel's agent, intentionally converted the LinkedIn ™ and Twitter ™ accounts where she intended to change the information on those accounts and the passwords for those accounts, thereby interfering with Shapiro's right to control them. R. at 4.

U.S. Apparel motioned to dismiss all three counts pursuant to Rule 12(b)(6) of the State of Marshall Rules of Civil Procedure, arguing that Shapiro failed to state a claim upon which relief could be granted. R. at 5. The Circuit Court granted U.S. Apparel's motion. R. at 5. Shapiro timely appealed to the Third District of the Appellate Court of the State of Marshall, which certified the questions to this Court because the Appellate Court determined that the three questions raised by Shapiro were of such importance that this Court should decide them. R. at 5. This Court then accepted the case for review. R. at 5.

SUMMARY OF ARGUMENT

This Court should reinstate Shapiro's claims. The Circuit Court of Nashville erred in granting U.S. Apparel's motion to dismiss, because Shapiro states a valid claim in each Count of her three Count complaint.

Shapiro states a valid claim for intrusion upon seclusion because she had a reasonable expectation of privacy in the personal files in her workplace computer, and because U.S. Apparel's intrusion into that privacy was highly offensive. As to her expectation of privacy, Shapiro took steps to exclude others from accessing her personal files, such as

labeling the folder "personal." Nothing in the record establishes that Shapiro consented to any lack of workplace privacy. Also, Shapiro, as CEO, very likely had exclusive possession and control over her computer. Lastly and most importantly, Shapiro used the folder that Respondent intruded upon for entirely personal purposes.

Respondent's intrusion of Shapiro's reasonable expectation of privacy was also highly offensive. This is because, instead of honoring Shapiro's privacy, the Respondent chose at each step of the way to intrude further and further into Shapiro's personal affairs, culminating with a press conference where it exposed Shapiro's personal information to the world.

Shapiro properly states a claim against Respondent for violating the State of Marshall Computer Fraud and Abuse Act ("MCFAA"). The MCFAA prohibits knowingly accessing a computer without authorization or by exceeding authorized access to obtain personal information. Bennett did not have authorization or exceeded authorized access when, at the direction of Respondent, she accessed and obtained Shapiro's personal files and social media accounts. Simply having personal folders on work computers does not grant employers the authority to access that information. Rather, Shapiro never granted Respondent, nor did she grant Bennett permission to access and broadcast the contents of her personal files. Furthermore, Shapiro's social media accounts are a proxy for her personally and contain her personal information. Shapiro also affirmatively limited Bennett's access to her social media accounts where she instructed her not to access them without Shapiro's authorization. Finally, Shapiro adequately alleged facts showing that she suffered a loss as a result of Bennett's unauthorized access.

Shapiro properly states a claim for conversion in count III of her complaint. First, Shapiro states a claim because social media accounts are convertible property and Shapiro establishes she owns the accounts. Second, the Respondent seriously interfered with Shapiro's ownership rights to her accounts where they permanently dispossessed her from accessing the accounts by changing the passwords. Lastly, the social media accounts can be valued in multiple of ways such that this Court could apply a remedy where the Respondent is required to return them, pay attorney's fees for this action, and also possible punitive damages. Because Bennett, as agent for Respondent, seriously interfered with Shapiro's ownership rights to exercise control over the accounts, the circuit court erred in granting summary judgment on the conversion claim.

The citizens of the great State of Marshall must know that they have privacy, and they must know that when their privacy is intruded upon they can turn to the courts for protection. Therefore, this Court should overturn the circuit court's holding on all counts.

ARGUMENT

This Court should reinstate Shapiro's claims. The Circuit Court of Nashville erred in granting U.S. Apparel's motion to dismiss, because Shapiro states a valid claim in each Count of her three-Count complaint.

This case gives this Court the opportunity to protect the computer privacy of all citizens in the great State of Marshall, and make sure that the law keeps pace with technology:

> [T]hat the individual shall have the full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.

Samuel D. Warrant and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

First, Shapiro states a valid claim for intrusion upon seclusion, because she had a reasonable expectation of privacy in the personal files in her workplace computer, and U.S. Apparel's intrusion into that privacy was highly offensive. Second, Shapiro states a valid claim for violation of the State of Marshall Computer Fraud and Abuse Act because, at the direction of Respondent, Bennett knowingly accessed and obtained Shapiro's personal files and social media accounts without authorization or by exceeding authorized access thereby causing Shapiro to suffer a loss. Finally, Shapiro states a valid conversion claim because her social media accounts constitute convertible, valuable property that Shapiro establishes she owns and with which the Respondent intentionally and seriously interfered.

I. THE CIRCUIT COURT ERRED IN GRANTING RESPONDENT'S MOTION TO DISMISS BECAUSE SHAPIRO STATES A VALID CLAIM FOR INTRUSION UPON SECLUSION

Workers have privacy in their workplaces. *City of Ontario v. Quon*, 560 U.S. 746, 756 (2010) (citation omitted). People have privacy in their computers. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). Count I of Shapiro's complaint is about the scope and extent of an employee's reasonable expectation of privacy in her workplace computer and when an employer will be liable in tort for intruding upon that privacy.

This Court has previously adopted the tort of intrusion upon seclusion as defined by the Restatement (Second) of Torts § 652B (1977). R. at 3. Section 652B provides:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is sub-

> ject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The Comments and Illustrations to section 652B provide two classic bases of liability. The first is where a defendant examines or investigates a plaintiff's personal mail or records. Restatement (Second) of Torts § 652B cmt. b (1977). The second is where a defendant uses deception to gain unlicensed access to a plaintiff's business affairs. *Id*. at cmt. b, illus. 4.

That is what happened in this case. Respondent, operating behind Shapiro's back, gained access to Shapiro's personal files in her work computer that contained sensitive business plans for her future. Shapiro thus states a valid claim for relief because: (1) she held a reasonable expectation of privacy in the personal files in her computer; and (2) Respondent's intrusion into her files constitutes a highly offensive invasion of her privacy. Therefore, this Court should reverse the ruling of the circuit court below and reinstate Count I of Shapiro's complaint.

A. Shapiro Held a Reasonable Expectation of Privacy in the Personal Folder in Her Workplace Computer

Shapiro's reasonable expectation of privacy in the files in her workplace computer arises from two separate but related rights. The first is her right to privacy in her workplace, as recognized by *O'Connor v. Ortega*, 480 U.S. 709 (1987) (plurality). Although the Court issued a plurality opinion in *O'Connor*, "[a]ll Members of the Court agreed" that individuals do have some reasonable expectations of privacy in their workplaces. *City of Ontario*, 560 U.S. at 756 (citing *O'Connor*, 480 U.S. at 717 (plurality opinion), 731 (Scalia, J., concurring), and 737 (Blackmun, J., dissenting)). The second is her right to privacy in her computer as recognized by *Riley*, where the Court unanimously held that individuals have a reasonable expectation of privacy in their cell phones, or, as the Court said the phones could be called, "minicomputers."134 S. Ct. at 2489.

When examining individuals' expectations of privacy in their workplaces, their computers, or their workplace computers, courts generally consider four factors to determine whether those expectations are reasonable. First, and most commonly, courts consider whether the person took any steps to ensure that the area or item intruded upon remained private. *United States v. Ziegler*, 474 F.3d 1184, 1190 (9th Cir. 2006). Second, courts consider whether a person has consented in any way to a lack of privacy, and if so the scope of that consent. *Muick v. Glenayre Elec*., 280 F.3d 741, 743 (7th Cir. 2002). Third, courts consider the ownership, possession, and control of the area or item searched. *O'Connor*, 480 U.S. at 718. Finally, courts consider whether the item or area intruded upon was used for personal or work purposes. *Blake v. Wright*,

179 F.3d 1003, 1009 (6th Cir. 1999).

In this case, all four of these factors favor Shapiro, and therefore she held a reasonable expectation of privacy in the personal files in her workplace computer.

1. Shapiro took Steps to Ensure that the Personal Files on her Workplace Computer Remained Private

Whether or not a person took any steps to ensure that an item or area intruded upon remained private is an incredibly important factor in determining the reasonableness of a person's privacy expectations. For example, in *Ziegler*, the Court held that *Ziegler* had a reasonable expectation of privacy in the contents of his office computer because his office was not shared by coworkers and kept locked, and because he password protected the computer. 474 F.3d at 1190; *see also Doris v. Absher*, 179 F.3d 420, 425 (6th Cir. 1999) (employees had reasonable expectation of privacy in conversations at work critical to their boss because they only spoke amongst themselves and always endeavored to make sure no one else heard the conversations); *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632, 637–38 (Tex. App. Ct. 1984) (employee held a reasonable expectation of privacy in workplace locker due to the fact that he purchased and used his own lock). Also relevant is whether a person has the authority or ability to exclude others from an area or item. *See Greywolf v. Carrol*, 151 P.3d 1234, 1245–46 (Ak. 2007) (holding that Greywolf had no expectation of privacy in her hospital room because she could not show that "she had the right to exclude others from her room").

Along these same lines, courts hold that when a person fails to take steps to ensure their own privacy in an item or area, any expectation of privacy in that item or area will be unreasonable. *Wilson v. Moreau*, 440 F.Supp. 2d 81, 104 (D. R.I. 2006) (library employee had no reasonable expectation of privacy in documents stored on the public library's computer system because the library was "an open and public work environment," and "the computers were available for public use"); *United States v. King*, 604 F.3d 125, 137 (6th Cir. 2010) (King had no reasonable expectation of privacy in hard drive because he failed to protect it with a password).

Here, Shapiro did take steps to ensure that her workplace computer remained private. First, Shapiro very likely password protected her computer, because as CEO, her computer contained highly sensitive company materials. R. at 1. Second, as was relevant in *Greywolf*, Shapiro (again as CEO) very likely did have the authority to exclude others from her workplace computer. Finally, Shapiro put the private files in her workplace computer in a folder marked "personal." R. at 2. This was definitely an affirmative effort to ensure that if anyone did

gain access to her computer, they would know which files were off limits, and which files were related to U.S. Apparel's business.

Former employees can lose their reasonable expectations of privacy in materials in their offices if, after they are terminated, they have an opportunity to remove personal belongings but do not do so. *See Shaul v. Cherry Creek Valley-Springfield Cent. Sch. Dist.*, 363 F.3d 177, 182–83 (2d Dist. 2004). However, in this case, the record is unclear as to whether Shapiro was given any opportunity to access her computer or remove her personal files from it after she was terminated. And, given that her termination was forced, it is very plausible that she had no such opportunity. R. at 2. Moreover, where an employer fails to return an employee's property, the employee will retain her reasonable expectation of privacy therein. For example, in *Armijo v. Yakima HMA, LLC*, the Court held that a former employee had reasonable expectation of privacy in her diary that her employer failed to return after she was terminated. No. 11–CV–3114–TOR, 2012 WL 2576624 *2 (E.D. Wash. July 3, 2012). Here, instead of returning Shapiro's personal files, Respondent held a press conference and broadcasted her personal information to the world.

So, Shapiro did take steps to protect her privacy and she may have never had an opportunity to recover her personal files after her termination.

2. It is Highly Unlikely that Shapiro Consented to any Lack of Privacy in Her Workplace Computer

When an employer has a policy of monitoring its employees' computer activities, and when an employee either constructively or affirmatively consents to that policy, such consent can destroy the employee's reasonable expectation of privacy. *See e.g.*, *Muick*, 280 F.3d at 743; *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002).

However, here the record is devoid of any such monitoring policy. And, if this Court reinstates Shapiro's claim and Respondent could produce such a policy on remand, the mere existence of a monitoring policy would not defeat Shapiro's claim. This is because, in order for an employer's monitoring policy to destroy an employee's reasonable expectations of privacy, the monitoring must be constant and routine. *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001). This rule makes good sense, because as *Levanthal* recognized only a policy that is used "routinely" or as part of a "general practice" can reasonably and effectively put an employee on notice that she has no privacy in her workplace computer. 266 F.3d at 74; *see also Covertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (reaching a similar holding).

In this case, there is nothing in the record indicating Shapiro consented to giving away any of her privacy, and it is unlikely that she ever

did give such consent.

3. Shapiro Exclusively Controlled and Possessed Her Workplace Computer, and it is Possible that She Also Owned the Computer

A person's ownership, possession, and control of an area or item intruded upon are also important when determining that person's reasonable expectation of privacy in the area or item. *O'Connor*, 480 U.S. at 718; *Ziegler*, 474 F.3d at 1190.

In *O'Connor*, one of the reasons the Court found that Ortega had a reasonable expectation of privacy in the contents of his desk was because he "did not share his desk or file cabinets with any other employees." 480 U.S. at 718. Similarly, in *Ziegler*, one of the reasons the Court held that Ziegler had a reasonable expectation of privacy his workplace computer was because "[h]is office was not shared by co-workers." 474 F.3d at 1190. In *Leventhal*, the Court held that Leventhal had a reasonable expectation of privacy in the contents of his computer because his office was private, had a door, and because Levanthal had exclusive use of his desk, cabinet, and the computer in his office. 266 F.3d at 73. Finally, in *Schowengerdt v. Gen. Dynamics Corp.*, the Court held that a naval employee had a reasonable expectation of privacy in personal photographs and letters his employer discovered inside his desk, because the desk was given to him for his "exclusive use." 823 F.2d 1328, 1335 (1987); *see also Varnado v. Dep't. Employ*, 687 So.2d 1013, 1024–25 (La. App. 1996) (employee had a reasonable expectation of privacy in his office computer because his "executive office" arrangement allowed only himself and his secretary access to his office, and therefore the office would be "considered private by most members of society").

In this case, it is very plausible that Shapiro had exclusive control and possession over her office and her work computer, because she was the CEO of U.S. Apparel. In terms of ownership, the record is unclear as to whether Shapiro bought or personally owned her work computer. But, even if she did not, ownership is the least important factor to consider (as compared to possession and control) when determining an individual's privacy interests, because a person's privacy interests do not rise and fall based only on her ownership of property. *Schowengerdt*, 823 F.2d at 1333 (citing *Katz v. United States*, 389 U.S. 347, 352 (1967)). As *Schowengerdt* recognized, the Supreme Court has rejected the idea that an employee must have a property right in an area or item to have a legitimate privacy interest there. 823 F.2d at 1333 (citing *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968)); *see also United States v. Barrows*, 481 F.3d 1246, 1248–49 (10th Cir. 2011) (despite the fact that employee owned computer he took to work, he had no expectation of privacy in it because he failed to use a password or take other steps to prevent others from using it). So, Shapiro's exclusive possession and

control of her workplace computer, and her possible ownership of that computer, strongly suggests that she had a reasonable expectation of privacy in the computer.

4. Shapiro Used the Computer Folder that Respondent Intruded Upon to Keep Highly Personal Files.

Similar to the question of an employee's ownership, possession, and control of an item or area is the question of what the item or area intruded upon was used for. Essentially, when determining whether a person has a reasonable expectation of privacy in an item or area in their workplace, the law makes a distinction between items or areas used for work activity and those used for personal activity. *O'Connor*, 480 U.S. at 718. When, as here, the item intruded upon is used or substantially related to any employee's personal activities, courts are more likely to hold that the employee has a reasonable expectation of privacy in that item. *Id.* at 718; *see e.g., Stengart v. Loving Care Agency, Inc*., 990 A.2d 650, 663–64 (N.J. 2010).

In *O'Connor*, one of the key reasons that the Court held that the employee in question had a reasonable expectation of privacy in the desk and file cabinets in his office was that the employee used those items to keep highly personal material, such as personal correspondences, financial records, teaching aids and notes, and personal gifts and mementos. 480 U.S. at 718; *see also Varnado*, 687 So.2d at 1024 (employee had a reasonable expectation of privacy in his office because he used it as a place to keep his personal records such as check books, bills, and insurance papers).

Similarly, in *Blake*, part of the reason the Court held that the employees had a reasonable expectation of privacy in their personal phone calls was because of the mere fact that the calls were personal. 179 F.3d at 1009. In *Rosario v. United States*, the Court held that employees had a reasonable expectation of privacy in their conversations made in a break room because "[t]he purpose of the room was inherently private," and the room was used to "safeguard [employees'] personal belongings and working instruments . . . " 538 F. Supp.2d 480, 497 (D.P.R. 2008). Finally, in *Stengart*, the Court held that an employee had a reasonable expectation of privacy in email communications with his attorney, because the emails were used to share inherently personal and confidential material. 990 A.2d at 663–64.

The result in all the above cases should hold true in this one, because Shapiro used the folder in her computer that Respondent intruded upon for personal purposes. Shapiro even labeled the folder "personal." (R. at 2); *see also Vernars v. K Young*, 539 F.2d 966, 969 (3d Cir. 1976) (employee had reasonable expectation of privacy in mail that was marked "personal"); *cf. Watkins v. L.M. Berry & Co*., 704 F.2d 577, 584

(11th Cir. 1983) (employer permitted to monitor an employee's phone calls, but such monitoring had to be limited in length and could only be long enough to make sure the phone call was not business related; after such time as call was determined personal, employee would have a reasonable expectation of privacy in the call).

So, as soon as Bennett saw that the title the folder was "personal," she should have known that it was private and that Shapiro was using it for personal purposes.

B. Respondent's Intrusion into the Personal Files on Shapiro's Computer was a Highly Offensive Invasion of Her Privacy.

In order for an intrusion to be highly offensive to a reasonable person, the interference with a plaintiff's seclusion must be substantial, and the result of conduct to which a reasonable person would strongly object. Restatement (Second) of Torts, § 652B cmt. d (1965); *Montgomery Ward v. Shope*, 286 N.W.2d 806, 808 (S.D. 1979). To determine what constitutes highly offensive conduct, courts consider five factors: (1) the degree of the intrusion, (2) the context, conduct and circumstances surrounding the intrusion, (3) the intruder's motives and objectives, (4) the setting into which the defendant intrudes, and (5) the expectations of those whose privacy is invaded. *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1009 (N.H. 2003); *see also Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 493 (Cal. 1998); *PETA v. Bobby Berosini, Ltd.*, 895 P.2d 1269, 1282 (Nev. 1991).

Generally, the question of whether conduct is highly offensive is "largely a matter of social conventions and expectations." *PETA*, 895 P.2d at 1281. For example, "while questions about one's sexual activities would be highly offensive when asked by an employer, they might not be offensive when asked by one's closest friend." *Id.* (citing J. Thomas McCarthy, *The Rights of Publicity and Privacy*, § 5.10(A)(2) (1993)). Further, courts have recognized that highly offensive conduct is not limited to intrusions upon physically defined areas or places, and that intrusions into one's "personality" or "psychological integrity" can be also highly offensive. *Phillips v. Smalley Maintenance Services, Inc.*, 435 So.2d 705, 710–711 (Al. 1983); *see also Bennett v. Norban*, 151 A.2d 476, 479 (Pa. 1959) (holding that outrageous conduct can involve intrusion into a person's "integrity" or "honor").

Within this framework, courts have held that employers' intrusions into the lives of their employees have been highly offensive in a multitude of contexts. For example, courts have held that employers conduct can be highly offensive when an employer: opens or copies an employee's personal mail, *Roth v. Farner-Bocken Co.*, 667 N.W.2d 651, 660–61 (S.D. 2003)); secretly places a listening device in an employee's office, *Slack v. Kanawha Cty. Hous. and Redeveloping Auth.*, 423 S.E.2d

547, 550–54 (W.Va. 1992); listens in on a phone conversation happening in an office that the employer told the employee to use for his private telephone calls, *Fisher v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 927 (W.D. Wis. 2002); accesses an employee's personal email account to obtain evidence to support termination efforts of the employee, *Murphy v. Spring*, No. 13–CV–96–TCK–PJC, 2013 WL 5172951, *10–11 (N.D. Ok. Sept. 12, 2013); *Fischer*, 207 F. Supp. 2d at 928; or reads a former employee's diary. *Armijo*, No. 11–CV–3114–TOR, 2012 WL 2576624, at *2.

When a defendant gains unauthorized access to files on a plaintiff's computer or hard drive, courts have also held that such conduct can be highly offensive. *See e.g.*, *Coalition for an Airline Passengers' Bill of Rights v. Delta Air Lines, Inc.*, 693 F. Supp.2d 667, 675 (S.D. Tex. 2010); *Dalley v. Dykema Gossett*, *P.L.L.C.*, 788 N.W.2d 679, 690–91 (Mich. Ct. App. 2010).

The facts of *Roth* are very similar to this case. In *Roth*, Roth's former supervisor opened a personal piece of Roth's mail that an attorney sent to his company by accident (Roth was no longer employed there). 667 N.W.2d at 658. His supervisor opened the mail "in the regular course of business," but after determining that the mail was personal and belonged to Roth, the supervisor read the entire contents of the mail packet, made photocopies, and then gave the copies to his supervisor. *Id.* Based on these facts, the Court held that Roth's former employer's conduct was highly offensive. *Id.* at 663–64. Here, just as in Roth, Bennett may have had legitimate business motives for accessing Shapiro's computer. However, upon seeing the personal files within the computer, Bennett (just like Roth's supervisor) should have not opened or read anything inside the personal folder or given any of Shapiro's personal information to her superiors, and her actions were highly offensive.

In *Murphy*, the Court held that Murphy's supervisors' action of intentionally accessing her private email account in order to gain evidence to support their recommended termination of her employment could be highly offensive conduct. No. 13–CV–96–TCK–PJC, 2013 WL 5172951, at *11. Similarly, in *Fischer*, Fischer's former employer gained access to Fischer's personal emails in order to justify its termination of him. 207 F. Supp.2d at 928. The Court held that this conduct could be highly offensive and thus denied the defendants' motion for summary judgment. *Id.* Again, both *Murphy* and *Fischer* are similar to this case because it is very plausible that Respondent directed Bennett to access Shapiro's computer in order to get information justifying her termination.

Finally, in *Dalley*, the Court found that where agents of the defendant, acting through subterfuge, gained access to Dalley's computer and hard drive in order to copy files, a reasonable juror could find this

conduct objectionable. 788 N.W.2d at 690; *see also Coalition for an Airline Passengers' Bill of Rights*, 693 F. Supp.2d at 675 ("The court concludes that hacking into a person's private computer and stealing personal correspondence would . . . be highly offensive to a reasonable person."). Here, Respondent also displayed a level of subterfuge because they waited until after Shapiro had been removed from the company to access her computer. Had Respondent approached Shapiro before she was terminated, she could have easily assisted the company in removing business-related materials from her computer while at the same time ensuring that her personal files were not intruded upon.

Employers often argue that they are justified in intruding into their employees' computers because: (1) they need to make sure employees are not wasting too much time doing personal tasks, (2) they need to protect their company's confidential information, and (3) monitoring helps avoid employers' liability in civil suits where employers brought in as defendants under the theory of respondeat superior. Meir S. Hornug, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 Fordham J. Corp. & Fin. L. 115, 122 (2005). However, none of these justifications are present in this case. At the time of the intrusion, Shapiro was no longer an employee, so any concerns about productivity or respondeat superior were absent. Also, Shapiro presumably no longer had access to her workplace computer after her termination. So, at best Respondent only needed to make sure that Shapiro had not leaked any information in the past, and this need does very little to downplay the company's highly offensive invasion of Shapiro's privacy.

What is most striking about Respondent's behavior in this case is the degree of its intrusion into Shapiro's privacy. After Shapiro was terminated, Respondent could have chosen not to intrude into her computer. After the company intruded into her computer, it could have chosen not to open Shapiro's personal folder. After Respondent chose to open the personal folder, it could have chosen not to open the files within that folder. After it chose to open the files, it could have chosen to keep the highly sensitive and personal information it discovered within the company. Instead, at each step of the way, Respondent chose to intrude further and further, culminating with the company holding a press conference and exposing Shapiro's personal information to the entire world.

In conclusion, Shapiro's right to privacy must be protected:

> The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.
>
> *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 234 (Minn. 1998).

Here, Respondent intruded upon Shapiro's reasonable expectation

of privacy in a gross, wrong, and highly offensive manner, and stole from her the right to choose which parts of her life she wanted to keep private, and which parts she wanted to make public.

The citizens of the great State of Marshall must know that they have privacy. They must know that they have privacy in their workplaces, in their computers, and in their personal affairs. And they must know that when their privacy is intruded upon, they can turn to the courts for protection. Therefore, Shapiro respectfully asks this Honorable Court to reverse the decision of the circuit court below and reinstate her claim for intrusion upon seclusion.

II. THE CIRCUIT COURT ERRED IN GRANTING RESPONDENT'S MOTION TO DISMISS BECAUSE SHAPIRO PROPERLY STATES A CLAIM AGAINST THE RESPONDENT FOR VIOLATING THE STATE OF MARSHALL COMPUTER FRAUD AND ABUSE ACT

Shapiro properly states a claim against Respondent for violation of the State of Marshall Computer Fraud and Abuse Act ("MCFAA"). ¶ 1030(a) (2008). The MCFAA provides in part:

> (1) Whoever 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; and (2) Any 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.
>
> Marshall Stat. Ann. ¶ 1030(a)(2008).

The MCFAA emulates the federal Computer Fraud and Abuse act ("CFAA"). 18 U.S.C. § 1030 (West 2008). The CFAA prohibits unauthorized access or exceeding authorized access to computers when the access is used to obtain information. *Id.* at § 1030(a). The CFAA also provides for a civil cause of action to obtain compensatory damages. *Id.* § 1030(g); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC.*, 428 F.3d 504, 510-11 (3d Cir. 2005).

Other states, like the state of Marshall, have also modeled their state computer crime statutes after the CFAA. *See, e.g.*, Cal. Penal Code § 502 (West 2011); 18 Pa. Consol. Stat. Ann. § 7611 (West 2003). Accordingly, when interpreting state computer crime counterpart statutes, courts often look to the text of the CFAA and the relevant case law. *See e.g., State v. Riley*, 988 A.2d 1252, 1259 (N.J. 2009); *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 637 (E.D. Va. 2009).

The Circuit Court's decision should be reversed. Shapiro properly

stated a claim against Respondent for violation of the MCFAA because (1) At the direction of Respondent, Bennett committed computer fraud both when she accessed Shapiro's personal files and Shapiro's social media accounts without authorization; and (2) Shapiro suffered the requisite loss to state a claim under the MCFAA.

A. Shapiro Adequately Stated a Claim for Two Separate Violations of the MCFAA Where Bennett Accessed both Shapiro's Personal Files and Social Media Accounts Without Authorization

Shapiro adequately stated a claim against Respondent for Bennett's violation of the MCFAA on two separate occasions. Under the CFAA, "knowingly" accessing a computer "does not require proof of intent to defraud." *United States v. Willis*, 476 F.3d 1121, 1125 (10th Cir. 2007). Ultimately, the only proof necessary is "that the defendant intentionally accessed information from a protected computer." *Id.* The acts of opening files or entering in passwords without permission in and of themselves corroborate intent. *Id.* at 1125, n.1; *see United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012). Therefore, Bennett's actions of opening a clearly labeled "personal" folder as well as changing the social media account passwords in and of themselves corroborate intent.

Furthermore, Respondent is vicariously liable for the conduct of its agent, Bennett, when she committed computer fraud at their direction. Courts have held that an employer can be vicariously liable for an employee's violation of the CFAA if those transgressions occur when the employer directs the employee's conduct. *See e.g., Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F.Supp.2d 468, 472 (S.D.N.Y.2004). Respondent affirmatively instructed Bennett to access and obtain Shapiro's personal files from her desktop computer. R. at 2. Respondent also instructed Bennett to access Shapiro's LinkedIn ™ and Twitter ™ accounts, and to delete her name, photo and other personal information as well as changing the account passwords, all without Shapiro's consent. R. at 3. Respondent is therefore liable for Bennett's improper actions.

1. Bennett Did Not have Authorization to Access and Obtain Shapiro's Personal Files.

Shapiro did not give Bennett authorization to access and obtain her personal files. Both the MCFAA and the CFAA do not provide a definition for "authorization," however, courts have defined it as "permission or power granted by an authority." *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). Both the MCFAA and the CFAA allow "[a]ny person" who suffers a loss under the statutes to bring a civil cause of action. § 1030(g); ¶ 1030(a)(2). "Any" person means that a plaintiff does not have to be the owner of an improperly accessed computer. Rather, a defendant is considered "without authorization" if he

improperly accesses the data of another even if the access is from his own computer. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004).

For example, in *Lazette v. Kulmatycki*, the plaintiff installed her personal email account on a company owned blackberry device. 949 F. Supp. 2d 748, 751 (N.D. Ohio 2013). Upon her termination, the plaintiff returned the device to her employer, however, the employer then accessed and disclosed personal messages that plaintiff left on the device. *Id.* Plaintiff filed suit under the Stored Communications Act that, like the CFAA and MCFAA, prohibits access without authorization. 18 U.S.C. § 2511(2)(d) (West 2008). The Court held that because plaintiff did not grant permission to obtain her personal messages, the supervisor was not authorized to access them even if plaintiff had left the messages on a company owned device. *Lazette*, 949 F. Supp. 2d. at 762.

Similarly, the Ninth Circuit in *Theofel* reversed dismissal of a CFAA claim where defendant accessed plaintiffs' email accounts without permission from a company computer. *Theofel*, 359 F.3d at 1079. Although defendant subpoenaed plaintiffs' personal emails, he was still without authorization because he accessed the accounts without plaintiffs' permission. *Id.* at 1078; *see also, Modrowski v. Pigatto*, 712 F.3d 1166, 1167 (7th Cir. 2013) (employee's act of merging personal and business emails does not grant employer to access merged personal information).

In the above-mentioned cases, the defendants owned the accessed computer. However, the defendants nonetheless "accessed a computer without authorization" because they were not granted permission to access the personal information within the computer. If Shapiro had left her credit card in her former office at U.S. Apparel, it would not grant U.S. Apparel authorization to obtain and spend on the card as they please.

Even if Shapiro did not personally own her desktop computer from which her personal files were accessed, just as the plaintiffs in *Theofel* and *Lazette*, she never gave permission to Bennett or Respondent to access, and obtain her personal information. *See Theofel* 359 F.3d at 1079; *Lazette*, 949 F. Supp. 2d at 751. As the Court in *Lazzette* reasoned, leaving personal information on company devices does not grant employers, or Respondent in the present case, permission to obtain that information. Further, simply syncing personal and company devices also does not grant Respondent authorization to access Shapiro's personal files. *See Modrowski*, 712 F.3d at 1167.

With the abundance of new technologies, syncing personal devices to work computers has not only become common practice among employees, but companies are also creating special programs asking employees to sync their personal devices to work computers for efficiency.

For example, Dell conducted a survey and found that companies

with such programs saw a 74% productivity increase. Sarah Marshall, *It Consumerziation: A Case Study of BYOD in a Healthcare Setting*, Tech. Innovation Mgmt. Rev., http://timreview.ca/article/771 (last visited Sept. 29, 2014). Allowing companies like U.S. Apparel to then grab whatever synced personal information they please would jeopardize every employee's protections against theft of electronically stored personal information. As the legislative history of the CFAA indicates, Congress viewed the statute as "doing for computers what trespass and burglary laws did for real property." Matthew Kapitanyan, *Beyond Wargames: How the Computer Fraud and Abuse Act Should be Interpreted in the Employment Context*, 7 I/S: J. L. & Pol'y for Info. Soc'y 405, 410 (2012).

In the alternative, even if this Court finds that Bennett had authorization, she still violated the MCFAA because she exceeded her authorized access. Since the MCFAA does not provide a definition for "exceeds authorized access," a comparison to the CFAA is instructive. The CFAA defines exceed authorized access as "to access a computer with authorization but utilizing access to obtain or alter information the accessor was not authorized to obtain or alter." CFAA. § 1030(e)(6) (emphasis added).

Courts differ in applying the definition and as a result a majority and minority application of the phrase have emerged. The majority view holds that a person exceeds authorized access when they misuse information that they are otherwise entitled to access. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010). The minority view holds that a person exceeds authorized access when they have permission to access the computer but access information thereon to which they are not entitled. *Brekka*, 581 F.3d at 1133. Bennett exceeded authorized access under both the majority and minority views.The majority of courts broadly construe exceeding authorization and expand the phrase's scope with each new fact pattern. *Rodriguez*, 628 F.3d at 1263. For instance, in *Yessin* the defendant accessed plaintiff's business email without her authorization to gain leverage in the pending divorce proceeding between them. 686 F. Supp. 2d at 634. The defendant argued that as manager, he was authorized to access business email accounts and that he accessed the account in an effort to ensure plaintiff was not usurping corporate opportunities. *Id.* at 637. In rejecting these arguments, the Court held that the scope of an individual's authorization to access a computer is analyzed on the basis of the expected norms of intended use. *Id.* at 636. Because defendant's access violated expected norms of intended use, the Court denied defendant's motion to dismiss for both the state and federal computer fraud laws. *Id.* at 637.

In *Rodriguez*, although the plaintiff, as an employee, had authorization from his employer to access all computer information, he nonetheless exceeded authorized access when he obtained others' personal

information for non-business reasons. 628 F.3d at 1263. In finding that Rodriguez exceeded his authority under the CFAA, the cCurt was not persuaded by his argument that he did not use the information for a criminal purpose. *Id.* at 1264.

In the present case, through Bennett, Respondent also exceeded authorized access when it improperly accessed Shapiro's personal information in a way that violated expected norms of intended use. Respondent may argue, as the defendant in *Yessin* attempted but failed, that they accessed Shapiro's personal files for business purposes. However, the expected norms of accessing business information do not entail opening a clearly labeled "personal" folder and then negatively broadcasting the personal contents through a press conference. R. at 3.

Bennett's unlawful actions also satisfy the minority view of exceeding authorization, which imposes liability on a former employee when his initial access to a computer is authorized, but then access information within the computer that he is not entitled to access. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204-05 (4th Cir. 2012). Thus, the narrow view focuses on the authority to access information not the misuse of that information. *Id.* The Court in *Brekka* held that where an employer does not limit an employee's access to any company information, misusing that information does not constitute exceeding authorized access. 581 F.3d at 1133. Consequently, even if this court finds that Bennett, as an employee, was authorized to access U.S. Apparel's information, Bennett nonetheless exceeded authorized access by opening a clearly labeled "personal" folder, not company information. R. at 2. Neither Bennett nor Respondent was entitled to access non-company personal information.

Thus, at Respondent's direction, Bennett accessed and obtained Shapiro's personal information without Shapiro's authorization or by exceeding authorized access.

2. Bennett Committed Computer Fraud When She Accessed and Altered Shapiro's Personal Social Media Accounts without Shapiro's Authorization

Shapiro adequately stated a claim for computer fraud, where Bennett accessed Shapiro's LinkedIn ™ and Twitter ™ accounts, deleted her name, photo, and personal information, and changed the account passwords, all without Shapiro's authorization.

LinkedIn ™ is a professional network on the Internet. R. at 2. Twitter ™ is a social network and a blogging site that allows users to send and read short messages called "tweets." R. at 2. These websites allow users to create their own public profiles and connect with other users based on interests in music, movies, other activities, and mutual friends. R. 1-2.

In social media account disputes, the account itself is considered a "computer." The CFAA defines a computer as a high-speed data processing device and includes "any data storage facility or communications facility directly related to or operating in conjunction with such device." § 1030(e)(1). In order for a website to access the Internet, it must access the host server. *United States v. Drew*, 259 F.R.D. 449, 456-57 (C.D. Cal. 2009). Social media accounts are stored and hosted on their respective "data storage facility or communications facility directly related to or operating in conjunction with" a computer as defined in the CFAA. § 1030(e)(1); See Steven J. Vaughan-Nichols, *How Social Networking Works*, IT World (Jan. 7, 2010), http://www.itworld.com/software/91803/how-social-networking-works. Accordingly, when Bennett accessed and altered Shapiro's personal LinkedIn ™ and Twitter ™ accounts, she was accessing a "computer."

Business email accounts are considered "personal" accounts based on their contents. *Yessin*, 686 F. Supp. 2d at 634. Although plaintiff's email account in *Yessin* was a business email opened during the course of her employment, the Court still considered the account to be plaintiff's because it contained personal information, and access to the account without permission is unauthorized. *Id* at 637. Similarly, although the social media accounts at issue were opened while Shapiro was working at U.S. Apparel, and although the LinkedIn ™ account contained "U.S. Apparel" along with "Shapiro" in the account name, the accounts are still Shapiro's because they contained her personal information. R. at. 1.

Social media profiles are perceived by other users as a proxy for the individual, thus, Shapiro's sharing of photos, personal credentials, and personal information made her Twitter ™ and LinkedIn ™ accounts a proxy for her personally and represented her as an individual. Danah Boyd, *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications, A Networked Self: Identity, Community, and Culture on Social Network Sites* 39, 43 (Zizi Papacharissi ed., 2010). Because Shapiro never gave Bennett permission to alter personal information on the accounts, nor change the passwords, Bennett acted without authorization under the MCFAA.

Bennett acted based on Respondent's instructions not Shapiro's, and where a person that lacks authority grants the permission, access is construed as "without authorization." *Brekka*, 581 F.3d at 1133. U.S. Apparel's policy prohibits owners of social media accounts to give out their passwords to others. If under its policy Respondent does not have authority to any social media account passwords, then Respondent does not have the power to grant Bennett access to those accounts.

Even if this Court finds that Bennett had authorization because Shapiro initially gave her the account passwords, Bennett still exceeded authorized access under both broad and narrow views. Under the broad

view, Bennett exceeded authorized access because she misused Shapiro's accounts where she altered the personal information and changed the passwords. *See Rodriguez*, 628 F.3d at 1263. Under the narrow view, Shapiro restricted Bennett's access to the accounts by affirmatively instructing her that she could not access the accounts without Shapiro's authorization. R. at 1; *see Brekka*, 581 F.3d at 1133. However, since Shapiro's termination, Bennett has continuously accessed Shapiro's LinkedIn ™ and Twitter ™ accounts without Shapiro's permission.

Therefore, Shapiro adequately stated a claim for two separate violations of the MCFAA, where Bennett accessed both Shapiro's personal files and Social Media accounts without authorization.

B. Shapiro Pleaded Sufficient Facts to Create a Plausible Inference that She Suffered a Loss as a Result of Respondent's Violation of the State of Marshall Computer Fraud and Abuse Act.

Shapiro suffered a loss as a result of Bennett's unauthorized access of her personal files and social media accounts. Both the MCFAA and CFAA provide a civil remedy for loss or damage resulting from a violation of the statutes. Although the MCFAA and CFAA have similar civil remedy provisions, there is one key difference. The CFAA requires a minimum damages threshold of $5000, whereas the MCFAA does not require any minimum damages. As such, any application of the CFAA that turns on minimum damages is irrelevant for MCFAA purposes.

The CFAA defines the term "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and… any revenue lost, cost incurred, or other consequential damages incurred[.]" §1030(e)(11) (emphasis added). The definition is therefore quite broad. The term "damage" is defined more narrowly under the CFAA requiring "impairment to the integrity or availability of data… a system, or information[.]" §1030(e)(8). Both the MCFAA and CFAA state that a victim of computer fraud may allege either loss or damage. As such, "damage" does not need to be shown if a plaintiff can allege a "loss." *See e.g., Motorola, Inc. v. Lemko Corp*., 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009).

1. Shapiro Suffered a Loss as a Result of Bennett's Unauthorized Access to Shapiro's Personal Files.

Shapiro alleged sufficient facts to show that she suffered a loss under the MCFAA by reason of Bennett's unauthorized access to her personal files. The Ninth Circuit has stated that loss of business or money spent to "restore or maintain some aspect of a business affected by a violation," constitutes economic loss and is recoverable under the CFAA. *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir.

2004).

When a plaintiff ran for mayor against the defendant in *Steinbach v. Village of Forest Park*, the defendant improperly accessed plaintiff's personal emails during the campaign. No. 06 C 4215, 2009 WL 2605283, at *1 (N.D. Ill. Aug. 25, 2009). The Court held that the loss of possible income and opportunity as an elected official were sufficient damages because the defendant used those unauthorized emails for his competitive edge. *Id.* at *6.

In *Yee v. Lee*, a defendant attempted to sabotage a plaintiff's business plans by accessing his personal emails without authorization and exposed those plans to others. C 1202474 WHA, 2012 WL 4343778, at *3 (N.D. Cal. Sept. 20 2012). The Court held that plaintiff alleged adequate facts to constitute a loss under the state computer crime law. *Id.* Respondent negatively disclosed to the world Shapiro's plans to start a new clothing company. R. at 3. Consequently, Shapiro suffered a loss that is very similar to that of Steinbach's and Yee's. As a result of Respondent's actions, Shapiro has lost possible income and business opportunities from her company. Further, if Shapiro continues with the plan to open her company, she has suffered the loss of "conducting a damage assessment" from Respondent's negative broadcasting, "the cost of responding to an offense" and "other consequential damages." §1030(e)(11). Shapiro will have to spend money to "restore" her company reputation and recover any lost "business affected by [Respondent's] violation" of the MCFAA. *See Creative Computing*, 386 F.3d 930 at 935.

Respondent's argument that Shapiro's act of leaving her personal files on her desktop computer forfeits the right to assert damages is unavailing. As the Ninth Circuit reasoned, even if the victim could have prevented all harm either by removing the personal information or installing security measures, "a causal chain from the perpetrator to the victim is not broken by vulnerabilities that the victim negligently left open." *See Creative Computing*, 386 F.3d at 935. In finding that plaintiff suffered a loss from defendant's improper access of confidential information, the Court stated that defendant's argument that plaintiff could have prevented some of the harm is "analogous to a thief arguing that I would not have been able to steal your television if you had installed deadbolts instead of that silly lock I could open with a credit card." *Id.*

2. Shapiro Suffered a Loss as a Result of Bennett's Unauthorized Access to Shapiro's Social Media Accounts.

Shapiro alleged sufficient facts to show that she suffered a loss under the MCFAA by reason of Bennett's unauthorized access to her social media accounts. The MCFAA, like many state law computer crime statutes, does not require any minimum damages threshold. See, e.g., Neb. Rev. Stat. § 28-1343.01 (West 2014); S.D. Codified Laws § 43-43B-1

(2014); 18 Pa. Consol. Stat. § 7611 (West 2003). As such, as long as Shapiro states a loss, no matter how minimal, she has a claim under the MCFAA.

For example, in *Miller v. Meyers*, defendant was found liable under a state computer crime statute for accessing plaintiff's social media account without authorization. 766 F. Supp. 2d 919, 924 (W.D. Ark. 2011). In denying defendant's motion to dismiss, the Court found that defendant incurred at least some minor loss in changing her passwords and assessing the consequences of the defendant's improper access. *Id.*; *see Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 982 (M.D.Tenn.2008) (allowing plaintiff to allege minor losses under a similar state statute).

In *Ardis Health, LLC v. Nankivell*, the defendant was hired to maintain passwords for the company's social media accounts, but refused to hand in those passwords when she was terminated. No. 11 Civ. 5013(NRB), 2011 WL 4965172, at *2 (S.D.N.Y. Oct. 19, 2011). In ruling for the plaintiffs, the Court stated that they were suffering irreparable harm as a result of defendant's refusal to return the passwords. *Id.* at 2. Although *Ardis* was brought under the Copyright Act, the case illustrates that social media accounts have value and losing access to those accounts causes harm to the owner.

Under the MCFAA, Shapiro need only allege some minor loss. Just as in *Miller* and *Ardis*, Shapiro also suffered a loss when Bennett locked Shapiro out of her social media accounts and altered Shapiro's personal information. Shapiro suffered a loss in assessing the damages and consequences of Bennett's actions. Also, as a result of Bennett's unauthorized access, people searching for Bennett on their accounts will be routed to an altered account representing Valentini instead. Shapiro invested ten years of time and effort in developing her reputation in the business world and used her social media accounts to connect with friends and family. R. at 2.

While in another case a court dismissed a LinkedIn ™ CFAA claim, that court misconstrued "loss" to require being associated with impairment to a computer. *Eagle v. Morgan*, No. CIV.A. 11-4303, 2012 WL 4739436, at *3 (E.D. Pa. Oct. 4, 2012). That definition is for damage under the CFAA not loss. Loss is "any reasonable cost" incurred by a violation. ¶ 1030(a).

In conclusion, Shapiro adequately stated a claim against Respondent for violation of the MCFAA. At the direction of Respondent, Bennett knowingly accessed and obtained Shapiro's personal files and social media accounts without authorization or by exceeding authorized access. Further, Shapiro suffered a loss as a result of this violation.

III. THE CIRCUIT COURT ERRED IN GRANTING RESPONDENT'S MOTION TO DISMISS BECAUSE SHAPIRO PROPERLY STATED A

VALID CONVERSION CLAIM

The facts alleged in Shapiro's complaint establish a claim upon which relief can be granted. When an actor exercises dominion or control over a plaintiff's goods in a way that is in fact inconsistent with the plaintiff's rights, conversion occurs. Prosser and Keeton on Torts § 15 at 92 (5th ed. 1984). This Court in a previous decision adopted the Restatement (Second) of Torts definition of conversion. R. at 4. This Restatement provides: "Conversion is an intentional exercise of dominion or control over a [property] 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 [property]." § 222A(1) (1965).

Here, Shapiro states a valid claim. First, she can show that the Respondent intentionally exercised dominion over her LinkedIn ™ and Twitter ™ accounts. These accounts constitute convertible property because electronic programs are covered under the merger doctrine, which provides that intangible rights of ownership merged within a printed, tangible document representative of the whole will be covered in conversion actions. Like how possession of a credit card represents possession of a bank account, so too, possession of login pages with the new passwords to Shapiro's accounts represents possession of these accounts. Further, Respondent and Bennett should have known that Shapiro owned her accounts because not only did Respondent's policy disallow the company's possession of such accounts, but also Shapiro gave Bennett specific instructions regarding these accounts that Bennett disobeyed.

Second, the Respondent's interference with Shapiro's right to control her accounts was serious because the Respondent, through Bennett, permanently deprived Shapiro of her ability to access her network that she developed over ten years through LinkedIn ™ and Twitter ™. The value of these accounts can be determined in multiple ways, such that justice requires the Respondent to either return the accounts or to pay their value. Therefore, this Court should reinstate Shapiro's claim for conversion.

A. Shapiro's Accounts Constitute Convertible Property and Shapiro Establishes that She Owns Her Accounts

Shapiro's social media accounts constitute convertible property. Moreover, Shapiro establishes her ownership rights to her accounts.

1. Shapiro's Social Media Accounts are Convertible Property under the Merger Doc-trine.

Electronic social media accounts constitute property that can be converted. The Restatement (Second) of Torts and jurisprudence shows

proper application of conversion in Internet or computer related property. *See Kremen v. Cohen*, 325 F.3d 1024, 1034 (9th Cir. 2003) (conversion of domain name); *Nat'l. Sur. Corp. v. Applied Sys., Inc*., 418 So. 2d 847, 848 (Ala. 1982) (conversion of software programs); Restatement (Second) of Torts § 242. Section 242 of the Restatement (Second) of Torts provides that "where the conversion is of a document in which intangible rights are merged," a theory known as the merger doctrine, "the damages [of a conversion claim] include the value of such rights." Restatement (Second) of Torts §242(1); *see Thyroff v. Nationwide Mut. Ins. Co*., 460 F.3d 400, 405 (2d Cir. 2006) (conversion of access to a computer software system). While the Restatement (Second) of Torts, written in 1965, states that "it is at present the prevailing view that there can be no conversion…of such intangible rights as the goodwill of a business or the names of customers," it goes on to say, "[t]he process of extension has not … terminated." Essentially, "nothing said in this Section is intended to indicate that a proper case [for] liability for intentional interference with some other kind of intangible rights may not be found." Restatement (Second) of Torts §242 cmt f. Courts today are applying the remedy that best administers justice rather than looking to what property is the most tangible. *See Applied Sys., Inc.*, 418 So. 2d at 848 ("a theft of intangible property is a violation of the criminal law and should be civilly remediable").

Moreover, the credence to give to the "general rule" may also be thinner than it appears. A 2007 Massachusetts case, *In re TJX Cos. Retail Sec. Breach Litig*., denied a conversion claim within a motion to amend for information electronically stored with debit and credit cards that had been stolen. Though the First Circuit noted the district's resistance to follow other circuits that allow for conversion of intangible electronic property, the Circuit's review of the case in 2009 merely held that the lower court did abuse its discretion when it denied the claim because it could have been presented in the original complaint and did not rely on newly discovered facts. 564 F.3d 489, 500 (1st Cir. 2009). Also, while the D.C. Circuit allegedly does not entertain conversion actions for intangible property, they cite to Maryland state law precedent for this refusal. *Xereas v. Heiss*, 933 F. Supp. 2d 1, 7 (D.D.C. 2013) (referencing *Council on Am. Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 340 (D.D.C. 2011)).

This Court should look to the cited *Gaubatz* Maryland case at page 340, where that court held the case was decided on other grounds, as the plaintiff failed to allege that the defendant had exercised "ownership dominion or control" over the plaintiff's property. 793 F. Supp. 2d at 340. Decisions made on other grounds can hardly be called a general rule.

A simple example of convertible intangible property is electricity: if a converter takes an electric company's electricity without paying for it

by circumventing the meter, courts do not bypass justice simply because electricity is intangible. *See DeLong v. Osage Valley Elec. Cooperative Ass'n.*, 716 S.W. 2d 320 (Mo. App. 1986). With today's dependence on computers, "it would be a curious jurisprudence that …[t]orching a company's file room would then be conversion while hacking into its mainframe and deleting its data would not." *Kremen*, 325 F.3d at 1034.

Under the merger doctrine, a plaintiff may show a conversion action where the intangible property is merged with a document. For example, in *Thyroff*, an insurance agent sued his former company for conversion where, following his termination, the company repossessed his remote access software account in which he had created client contacts and wrote notes regarding those contacts while at the company. 460 F.3d at 405. Even where New York law stated "a conversion claim law may not lie for intangible property," the Court held conversion occurred because Thyroff's claims involved not only personal lists but also access to the programs themselves. *Id.*

The Second Circuit analogized to a stock certificate, where intangible rights to the stock merged in the tangible stock certificate. *Id.* Thus, the merger doctrine properly extended to the remote access account because the electronic data merged into the computer program. *Id.* Moreover, merger doctrine applies even where the tangible documents only shows a right to the property without embodying the entire thing. *Stebbins v. N. Adams Trust Co.*, 243 Mass. 69, 76, 136 N.E.880, 884 (1922) (savings account passbook constituted convertible property because, at that time, passbooks were required to make a withdrawal); *Gauntt v. United Ins. Co. of Am.*, 853 F. Supp. 1382, 1385 (M.D. Ala. 1994) (life insurance policy constituted convertible property where it was the sole evidence of the terms, such that defendant's retention of the policy denied the plaintiff her ability to know her rights).

Here, Bennett changed the passwords on each of Shapiro's social media accounts and effectively cut off Shapiro's access to control them. R. at 4; *see Gauntt*, 853 F. Supp. at 1385. Shapiro wants to be able to reach her followers and message her contacts. R. at 5; *see Stebbins*, 243 Mass. at 76. If the login pages for the accounts were printed out with Shapiro's usernames and passwords, this document fits under the merger doctrine. *See Thyroff*, 460 F.3d at 405. This document would be in the Respondent's, not Shapiro's, possession given Bennett's actions. *See* R. at 3. Therefore, the social media accounts, while intangible, constitute convertible property.

2. Shapiro Establishes Valid and Exclusive Ownership of Her Accounts.

Shapiro owns the accounts because she had the power to limit other's access to the accounts. Moreover, the Respondent does not own the

accounts because its own policy states Bennett would not have access to Shapiro's accounts to materially alter them for Valentini. Ownership rights can be established even where a former employee creates work for a company and the company refuses to pay for the work they take. *Fed. Fire Prot. Corp. v. J.A.Jones/Tompkins Builders, Inc*., 267 F. Supp. 2d 87, 90-91 (D.D.C. 2003). In *Federal Fire*, a general contractor refused to pay for but continued to use his former subcontractor's construction drawings with another subcontractor on the same project. 267 F. Supp. 2d at 92. The Court held in favor of the subcontractor, reasoning that the allegation of ownership rights was "clearly sufficient to justify an award of punitive damages for the intentional tort of conversion." *Id.* at 91. The Court also noted that in the complaint, the drawings and the breached business contract were distinct harms, and conversion applied to the drawings. *Id.* at 92.

Moreover, when the property is wrongfully taken, demand and refusal is not required to show that a plaintiff has ownership rights. For example, where a former shareholder brought an action against a technology company for conversion of his stock certificates, the plaintiff showed he had a valid ownership right to the certificates when he produced the company's pledge agreement with him. *Guice v. Sentinel Tech., Inc*., 294 Ill. App. 3d 97, 112, 689 N.E.2d 355, 366 (Ill. App. Ct. 1st Dist. 1997). The plaintiff in *Guice* had to prove that he had demanded the property back and that the company had refused his demand only because, the Court noted, the defendant there had rightfully acquired the property. *Id.* at 111.

Unlike *Guice*, showing demand and refusal is not required in this case because the Respondent's own policy states Bennett would not have access to Shapiro's accounts to materially alter them for Valentini, so this case involves a wrongful taking. R. at 1, 3; *cf. Guice*, 689 N.E.2d at 365. Like *Federal Fire*, the paper mill did not own the subcontractor's drawings, the company that paid for the paper did not own the subcontractor's drawings, but rather the subcontractor owned the drawings because he put in the effort. 267 F. Supp 2d at 92. Here, even if Shapiro did not fill out the form creating the account, Shapiro was the one giving the accounts substance by promoting the company. R. at 2. Moreover, she establishes ownership where she used the accounts not only to promote the company but also to post and follow family, friends, and other acquaintances, so Shapiro did not waive her right to these accounts, where her limiting instruction served as a clear indication she did not waive control over the accounts. R. at 1; *see Guice*, 689 N.E.2d at 363 (oral notice supports a contention that plaintiff did not waive rights to the property). A mistaken belief by Bennett that she only needed a CEO's authorization to access the account will not relieve her or the Respondent of liability where she should have known of the company policy, because the "the viability of a conversion claim turns on which party

holds title when the purported conversion takes place." *Sun Coast Merch. Corp. v. Myron Corp.*, 393 N.J. Super. 55, 84, 922 A.2d 782, 800 (App. Div. 2007).

B. The Respondent Seriously Interfered with Shapiro's Ownership Rights to Her Social Media Accounts by Locking Her out of Them Through Bennett's Changing of The Passwords.

The Respondent intended to seriously interfere with Shapiro's property rights to access and operate her accounts. The Restatement (Second) of Torts lists factors in determining "the seriousness of the interference and the justice of requiring the actor to pay the full value," including: (a) the extent and duration of the actor's exercise of dominion or control; (b) the actor's intent to assert a right 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 property; and (f) the inconvenience and expense caused to the other. Restatement (Second) of Torts §222A(2). The factors relating to a serious interference are disjunctive. Also, intent need not be wrongful for justice to require payment: the intent need only be to interfere with the property of another. *See Myron Corp.*, 922 A.2d at 800.

The growing rule in common law is that conversion actions for social media accounts taken by employers survive motions to dismiss because interferences for which relief can be granted occur. *See, e.g., Eagle*, No. CIV.A. 11-4303, 2012 WL 4739436 (E.D. Pa. Oct. 4, 2012); *PhoneDog v. Kravitz*, No. C11-03474 MEJ, 2011 WL 5415612, at *1 (N.D. Cal. Nov. 8, 2011). In *Eagle* mentioned above, the CFAA count failed but the plaintiff won on her conversion count. The Court held the conversion claim should stand because the defendant had failed to properly raise and brief the issue for summary judgment. *Id.* at *9 n.6.

The Court also found that the defendant seriously interfered with Dr. Eagle's LinkedIn ™ account because: (a) the former employer's exercise of control over the account was for an extended period of time; (b) the intent of the company was to "mine" and "own" the account that was established by the plaintiff; (c) their good faith in their policy, though they changed the password to the account the day after she was terminated; (d) the interference with the account was ongoing; (e) the harm to the plaintiff was that she was deprived of her ability to reconnect with family, friends and colleagues over the site as well as her ability to build her relationships, both social and professional; and (f) that the plaintiff alleged harm in that those searching to connect with her online were misrouted to a LinkedIn ™ page featuring a new employee's name and photograph, but Dr. Eagle's honors and awards, recommendations, and connections remained intact. *Id.* at *1; *see* Restatement (Second) of

Torts §222A(2). On these facts alleged, the Court did not dismiss the claim, so it must have reasoned that the petitioner properly stated grounds on which relief could be granted even where defendant failed to brief the issue. *Eagle*, No. CIV.A. 11-4303, 2012 WL 4739436 at *9, n. 6. After all, "a trial court has the power to dismiss an action sua sponte for failure to comply with the rules of civil procedure," including Fed. R. Civ. P. 12(b)(6). *E.g., Trest v. Cain*, 522 U.S. 87, 90 (1997).

Additionally, when an employee was granted limited access to another's social media account and used it beyond the scope of the employment agreement, the conversion action survived a respondent's motion to dismiss because: (1) the owner sufficiently pled that the employee exceeded the scope of their granted authority with the account which (2) led to serious interference with the owner's exercise of its property rights. *PhoneDog*, No. C11-03474 MEJ, 2011 WL 5415612 at *1. The Court held that there was serious interference because: (a) the employee with limited access to the owner's account refused to surrender the account following the separation; (b) he changed the Twitter ™ handle inconsistent with the owner's right of control; (c) his good faith was circumspect where the owner expressly limited his access and the former employee overstepped that limitation; (d) the employee's interference was ongoing; (e) that the owner's harm was based both on right to possess the account as well as the interference with its access and use; and (f) that the employee harmed the owner where owner could not use the handle and the employee now used the handle to promote a competitor. *Id.* at *4-5, *9; *see* Restatement (Second) of Torts §222A(2). Like *Eagle*, the former employee Kravitz was granted access to the passwords, but he did not abide by the limiting instructions given to him by the owner after he was let go. *PhoneDog*, No. C11-03474 MEJ, 2011 WL 5415612 at *9; *Eagle*, No. CIV.A. 11-4303, 2012 WL 943350 at *4-5. The conversion claim survived because the owner had adequately alleged that it had the right of possession and that the conversion was knowing or intentional. *Id.* at *9.

So too here, all Restatement (Second) of Torts §222A(2) conversion factors are met. First, Bennett's action as the Respondent's agent materially altered the accounts when she changed the names on the accounts and the photos to reflect Valentini rather than Shapiro, R.at 3; *see Eagle*, No. CIV.A. 11-4303, 2012 WL 943350 at *1; Restatement (Second) of Torts §222A(2)(a). Second, the Respondent asserted ownership rights inconsistent with Shapiro's right of control when it had Bennett transfer the accounts, R. at 3; *see Eagle*, No. CIV.A. 11-4303, 2012 WL 943350, at *1; *PhoneDog,* No. C11-03474 MEJ, 2011 WL 5415612, at *4; Restatement (Second) of Torts §222A(2)(b).

Third, the Respondent's good faith lacks value where Shapiro expressly limited Bennett's access and there was a policy in place that the Respondent would not have access. R. at 3, 4-5; *see Eagle*, No. CIV.A.

11-4303, 2012 WL 943350, at *1; *PhoneDog,* No. C11-03474 MEJ, 2011 WL 5415612, at *9; Restatement (Second) of Torts §222A(2)(c). Fourth, the Respondent continues to keep passwords from Shapiro, and intends to do so permanently, R. at 3; *see Eagle*, No. CIV.A. 11-4303, 2012 WL 943350, at *1; *PhoneDog*, No. C11-03474 MEJ, 2011 WL 5415612, at *4; Restatement (Second) of Torts §222A(2)(d). Fifth, the accounts now have Shapiro's previous tweets and associations, honors, and awards respectively, but the name and photo associated with the accounts are of Respondent's new CEO, Valentini, a competitor. R. at 3; *see Eagle*, No. CIV.A. 11-4303, 2012 WL 943350, at *1; Restatement (Second) of Torts §222A(2)(e). Lastly, the Respondent continues to interfere with Shapiro's possessory right to information within the accounts, as well as her right to access the programs allowing her to build her network by reaching out to followers and contacts associated with her within these accounts. R. at 2, 4; see *PhoneDog*, No. C11-03474 MEJ, 2011 WL 5415612, at *4-5, 9; Restatement (Second) of Torts §222A(2)(f).

Like *Eagle*, Shapiro is the former CEO who was terminated and established her LinkedIn ™ account while she worked at U.S. Apparel. However, she used the accounts not only to promote the company but also to "reconnect with family, friends, and colleagues," building social as well as professional relationships. R. at 1; *see Eagle*, No. CIV.A. 11-4303, 2012 WL 943350, at *1. Shapiro's assistant Bennett assisted Shapiro in maintaining her account, having access to the password, but unlike *Eagle*, no policy was in place that allowed Respondent to effectively "own" the LinkedIn ™ account or "mine" the information by having Bennett access the passwords. R. at 1 ("contrary to U.S. Apparel's policy"); *cf. Eagle,* No. CIV.A. 11-4303, 2012 WL 943350, at *1. So, the Respondent's actions seriously interfere with Shapiro's ownership rights, thus constituting conversion.

C. Shapiro's Right to Control the Information within the Accounts is Valuable Such That Justice Requires the Respondent to Pay Her the Full Value of the Accounts, which can be Determined Multiple Ways.

Lastly, the value of Shapiro's social media accounts can be determined in a variety of ways. An owner entitled to a conversion judgment can recover based on either: (1) the value of the subject matter or her interest in it at the time and place of the conversion; or (2) in the case of commodities of fluctuating value, the highest replacement value of the commodity within a reasonable period during which she might have replaced it. Restatement (Second) of Torts §927(1) (1979).

A converter may also be justly required to pay the full value of the property through: (1) the return the stolen property, *see Kunstsammlungen Zu Weimar v. Elicofon*, 678 F.2d 1150, 1165 (2d Cir. 1982) (judgment in favor of art museum required respondent to return

stolen paintings); (2) attorney fees, *see Welch v. Kosasky*, 24 Mass. App. Ct. 402, 406 (1987) (damages and attorney fees related to converted silverware); and (3) even punitive damages. *See Fed. Fire*, 267 F. Supp. 2d at 92. Here, methodologies exist that determine the value of a person's social media accounts: Twitter's ™ analytics platform; closed-loop marketing analytics, or marketing relying on internet traffic data; as well as educated estimates are just three sources Shapiro could have used in proving her case. Dan Zarella, *How to Calculate the Value of Your Social Media Followers*, HubSpot (Nov. 26, 2012), http://bit.ly/NJmeEH.

Factors in these valuations include: how many people "follow" the person; how many "unfollow" the person each day; how often tweets or posts are posted; how many clicks those posts are receiving; the account's visit-to-lead rate; and the average conversion value of that vision-to-lead rate. *Id.* As such, the value of these accounts can be calculated. Additionally, calculating the value of ten years' worth of work connecting people to your profile, posting, and tweeting would require a detailed factual allegation not required at this stage of the pleadings. *See Iqbal*, 556 U.S. at 678 (pleadings must show content that allows the court to draw the reasonable inference); *Bell Atl. Corp. v. Twombly*, 127 S. Ct. 1955, 1964 (2007) (while plaintiff must provide grounds demonstrating its entitlement to relief, he or she need not plead detailed factual allegations to survive a 12(b)(6) motion). Finally, the Respondent may also be justly required to repay Shapiro by: (1) returning her accounts; (2) paying her attorneys' fees; and possibly even (3) paying punitive damages. *See Elicofon*, 678 F.2d at 1165; *Welch*, 24 Mass. App. Ct. at 406. As such, the Respondent should be justly required to pay Shapiro the full value of her social media accounts where the value is determinable by a jury using the previously mentioned types of relief.

Therefore, Shapiro's social media accounts are valuable, convertible property that Shapiro established she owns and with which the Respondent intentionally interfered. So the trial court erred in its dismissal order of Shapiro's count III for conversion. This Court should reinstate Shapiro's conversion claim.

CONCLUSION

For the foregoing reasons, the judgment below should be reversed.

Dated: October 1, 2014.

Respectfully submitted,

/s/_____
Attorneys for the Petitioner