UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 2 Article 4

2014

The Thirty-Third Annual John Marshall Law School International Moot Court Competition in Information Technology and Privacy Law: Bench Memorandum, 31 J. Marshall J. Computer & Info. L. 237 (2014)

Adam Florek

Anisha Mehta

Danielle Young

Michael Greene

THE 33RD ANNUAL JOHN MARSHALL INTERNATIONAL MOOT COURT COMPETITION IN INFORMATION TECHNOLOGY AND PRIVACY LAW

OCTOBER 23-24, 2014

BENCH MEMORANDUM

ADAM FLOREK

ANISHA MEHTA

DANIELLE YOUNG

MICHAEL GREENE

INTRODUCTION

Petitioner Jane Shapiro appeals the Circuit Court of Nashville County's order granting the motion of Respondent, U.S. Apparel, to dismiss Petitioner's three-count complaint. Petitioner alleged an intrusion upon her seclusion, computer fraud, and conversion.

The first issue in this case is whether Respondent's access to Jane Shapiro's corporate desktop computer files and disclosure of private information relating to her business dealings with Hanoi Labor, Co. was an intentional intrusion upon her seclusion. The second issue is whether Sharon Bennett, as an agent of U.S. Apparel, committed computer fraud when she knowingly accessed Shapiro's corporate desktop computer, her personal files on that computer, her social media accounts, and her personal files on that computer without Shapiro's authorization. The third issue is whether Bennett, acting as an agent of U.S. Apparel intentionally converted the LinkedIn and Twitter accounts along with the information contained therein, thereby interfering with Shapiro's right to control her accounts.

PROCEDURAL HISTORY

Shapiro filed her complaint in the Circuit Court of Nashville County, alleging intrusion upon seclusion, computer fraud, and conversion. U.S. Apparel moved to dismiss all three counts, and the Circuit Court granted the motion to dismiss on all three counts. The Circuit Court held that Shapiro had failed to state a claim upon which relief can be granted, pursuant to State of Marshall Rules of Civil Procedure, § 12(b)(6). Shapiro appealed, and the Appellate Court of the State of Marshall reasoned that the three questions raised were of such importance that they should be decided by the Supreme Court, and therefore certified them to the state's Supreme Court. The Supreme Court of the State of Marshall accepted the case for review and designated Shapiro as Petitioner and U.S. Apparel as Respondent

ANALYSIS

I. COUNT I: INTRUSION UPON SECLUSION

A In General

Jane Shapiro has brought a claim of intrusion upon seclusion against her former employer U.S. Apparel. According to the Restatement (Second) of Torts § 652B, which has previously been adopted by the Supreme Court of Marshall, "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."[1] Liability for this tort arises if the following elements are met: there must be an unauthorized intrusion or prying into the plaintiff's seclusion; the intrusion must be offensive or objectionable to a reasonable person; the matter upon which the intrusion occurs must be private; and anguish or suffering must result from the intrusion.[2]

B. Elements of Intrusion Upon Seclusion

1. An unauthorized intrusion or prying into the plaintiff's seclusion

The first element that Shapiro must prove is that U.S. Apparel committed an unauthorized intrusion or prying into Shapiro's seclusion. The Restatement (Second) of Torts provides that the "tort of intrusion into another's seclusion is not based on publication or publicity, but on the offensive prying into another's home, personal belongings, or conversations."[3] First, Shapiro will argue that U.S. Apparel intentionally intruded upon her seclusion by accessing her personal computer files, located on her office desktop, in a folder labeled "Personal." Second, she will likely argue that Bennett's disclosures of private information obtained from Shapiro's personal files regarding her business dealings with Hanoi Labor, Co. to Shapiro's replacement Victor Valentini and subsequently to U.S. Apparel Chairman Thomas Stephan were further intrusions upon her seclusion.

Valentini instructed Bennett to access files on Shapiro's desktop computer. The folder that was located and opened was labeled "Personal." Subsequently, Bennett opened a file labeled "Threads Business Plan" therein and disclosed its contents to Valentini, who reported it to Stephan. Upon discovering the folder labeled "Personal," Bennett should have proceeded to delete the folder or forward its contents to Shapiro herself. Moreover, Bennett and Valentini should have expected to find private information in the folder, which suggests their prying was intentional.

Shapiro will also argue that by labeling the folder "Personal," she put Bennett on notice as to the personal and private nature of the folder's contents, and that Bennett therefore knew or should have known that she lacked authority to permit others to access the files. Although liability results from the intrusion into private matters rather than any subsequent publication, U.S. Apparel's press conference and public disclosure of Shapiro's business plans makes her argument even more compelling.[4]

---

1. Record at 3; RESTATEMENT (SECOND) OF TORTS § 652B (1977).
2. *Id.*
3. *Id.*
4. *Id.*

In defense, U.S. Apparel will argue that no intrusion occurred and that the company was authorized to access information stored on the computer. The desktop computer was U.S. Apparel's property and was under its control both during and after Shapiro's employment, and the information that Bennett accessed was stored on that computer; the company's access to that information was therefore neither an intrusion nor unauthorized. Furthermore, Shapiro herself caused her data to be synced from her personal devices to the desktop computer, and she could have canceled that synchronization upon leaving the company if she did not want to continue making the data accessible to the company.

In addition, U.S Apparel will ask that this court follow the ruling set forth in *Maremont v. Susan Fredman Design Grp*.[5] In *Maremont*,[6] an interior decorator filed suit against her employer after the employer authored frequent posts using the employee's personal Facebook and Twitter accounts. The court ruled that the employee failed to develop her argument that employer's intrusion onto her personal "digital life" was actionable under the common law theory of unreasonable intrusion upon the seclusion of another.[7] Similarly, U.S Apparel will argue that Shapiro has also failed to develop the argument that U.S Apparel's actions are actionable under the common law theory of unreasonable intrusion upon seclusion. Finally, the subsequent disclosure of the information to others is irrelevant to whether an intrusion occurred, because the intrusion tort turns solely upon the unauthorized access, rather than any further disclosure.

2. The intrusion must be offensive or objectionable to a reasonable person

Under the Restatement (Second) of Torts, "[t]here is no liability unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable person would strongly object."[8] Shapiro may argue that accessing a folder labeled "Personal" is inherently offensive and objectionable. A reasonable person would strongly object to an individual reading the contents of such a file, and further object to the file being disseminated further or published. The base of Shapiro's argument will likely be that a party has a reasonable expectation of privacy in personal information stored on a device that is synced with personal devices. The argument is especially strong when materials are clearly labeled as being personal in nature.

---

5. Maremont v. Susan Fredman Design Grp., Ltd., 772 F.Supp.2d 967 (N.D. Ill. 2011).

6. *Id.*

7. *Id.* at 973.

8. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

In response, U.S. Apparel will argue that any intrusion that may have occurred was not offensive because it owned the computer on which the information was stored, and it accessed the information because its own business interests were at stake, and not because of any inappropriate interest in Shapiro's personal affairs. The second element of the tort requires "a prying or intrusion, which would be offensive or objectionable to a reasonable person, into a person's private concerns."[9] In *Sitton*, an employer's access to email stored on an employee's computer was not sufficiently unreasonable to constitute an invasion of privacy. The employer was investigating a matter involving its own business interests, and the court held that its access was therefore reasonable under the circumstances.[10] U.S. Apparel will likely ask the court to hold that the act was reasonable because the information was stored on its own computer and the company's legitimate interests were at stake.

3. Private Matters

The third prong of any claim for intrusion upon seclusion requires "the matter upon which the intrusion occurs must be private."[11] Here the court must look to the nature of the data recovered from the desktop computer and determine whether it was reasonably expected to be private.

Here Shapiro will argue that the business plans were private in nature. The court in *Vega v. Chicago Park District* gave examples of private matters and included therein "future work plans."[12] Here the documentation found on the desktop computer was for an as of yet unrealized company, Threads, that Shapiro would establish and presumably run the in the wake of her removal from U.S. Apparel. This future career planning is certainly sufficient to rise to the level of future employment.[13]

Further, Shapiro should point to the distinction between personal and private facts. The fact that information may be personal in nature does not make it private.[14] Private facts are those that are embarrassing or offensive if made public and include future work plans.[15] The tort of intrusion upon seclusion also applies to actions involving prying into private matters such as "opening a person's mail, searching a per-

---

9. Sitton v. Print Direction, Inc., 718 S.E.2d 532, 537 (Ga. Ct. App. 2011).

10. *Id.*

11. Melvin v. Burling, 490 N.E.2d 1011, 1013-1014 (Ill. App. Ct. 1986).

12. Vega v. Chicago Park Dist., 958 F. Supp. 2d 943, 959 (N.D. Ill. 2013).

13. *See generally* Johnson v. K mart Corp., 723 N.E.2d 1192 (Ill. App. Ct. 2000) (expanding on what future work plans may entail).

14. *Vega*, 958 F. Supp. 2d at 959.

15. *Id.*

son's safe or wallet…"[16]

U.S. Apparel will most likely dispute that the data taken was private, citing the third party disclosure doctrine, which holds that one does not have a legitimate expectation of privacy in data voluntarily turned over to a third party.[17] Shapiro caused the materials in question to be located on the U.S. Apparel-owned computer, essentially turning the materials over, in some capacity, to US Apparel. This disclosure stripped the data in question of its private status and means that Shapiro ran the risk of U.S. Apparel further disclosing the data.

U.S. Apparel's argument however, is convoluted by the BYOD[18] nature of the devices. Because Shapiro used her personal laptop and cell phone for company purposes, her relationship with the U.S. Apparel computer was more complex than simply directly turning over the information in question. Her devices synced automatically with her office computer, potentially exposing otherwise personal files to the company. However, the device and materials synced may have been configurable to limit the synced information to only company related data.

Finally, both parties should address the reasonableness of Shapiro's expectation of privacy in her folder labeled "Personal" on U.S. Apparel's office computer. When evaluating the reasonableness of one's expectation of privacy there is typically a two-part analysis: (1) whether the individual has an expectation of privacy; and (2) whether that expectation is one which society is willing to accept as reasonable.[19] Again, because of the BYOD practice this presents a difficult issue. Regardless, when evaluating the second prong, society's acceptance of the reliance as reasonable, the totality of the circumstances should be taken into account and the nature of the problem examined.

4. Anguish & Suffering

The final prong of a tort claim for intrusion upon seclusion is that the intrusion caused anguish and suffering.[20] Injury is not merely presumed from the intrusion, the plaintiff must prove that an actual injury resulted.[21]

U.S. Apparel may argue that any harm suffered by Shapiro result-

16. *Id.*

17. In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 120 (E.D.N.Y. 2011)(citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

18. BYOD, or Bring Your Own Device, refers to a company policy permitting employees to bring personally owned mobile devices to the workplace.

19. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (establishing the now fundamental two-part test to evaluate an individual's privacy expectation in any setting); see also Smith v. Maryland, 442 U.S. 735, 740 (1979).

20. Melvin v. Burling, 490 N.E.2d 1011, 1013-1014 (Ill. App. Ct. 1986).

21. Schmidt v. Ameritech Illinois, 768 N.E.2d 303, 316 (Ill. App. Ct. 2002).

ed not from any access to her private information, but from the subsequent publication of that information. The basis for intrusion upon seclusion is the intrusive and offensive prying into another's privacy, not publication or publicity.[22] Here Shapiro did not suffer any harm due to the intrusion itself; the harm came from subsequent publication of her plans along with indictment for the labor conditions at the factory where she planned to produce the garments. Because the harm did not flow from the intrusion this element cannot be met.

Shapiro, however, may argue that the intrusion itself sufficiently spoiled her business plans by making them known to her major competitor, U.S. Apparel. The intrusion alerted her primary competitor to her design, business plan, and manufacturer. However, she would bear the burden of proving that her injuries were caused by that access rather than by the subsequent publicity.

II. COUNT II: COMPUTER FRAUD

A. In General

The State of Marshall Computer Fraud and Abuse Act, § 1030(a) (2008) provides in part that:

> 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 damages or injunctive relief or other equitable relief.

Similarly, the federal Computer Fraud and Abuse Act ("CFAA") provides that a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" or "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value" is subject to criminal liability.[23] Because of the similarity of these statutes, cases applying the federal statute are likely to be helpful in interpreting the Marshall statute.

The Marshall statute applies when "a person (1) knowingly accesses a computer without authorization or exceeding authorized access; and (2) obtains personal information through such conduct, thereby

---

22. RESTATEMENT (SECOND) OF TORTS § 652B (1977); Lovgren v. Citizens First Nat. Bank of Princeton, 534 N.E.2d 987, 989 (Ill. 1989).

23. 18 U.S.C. § 1030(a)(2),(a)(4) (2012).

committing computer fraud."[24] Furthermore, use of a third party's computer to access a website, rather than one's own computer, does not preclude liability under the CFAA.[25]

B. Elements

1. Knowingly Accessing a Computer Without Authorization or Exceeding Authorization

It is not in dispute that Bennett had knowledge of accessing her employer's desktop computer. However, it is in dispute whether she had authorization, or exceeded her authorization, and these issues may depend upon who was able to offer authorization. U.S. Apparel will argue that Bennett's access to the employer-issued desktop computer, where Shapiro's files were located, was within her authorized access.

First, the access took place on a company-issued device and therefore Bennett did not trespass onto a personal device to receive information.[26] In addition, Bennett acted under the direction of Valentini, who had authority over the company's computers and authorized Bennett to use the computer as well as to obtain information for legitimate U.S. Apparel business purposes.[27]

Shapiro will claim that U.S. Apparel exceeded its authorization by granting Bennett access to Shapiro's "Personal" folder, exceeding her authorization to access only business-related information.[28] An employer gives an employee "authorization" to access a company computer, within the meaning of the CFAA, when the employer gives the employee permission to use it.[29] Here, Shapiro will argue that Bennett was only given permission to access business related information, not her personal files.

U.S. Apparel will argue that case law and statutory language do not distinguish between the authorization of accessing business or personal information on a computer, but rather only talks about authoriza-

---

24. State of Marshall Computer Fraud and Abuse Act, § 1030(a) (2008) (R. 4).

25. eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (directing a user's computer to the eBay website, rather than using the defendant's own computer, does not prevent a claim of unauthorized access).

26. *See* City of Ontario. v. Quon, 560 U.S. 746, 750 (2010) (rejecting Fourth Amendment challenge to city's warrantless access to personal text messages on city-owned pagers).

27. *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 620 (E.D. Pa. 2013) (departing managers did not access company's computers "without authorization," nor "exceed authorized access," in violation of the CFAA because they had permission and passwords to use the company's trade secret and confidential information for legitimate business purposes and did not have restrictions in what they could download).

28. Record at 2.

29. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).

tion of access to the computer itself. Therefore, U.S. Apparel will argue that Bennett had authorization to access the computer under the direction of both Shapiro and Valentini.

The federal CFAA includes a definition that may support Shapiro's position. "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the current user is not entitled so to obtain or alter."[30] Although Shapiro provided Bennett with access to the computer temporarily, Bennett arguably exceeded her authorization by obtaining personal information and altering her personal accounts within that computer.[31]

In addition, the order to change Shapiro's passwords terminated Shapiro's own access to her personal files and accounts, which constitutes a significant alteration in her arguably protected information.[32]

2. Obtaining Personal Information Through the Unauthorized Access

Employers may be given access to a computer with business-related information on it when there is a "legitimate interest in unfettered access" to the computer and it outweighs any harm to the employee.[33] However, Shapiro will argue that U.S. Apparel has not or cannot establish that it has a legitimate interest to such unfettered access to the server, and therefore its interest cannot outweigh the harm done to Shapiro. U.S. Apparel will argue that there is a legitimate interest outweighing any harm done to Shapiro. Therefore, in order to assess the level of harm here, one must look to whether the content obtained was protected personal information or unprotected business-related information.

U.S. Apparel will argue that access to the social media accounts was pertinent to its business and therefore outweighed any potential harm to Shapiro. The Twitter account bore the company's name ("@U.S.Apparel_Shapiro") and both it and the LinkedIn account were used in furtherance of the business.[34] For instance, the accounts were used to promote and communicate with the public and the professional

---

30. 18 U.S.C. § 1030(e)(6); *see also Id*.

31. *But see Brekka*, 581 F.3d 1127 (holding that employee exceed authorized access when he e-mailed documents from his work computer to himself and to his wife while he was still employed).

32. *See* Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006) (explaining that employee's alleged installation of program on employer's computer that caused deletion of files would violate the CFAA).

33. Kimberly Peretti & Bruce Sarkisian, *Peering into Personal Space: Investigating Employee-Owned Mobile Devices*, 17 J. INTERNET L. 3, 4 (2014) (quoting Enargy Power Co. v. Xiaolong Wang, No. 13–11348–DJC, 2013 WL 6234625 (D. Mass. Dec. 3, 2013)).

34. Record at 1.

network on behalf of the company.[35]

Shapiro will argue that her social media accounts were primarily personal accounts even though she also used them in connection with her professional responsibilities. Her content and passwords should be protected because she had control over them and had a heightened expectation of privacy with respect to the content and passwords. Additionally, Shapiro accessed these networks predominantly through her personal devices.[36] She used the accounts for personal use in addition to her professional duties, such as connecting with friends and family, listing her achievements and associations, and building her reputation.[37] Shapiro may also argue that she provided the passwords to Bennett through her role as a personal assistant rather than a strictly business capacity.[38] Furthermore, Shapiro explicitly stated Bennett did not have authority to access Shapiro's social networking accounts without her direct authorization.[39]

Shapiro will also argue that the business plans, entitled "Threads Business Plan," was unrelated to U.S. Apparel and constituted personal information that was unintentionally synced from her personal devices to her desktop computer.[40] However, this case may be considered analogous to *Sitton v. Print Direction*, where an employee used a combination of work and personal devices to create a business plan for a new and similar competing business. The employer was authorized to access the information due to the nature of the content and the fact that it was accessible from a company computer.[41]

III. COUNT III: CONVERSION

A. Overview

In her third count, Shapiro brought a common law conversion claim.[42] The Supreme Court of the State of Marshall has adopted the Restatement (Second) of Torts' definition of conversion:

(1) Conversion is an intentional exercise of dominion or control over a

---

35. *Id*.

36. *See* Peretti & Sarkisian, supra note 33, at 4. ("If employers access data on employee-owned devices, employees can make a strong case for invasion of privacy in the event the employees can prove that they had a reasonable expectation of privacy in their devices.").

37. Record at 2.

38. Record at 1.

39. *Id*.

40. Record at 2.

41. Sitton v. Print Direction, Inc., 718 S.E.2d 532, 535 (Ga. Ct. App. 2011) (holding that access by employer was not "without authority" under similar statute).

42. Record at 4.

> 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.

A common law claim of conversion must first establish the intentional interference of another's property, and second that the interference was of such gravity that justice requires the other to pay full value of the property. Conversion is an "intentional exercise of dominion or control" of another person's property.[43] The exercise of dominion or control must "seriously interfere with the right of another to control it," such that the actor "may justly be required to pay the other the full value of the chattel."[44]

Shapiro must first establish that the LinkedIn and Twitter accounts, as well as the information contained in them, are in fact property for purposes of her conversion claim.45 Few states have recognized electronic data, such as domain names and computer-stored data, as recognized property under conversion claims.46 Shapiro will argue that

---

43. RESTATEMENT (SECOND) OF TORTS §222A (1965).

44. *Id*.

45. Zoe Argento, *Whose Social Network Account? A Trade Secret Approach to Allocating Rights*, 19 MICH. TELECOMM. & TECH. L. REV. 201, 273 (2013) (noting that courts are in the process of recognizing that social media accounts like Twitter are tangible property and should be given similar protections as other tangible property, and the trend is to view conversion claims as applicable to the theft of social media accounts and the information contained in them).

46. *See* Famology.com Inc. v. Perot Systems Corp., 158 F. Supp. 2d 589 (E.D. Pa. 2001) (applying Pennsylvania law, conversion could not be brought for misappropriation of domain names because they were not tangible property); *see also*, In re TJX Companies Retail Sec. Breach Litigation, 527 F. Supp. 2d 209 (D. Mass. 2007) (applying Massachusetts law, credit card information was aggregate data is intangible information and not property as recognized under common law conversion claims); *but see* Kremen v. Cohen, 337 F.3d 1024, 1033 (9th Cir. 2003) (allowing claim for conversion of domain name under California law); *see also* Astroworks, Inc. v. Astroexhibit, Inc., 257 F.Supp.2d 609, 618

the characteristics of her social network accounts resemble typical personal property.[47] Shapiro will argue she used passwords to protect her work, as her use of the accounts to increase the brand name and recognition represent the "fruits of her labor," which transform the accounts into her personal property.[48]

U.S. Apparel is likely to argue that the information Shapiro is claiming was converted is no more than aggregate data, similar to bank or credit card information.[49] Intangible property interests in customer information and "followers" on Twitter are not as protectable, as the common law only protects tangible property from conversion.[50] However, California law apparently does recognize conversion of intangible property, especially when there is a connection between paper or electronic documents.[51]

Shapiro must prove that Bennett, acting as an agent of U.S. Apparel, intentionally interfered with her dominion or control of the LinkedIn and Twitter accounts, as well as the information contained in and the contacts and followers associated with them. Shapiro will argue that the changing of the name of the Twitter account name from "@U.S.Apparel_Shapiro" to "@U.S.Apparel_Valentini" demonstrates the intentional interference with her dominion of the account. Changing the passwords for these accounts, while maintaining them as active accounts, also shows the control intended by U.S. Apparel.[52]

U.S. Apparel will argue that the changing of the Twitter account name is similar to the change in a domain name and that Shapiro never had full property rights in the account as it was a component of her position while at the company. The loss of Shapiro's position precluded any further use by Shapiro of the Twitter account and therefore it was the right of U.S. Apparel to repurpose it.[53] However, Shapiro can argue that the ability for the Twitter account to be renamed shows that it is her property which was intentionally converted, and that U.S. Apparel could similarly create a new account for the new holder of the position

---

(S.D.N.Y. 2003) (allowing claim for conversion of website under New York law).

47. Argento, *supra* note 45, at 274; Val D. Ricks, *The Conversion of Intangible Property: Bursting the Ancient Trover Bottle with New Wine*, 1991 B.Y.U. L. REV. 1681, 1682 (1991) (previously held views of dominion and chattel have been inadequate at providing the required justice when conversion claims have been denied because they could not meet the rigid standards, as historically was required).

48. Argento, *supra* note 44, at 273.

49. In re TJX Companies Retail Sec. Breach Litigation, 527 F. Supp. 2d 209.

50. *Id*.

51. Terarecon, Inc. v. Fovia, Inc., No. C 05-4407 CW, 2006 WL 1867734 (N.D. Cal. July 6, 2006).

52. Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272 (N.Y. 2007).

53. March Madness Athletic Ass'n L.L.C. v. Netfire, Inc., 162 F. Supp. 2d 560 (N.D. Tex. 2001).

from which she had been terminated.[54]

A common law conversion claim relies heavily upon subjective analysis of the seriousness of the interference.[55] Shapiro will argue that changing the passwords on the accounts shows the extent and duration of the control that Bennett is trying to assert over the accounts.[56] Although Shapiro was not the only person with access to the Twitter account, the account was an extension of her voice and all actions or communications through the account were attributed to Shapiro, which establishes her as the sole owner of the account, bolstering the claim of conversion of her property by interfering with her right of control.[57]

U.S. Apparel will argue that control of the accounts were part of the position that Shapiro held at the company, and her right to use them terminated when she was removed from her position.[58] Shapiro may counter that the work that she put into the accounts is the property that is being converted and that she has had sole property right in the accounts and the information.[59] The inconvenience and harm done is the loss of access to the accounts and the inability to retrieve the contacts and personal information that she had stored within the accounts when she worked for U.S. Apparel. From U.S. Apparel's perspective, those contacts and any other information associated with the accounts is solely the company's property, as it was accumulated by Shapiro while acting within the scope of her employment. Shapiro's position will be that her use of the accounts went beyond employment-related purposes, and they are her property despite the attachment to her former position.[60] This argument is bolstered by the presence of Shapiro's personal contacts, which clearly were made not in furtherance of her official position with U.S. Apparel but because of her personal relationship with friends and family members.

---

54. Argento, supra note 45, at 274.

55. *Id*. at 273.

56. Shmueli v. Corcoran Group, 802 N.Y.S.2d 871 (Sup. Ct. 2005) (where the exclusion of access to client lists that plaintiff maintained on a computer was sufficient for a claim of conversion); PhoneDog v. Kravitz, No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011) (denying dismissal of conversion claim, where a former employee refused to relinquish control of a Twitter account and changed the name of the account).

57. Argento, *supra* note 45, at 273.

58. *Kravitz*, 2011 U.S. Dist. LEXIS 129229, 2011 WL 5415612.

59. *Shmueli*, 802 N.Y.S.2d 871.

60. Astroworks, Inc. v. Astroexhibit, Inc., 257 F. Supp. 2d 609 (S.D. N.Y. 2003).