UIC John Marshall Journal of Information Technology & Privacy Law

Volume 25
Issue 2 *Journal of Computer & Information Law - Spring 2008*

Article 5

Spring 2008

The Twenty-Sixth Annual John Marshall International Moot Court Competition in Information Technology and Privacy Law: Bench Memorandum, 25 J. Marshall J. Computer & Info. L. 305 (2008)

Leslie Ann Reis

David E. Sorkin
John Marshall Law School, dsorkin@uic.edu

Panagiota Kelali

Jessica Diehl

Carlos A. Encinas

See next page for additional authors

The Twenty-Sixth Annual John Marshall International Moot Court Competition in Information Technology and Privacy Law: Bench Memorandum, 25 J. Marshall J. Computer & Info. L. 305 (2008)

Authors

Leslie Ann Reis, David E. Sorkin, Panagiota Kelali, Jessica Diehl, Carlos A. Encinas, Matthew Hector, Gina Spada, Steven Tseng, and Priya Krishnamoorthy Venkat

THE TWENTY-SIXTH ANNUAL

JOHN MARSHALL

INTERNATIONAL MOOT COURT COMPETITION

IN INFORMATION TECHNOLOGY AND PRIVACY LAW

OCTOBER 18 - 20, 2007

BENCH MEMORANDUM

Leslie Ann Reis
David E. Sorkin
Panagiota Kelali
Jessica Diehl
Carlos A. Encinas
Matthew Hector
Gina Spada
Steven Tseng
Priya Krishnamoorthy Venkat

IN THE SUPREME COURT OF THE STATE OF MARSHALL

Ron Baylor, Petitioner	))	
v.	)	No. 2007-CV-0315
ConDevel, Inc., Respondent	))	

I. INTRODUCTION

Petitioner, Ron Baylor, is appealing to the Marshall Supreme Court from an order granting summary judgment in favor of Defendant-Appellee, ConDevel. Baylor's lawsuit is based upon the misuse of his personal information obtained by ConDevel's employee, Steve Nesbit. Baylor alleges that ConDevel is liable for intrusion upon seclusion and violation of the Marshall Data Protection Act, 17 Marshall Code Section105 *et seq.*

A. PROCEDURAL HISTORY

Baylor's original complaint, filed on July 30, 2005 in the Circuit Court of the State of Marshall, alleged intrusion upon seclusion and violation of the notification provision of the Marshall Data Protection Act. ConDevel moved for summary judgment on both counts. The circuit court granted the summary judgment motion to Defendant on both counts finding that the tort of intrusion upon seclusion was not a viable cause of action in the Fourth Circuit and there was no violation of the notification provision of the Marshall Data Protection Act.

Baylor appealed to the Fourth Circuit Court of Appeals, which affirmed the circuit court's order. The Court of Appeals affirmed the summary judgment as to the intrusion upon seclusion claim on the basis that the Fourth Circuit has never specifically stated that the tort is actionable. The Court of Appeals reasoned that even if it were to recognize the tort, Baylor's claim would still fail as a matter of law because he failed to prove one of the elements of the tort namely, that the intrusion caused him anguish and suffering.

The Court of Appeals also affirmed as to the breach of the Marshall Data Protection Act on the basis that the data was acquired in good faith therefore it fell under the exception of Section 105(d) and no liability could be established.

Baylor petitioned for leave to appeal to the Supreme Court of Marshall. The Supreme Court granted leave to appeal the summary judg-

ment order as to both counts. The parties now appear before the Supreme Court of Marshall to present their arguments.

B. STATEMENT OF FACTS

The parties have stipulated that the court of appeals decision shall serve as the record on appeal. The court of appeals decision[1] sets forth the facts of the case as follows:

Respondent, ConDevel, is in the business of real estate construction and development. For years, it has been the leader in this industry in the State of Marshall. In the last few years, it has lost some of its market share to foreign corporations. In an attempt to appease its shareholders, ConDevel has made some large budget cuts and laid-off several employees. ConDevel's technology support department was particularly hard-hit by the lay-offs. The financial troubles have not though affected the ConDevel's "VIP Program." This program has been in existence for many years and was originally implemented to attract and foster loyalty among top executives. The program provides certain privileges or "perks" to ConDevel's high-ranked executives. Such privileges include the option to obtain membership in exclusive clubs, VIP lounges, luxury suites, limousine services and the like. The number and types of privileges awarded are based upon an employee's corporate status (including rank, seniority, and salary).

Petitioner, Ron Baylor, is an executive vice president at ConDevel. He is responsible for the operations, sales and human resources departments. He has worked hard and climbed up the ranks at ConDevel from a Sales Associate position he started 25 years ago, to his current status as vice president. He is a valued employee and over the years, has helped grow the company's revenue several fold. By virtue of his current position, Baylor has access to all employees' electronic personnel files including his own. Such files contain employee contact information, social security numbers, drivers license numbers, employee performance evaluations, employee salary data, employee benefits information, employee awards and honors, and other personal data.

Steve Nesbit is a young sales associate at ConDevel. He graduated college just a couple of years ago. He is smart, very ambitious and quite tech savvy like most people of his generation. He enjoys many forms of high-tech entertainment including computer gaming, blogging, and social networking web sites. He feels that information should be free and is a big fan of so-called "security sites." Through these illicit sites that make public information about computer vulnerabilities and provide in-

1. R. 1-6. The remainder of the Statement of Facts presented here is set forth verbatim as it appears in the court of appeals decision; the footnotes have been renumbered.

structions for hackers, Nesbit has gained a basic understanding of various security exploits and has dabbled with some very basic hacks.

Steve Nesbit also wants to take a quick ladder to the top of his company and enjoy all the benefits and perks of the executives. He has frequently expressed to his colleagues his disappointment that he would have to wait for years before enjoying any of the benefits restricted to the high level employees. He had been heard to say jokingly: "I wonder if there is another way to enjoy the good life reserved to the executives".

As a result of ConDevel's corporate budget cuts, at the time this action was originally filed, no computer upgrades had been made in two years. Moreover, as a result of the corporate lay-offs, the technical support department was and remains short-staffed. There were few resources devoted to improving or maintaining corporate information security and little attention paid to enforcing corporate technology policies.

At the time this action was filed, ConDevel had a Computer Usage Policy that stated, *inter alia*, "employees are responsible for safeguarding all equipment and software provided by the company." However, employees were not given any guidance as to what constituted appropriate safeguard measures. There were no procedures in place for computer monitoring, accounting or enforcement of this policy.

Nesbit, being a savvy "power" user, was aware that corporate information security measures were lacking. On several occasions, he commented to his supervisor that ConDevel's technology infrastructure and minimal security mindset were naive and not worthy of a company the size and importance of ConDevel. In one email to his supervisor, Nesbit stated that "ConDevel was a data-breach waiting to happen." However, no action was taken on Nesbit's complaints. He was consistently told to mind his own business and leave technological issues to the technology support department.

Nesbit, frustrated by the company's refusal to upgrade equipment and security measures, devised a plan to raise upper management's awareness of the company's technology vulnerabilities. Using information about hacking and "spyware"[2] he obtained from a site on the Internet, he designed a keylogger program – a small software program that could be installed on someone else's computer (the target computer), where it would run unnoticed by an average user. The keylogger would record keystrokes made on the target computer and store them in a plain text file. Each day at midnight, the program would email the day's text file back to Nesbit. He could then read through the text file at his leisure,

2. Spyware is usually defined as a computer program that is surreptitiously installed on a user's computer without that user's consent. The spyware program is often used to intercept information or take control over computer functions.

and use it to discover user names, passwords, and any other information entered via the target computer's keyboard. Nesbit had set the program to send the email to a private email address he maintained. It was his belief that using an address outside of ConDevel's network would make him more difficult to catch.

Nesbit intended to use his keylogger software to attack and document vulnerabilities on ConDevel computers. He planned to make a full report of his activities to corporate management. At the time he designed the keylogger program, he had not determined when or on which company computer(s) he would install it. Nesbit kept the keylogger program on a small USB "thumb drive"[3] that he carried with him at all times.

The opportunity for Nesbit to implement his plan presented itself on or about April 25, 2005. On his way back from the restroom, Nesbit passed by Petitioner Baylor's office. Baylor was engaged in a telephone conversation. Within earshot of Nesbit, Baylor announced that he would be leaving for a meeting "right now." Nesbit watched as Baylor left his office in quite a hurry. Nesbit realized that no other employees were in the area of Baylor's office, so he stepped into Baylor's office to look around. Nesbit noticed that Baylor had left his computer on and even though Nesbit had not originally planned to install his key logger software on Baylor's computer, he seized the occasion to install the keylogger program on Baylor's computer.

The next day, Nesbit started receiving emails from the keylogger program at his private email address. The emails contained records of every keystroke Baylor had entered through his keyboard onto his computer on a particular day. The keystroke information enabled Nesbit to ascertain Baylor's login and passwords used to access many company files including the human resources database that contained the electronic employee personnel files.

For the purpose of exposing ConDevel's computer vulnerabilities to company management, Nesbit used Baylor's login information to access the human resources database. He intended to poke around the files and submit a report of his findings to management. He hoped the report would not only raise management's awareness of the inadequate security, but also enhance his reputation as a team player and problem solver.

Once Nesbit accessed the human resource database, however, he discovered that he had access to the personally identifiable information of every employee, including Baylor. Nesbit also had access to the benefit system and "VIP Program" files used for setting up memberships at vari-

3. Also known as USB drives or flash drives are data memory storage devices that plug into personal computers through a universal serial bus (USB) interface. These drives are typically small, lightweight, and rewritable.

ous exclusive clubs. He immediately became fascinated by the opportunities that the executives at ConDevel were given and had a change of heart. He decided to forego informing management about the inadequate security in favor of using the employee files and VIP Program information for his own benefit.

Nesbit downloaded all of the human resource database files to his home computer. Examining Baylor's file, Nesbit noticed that Baylor had not joined many of the exclusive clubs available to him via his executive package. Nesbit accessed the benefit system and had several credentials issued to Baylor, but sent to Nesbit's home address. The credentials included a membership card to the Marshall League Club, the most exclusive private social club in the state. Nesbit started frequenting the Marshall League Club and several other establishments, gaining entry by using the credentials issued in Baylor's name. On May 25, 2005, at the Marshall League Club, Nesbit became seriously intoxicated and got into a fight with a prominent member of the club. The Club's security had to physically remove him from the premises and informed him that his membership was suspended.

After this incident, Nesbit decided to keep a low profile and refrained from using the membership card that had been issued in Baylor's name. Unbeknownst to Nesbit, many exclusive restaurants, social clubs and other establishments in the State of Marshall share a common "blacklist." When the Marshall League Club informed the other establishments that it had barred Baylor, other clubs revoked his membership, effectively blacklisting Baylor.

Petitioner Baylor did not begin to suspect that his personal information had been misused until he tried to take some friends to play golf at Shady Links, a local private course, on June 1, 2005. Baylor was informed that his membership had been revoked due to his behavior at the Marshall League Club. Baylor was deeply embarrassed and angry that he had never been informed of such a development. He wondered how he could have been barred from the Club when he was not a member and had not been there in years.

The following week, Baylor attempted to take his family to Les Deux Pommes, an upscale restaurant. He was told that he was not welcome in the restaurant and informed that his inappropriate conduct at the Marshall League Club was the reason. Baylor demanded to see the manager. The conversation became a heated argument and the restaurant manager shouted, "We do not want drunks and trouble makers in our restaurant!"

Following this second embarrassing incident, Baylor concluded that someone must be posing as him and using his VIP benefits. He knew that the only way to use the benefits was to have membership cards is-

sued. He also knew that the only method for obtaining the cards was via ConDevel's human resources system. So, Baylor initiated his own investigation. He reviewed the human resources database and realized that several membership cards had recently been issued in Baylor's name and was shocked to see that these cards were allegedly authorized and issued by Baylor himself.

Baylor concluded it was possible that some sort of a corporate security breach had occurred. He informed the appropriate managers and enlisted the help of one of the few technology experts at ConDevel, the director of the technology support department, who performed an analysis of Baylor's computer. A full scan of Baylor's hard drive revealed the keylogger software that had been surreptitiously installed by Nesbit. Further analysis of the program uncovered the external email address that Nesbit was using to receive files from the keylogger. This email address was eventually traced to Nesbit. When confronted by corporate management, Nesbit explained that the presence of the keylogger program was part of his plan to help the company by exposing ConDevel's computer vulnerabilities.

Nesbit was fired when ConDevel's management became aware of his actions. Management concluded that even though Nesbit had access to all employee personnel files and other data, no one outside the company accessed the files, thus no "true" data breach had occurred. Even so, ConDevel's management was concerned that news of this incident could harm ConDevel's reputation. The company's chief operating officer, in a voice mail message to the director of the technology support department stated: "As far as we know, no one knows that this ever happened. Let's keep it that way. The last thing we need right now is a lawsuit or a scandal. We cannot afford losing our good name and our clients."

Following the discovery of Nesbit's actions, the technology support department tightened security. ConDevel's management did not inform any one about the incident. It did not offer any investigation details to Baylor. Nor did it offer to assist Baylor in rebuilding his good name.

II. ISSUES PRESENTED FOR REVIEW

There are two issues raised on this appeal before the Supreme Court of Marshall: (1) whether the Court of Appeals erred in holding that the surreptitious installation of a so-called "keylogger" on Appellant's computer did not state a claim for a recognized cause of action for invasion of privacy under the theory of intrusion upon seclusion, and (2) whether the Court of Appeals erred in holding that Appellee, ConDevel was exempt from the notification provision of the Marshall Data Protection Act, 17 Marshall Code Section105 (2006).

III. ANALYSIS

A. STANDARD OF REVIEW

Summary judgment is a procedural device that enables a court to dispose of part or all of a case prior to trial. In the State of Marshall, summary judgment is governed by Rule 56 of the Marshall Rules of Civil Procedure. Under this rule, summary judgment is proper only if there is no genuine issue as to any material fact and the moving party is entitled to a judgment as a matter of law.[4] The court considers the pleadings, depositions, answers to interrogatories, admissions, and affidavits in assessing whether summary judgment is proper.[5] A genuine issue of material fact exists only if "a fair-minded jury could return a verdict for the [non-moving party] on the evidence presented."[6]

An appellate court reviews a grant of summary judgment *de novo,* applying the same standard as the trial court.[7] The reviewing court determines whether a genuine issue of material fact exists by viewing the evidence in the light most favorable to the non-moving party and drawing all reasonable and justifiable inferences in favor of that party.[8] The moving party has the burden of identifying the material facts which are without genuine dispute and support the entry of summary judgment in favor of the moving party.[9] The non-moving party, for its part, must identify which material facts raise genuine issues of dispute.[10] Because the entry of summary judgment "is a drastic means of disposing of litigation,"[11] it should be granted only when the moving party's right to relief is "clear and free from doubt."[12] However, the mere fact that there exists "some alleged factual dispute between the parties"[13] or "some metaphysical doubt as to the material facts"[14] is insufficient to defeat a motion for summary judgment.

B. AGENCY AS A THRESHOLD ISSUE

ConDevel is a party in this case under the parameters of agency law. Agency law requires that an employee acts solely for the benefit of the

4. Marshall R. Civ. P. 56(c) (cited at R. 1). Rule 56(c) is similar or identical to the corresponding provision of the federal rules, Fed. R. Civ. P. 56(c).
5. Fed. R. Civ. P. 56(c).
6. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 252 (1986).
7. Delta Sav. Bank v. U.S., 265 F.3d 1017, 1021 (9th Cir. 2001).
8. Anderson v. Liberty Lobby, Inc., 477 U.S. at 255.
9. Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986).
10. *Id.* at 324.
11. Purtill v. Hess, 489 N.E.2d 867, 871 (Ill. 1986).
12. *Id.*
13. Anderson v. Liberty Lobby, Inc., 477 U.S. at 247 (emphasis omitted).
14. Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 586 (1986).

employer in all matters connected with employment.[15] However, to establish a principal-agent relationship, where an employer may be held liable for the actions of an employee, it is not a requirement that the principal actually control the agent.[16] All that is required is that the principal have the ability or right to control the agent, whether the principal actually exercises that control.[17] Therefore, even though ConDevel did not assert actual control over Nesbit's activities, it will likely be argued that the principal-agent relationship can be established because ConDevel could have asserted control over Nesbit.

Furthermore, the law is well settled that an agent owes a duty to the principal of good faith and loyalty.[18] The agent is prohibited from using his or her position for one's own benefit at the principal's expense.[19]Additionally, the employee's performance of duties in good faith bars that employee from pursuing interests contrary to interests of the employer.

C. INTRUSION UPON SECLUSION

i. General

Baylor's first claim alleges that ConDevel committed an invasion of privacy in the form of intrusion upon seclusion. This tort is recognized by some, but not all jurisdictions. To be successful in an intrusion claim, a plaintiff must show four elements: (1) there was an unauthorized intrusion or prying into his seclusion; (2) the intrusion was offensive to or objectionable to a reasonable person; (3) the matter intruded upon was private; and (4) the intrusion causes anguish and suffering.[20] In the instant matter, the Court of Appeals granted summary judgment to ConDevel, holding in part that the 4th Circuit does not recognize the tort. However, other courts in the State of Marshall do recognize an invasion of privacy stemming from an intrusion upon seclusion to be a viable cause of action. Therefore, the first obstacle Baylor must overcome is the current circuit split among the courts in the State of Marshall.

ii. Circuit Split

The State of Marshall courts are still split on whether or not to recognize the tort of intrusion upon seclusion. Specifically, in the state of Marshall, the first and second circuits have already recognized the tort and adopted the language of the Restatement, while the third circuit has

15. Restatement (Second) of Agency § 387 (1958).
16. Schutz v. Arrow Fin. Servs., *LLC*, 465 F.Supp.2d 872, 877 (N.D. IL 2006).
17. *Id.*
18. Manufacturers Cas. Ins. Co. v. Martin-Lebreton, 242 F.2d 951, 953 (5th Cir. 1957).
19. Eagle Indem. Co. v. Cherry, 182 F.2d 298, 299 (5th Cir. 1950).
20. Melvin v. Burling, 49 N.E. 2d 1011, 1012 (Ill. App. Ct. 1986).

not had the opportunity to reconsider the issue, but concluded in a very old decision that the tort was not recognized.[21] The fourth circuit has never explicitly recognized the tort.[22]

The circuit split in the instant case is similar to the long-held, but recently resolved, split of the Illinois appellate districts, which came about after the Illinois Supreme Court's decision in *Lovgren v. Citizens First National Bank.*[23] In *Lovgren*, the court stated it did not implicitly recognize intrusion upon seclusion, despite laying out the elements and finding the plaintiff was unable to meet the elements of the tort.[24] The ambiguity of the *Lovgren* holding created confusion among the appellate districts because Illinois had already recognized three of the four branches of privacy torts embraced by the *Restatement of Torts* which adopted the theory developed by Professor William Prosser.[25] The third and fifth appellate districts took it upon themselves to recognize the tort despite the dicta in *Lovgren.*[26] Illinois appellate courts have addressed the issue in several different cases where the plaintiff would have succeeded in proving the elements, in district court, were it not for the confusion presented by the *Lovgren* decision.[27] Until very recently, in Illinois, the fourth district had not recognized the tort.[28] Today, all appellate districts in Illinois recognize the tort of intrusion upon seclusion.[29]

Baylor may argue that intrusion upon seclusion should be recognized because half of the Marshall circuits have already concluded the cause of action exists, and that he is able to meet the *prima facie* ele-

---

21. *See* R. at 6.

22. *Id.*

23. Lovgren v. Citizens First Nat'l Bank, 126 Ill.2d 411 (1989).

24. *Id.*

25. 1-6 Illinois Tort Law § 6.01(1) (citing the RESTATEMENT (SECOND) OF TORTS and describing the four-branch tort theory of invasion of privacy as including " (1) intrusion upon the seclusion of another RESTATEMENT (SECOND) OF TORTS § 652B, at 378 (1977); (2) appropriation of name or likeness of another RESTATEMENT (SECOND) OF TORTS § 652C, at 380 (1977); (3) publicity given to private life RESTATEMENT (SECOND) OF TORTS § 652D, at 383 (1977); and (4) publicity placing person in false light RESTATEMENT (SECOND) OF TORTS § 652E, at 394.n3").

26. 1-6 Illinois Tort Law § 6.01(1).

27. Johnson v. Kmart, 311 Ill.App. 3d 573, 578-579 (2000) (finding "a material issue of fact exists regarding whether a reasonable person would have found defendant's actions to be an offensive or objectionable intrusion. Thus, summary judgment should not have been granted." Also stating, "[w]e now expressly recognize a cause of action for the tort of invasion of privacy by intrusion upon seclusion in this state.")

28. Hall v. InPhoto Surveillance Co., 271 Ill.App. 3d 852, 855 (1995) (finding "the supreme court has specifically declined to settle the issue of whether the intrusion upon seclusion tort is actionable in Illinois."); *see also Burns v. Masterbrand Cabinets*, Inc., 369 Ill.App. 3d 1006, 1011 (2007).

29. *Burns*, 369 Ill. App. 3d at 1011.

ments. As in *Johnson v. Kmart*, Baylor should argue that the fact he is able to meet the elements of intrusion upon seclusion provides the fourth circuit the opportunity needed to formally recognize the tort.[30] Baylor could follow the reasoning of the Illinois decisions and point out that conflicts among districts within the state can only be remedied by the appellate court within that circuit. He may argue that now is the time for the Marshall fourth circuit to recognize the tort and rule in his favor because he is able to meet the elements of the cause of action.[31] As the plaintiffs in *Acuff v. IBP, Inc.* argued, Baylor may proffer the rhetorical question "[H]ad the [*Lovgren* court] not intended to adopt such a tort in the future, why would it take time to spell out the elements for such a tort and give examples?"[32]

ConDevel will likely respond to this argument by pointing out that in order to determine whether a cause of action will be recognized, courts must first establish the elements of the action itself and the Marshall courts have not done so.[33] ConDevel may further argue, as the court pointed out in *Acuff* that by asking the fourth district to read between the lines of the decisions of other courts is to ignore the warnings present in the circuit split itself.[34] By refusing to resolve the question of whether or not the tort of intrusion upon seclusion exists, the courts of Marshall have not yet decided the cause of action is worthy of remedy under the law.

Baylor could also cite to language in *Schmidt v. Ameritech* in which the first district of Illinois concluded it would recognize the tort, stating "in *Mucklow v. John Marshall Law School*, this district found that the plaintiff's allegations did not satisfy the first element of [the tort], but failed to express a view as to the conflict regarding the recognition of the

30. *Johnson*, 311 Ill.App. 3d at 981-982.

31. Burns v. Masterbrand Cabinets, Inc., 369 Ill.App. 3d 1006, 1011 (2007).

32. *Acuff v. IBP, Inc.*, 77 F. Supp.2d 914, 920 (C.D. Ill. 1999); *see also* Amati v. The City of Woodstock, 829 F. Supp. 998, 1010 (N.D. Ill. 1993) (stating "the court believes that there are several reasons why the Illinois courts would not so limit the cause of action. First, the Illinois Supreme Court has already cited with approval the RESTATEMENT (SECOND) OF TORTS § 652B (1977) and comments thereto in discussing the elements necessary to prove the tort of intrusion into seclusion. Second, several cases from other jurisdictions also support such a conclusion.")

33. *Id.* (stating "[P]erhaps the answer to this question is that the Illinois Supreme Court could not determine whether the factual scenario presented on appeal supported the elements of the tort of intrusion upon seclusion unless it first explained what the tort is and what elements must be established.")

34. *Id.* (stating "[F]urthermore, to ask this Court to read between the lines of the *Lovgren* decision for some signal that the supreme court plans to adopt the cause of action in the future is contrary to the court's admonishment: "We *emphasize* that our discussion of the tort of unreasonable intrusion into the seclusion of another, as enunciated by the Restatement and by Prosser, *does not imply a recognition* by this court of such a cause of action.")

intrusion-upon-seclusion cause of action, *i.e.,* it never said that the cause of action did not exist."[35] In using this language, Baylor could argue that intrusion upon seclusion is already recognized in the state of Marshall, but that until now, no plaintiff has clearly met the elements of the tort in the fourth circuit. Baylor should also point out that the circuits recognizing the tort have not been overruled by the Supreme Court, therefore signifying perhaps an implicit recognition of the tort.

ConDevel may counter that even if the tort of intrusion upon seclusion is recognized, Baylor is unable to meet the elements of the tort. However, ConDevel will likely point out that the Supreme Court has yet to recognize the cause of action despite previous decisions by appellate courts that do recognize the tort. ConDevel could also assert that although Marshall recognizes the right to privacy, "courts should proceed with caution in defining the limits of the right to privacy"[36] and argue that privacy rights should not be extended beyond those clearly enumerated by the Supreme Court.

iii. Elements of the Tort of Intrusion Upon Seclusion.

On appeal, the court granted summary judgment for ConDevel, holding in part that, should the court even decide to recognize the tort, appellant Baylor would be unable to satisfy one or more of the four elements of intrusion upon seclusion. To have succeeded on this claim, the court held, Baylor needed to prove that: (1) there was an unauthorized intrusion or prying into his seclusion; (2) the intrusion was offensive to or objectionable to a reasonable person; (3) the matter intruded upon was private; and (4) the intrusion causes anguish and suffering.[37] Although the Appellate Court specifically stated that Ron Baylor failed to prove the fourth element of the tort,[38] and the parties should focus their argument on that last element, a brief presentation of all elements is deemed appropriate for purposes of completeness of this memorandum.

1. *Unauthorized Intrusion or Prying*

To prove the tort of intrusion upon seclusion, the plaintiff must first prove there has been an unauthorized intrusion or prying into the plain-

35. 329 Ill.App.3d 1020, 1028 (2002) ("We agree with *Johnson* that this district's prior application of the four elements of the tort-without ever specifically asserting that a cause of action for intrusion upon seclusion exists-constitutes at least a peripheral prior judicial acceptance of the tort. In other words, we think that *Johnson* did not establish, or claim to establish, a new principle of law and was not a case of first impression. .") *Id.* at 1029.

36. Kelly v. Franco, 72 Ill.App. 3d 642, 646 (1979) (finding the tort of intrusion upon seclusion not to exist in the state of Illinois).

37. *Melvin v. Burling*, 49 N.E. 2d 1011, 1012 (Ill. App. Ct. 1986).

38. *See* R. at 7.

tiff's seclusion.[39] According to the Second Restatement, the invasion itself may be a physical intrusion, such as, physically entering a room, or the intrusion may occur by use of the defendant's senses.[40] For example, "eavesdropping via wiretapping has been conspicuously singled out on several occasions as precisely the kind of conduct that gives rise to an intrusion-on-seclusion claim."[41] Baylor should argue that the surreptitious installation of the keylogger program on his computer constitutes an unauthorized intrusion upon his seclusion because the information obtained through use of the keylogger program was password protected and obtained by Nesbitt's unauthorized prying into Baylor's computer.

On the other hand, ConDevel could argue that the information obtained from Baylor's computer is not private as to ConDevel because Nesbit obtained information from a company file and on a company computer. Therefore, information regarding Baylor's employee benefits was in ConDevel's possession before Nesbit even installed the keylogger system. Consequently, ConDevel could argue that Baylor could not have a reasonable expectation of privacy or seclusion in the company files or work computer.[42]

2. *Offensive to Reasonable Person*

The second element of the tort requires the plaintiff show the intrusion was offensive to or objectionable to a reasonable person.[43]The Second Restatement requires any intrusion be "highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object."[44] This element of the tort goes to "how" the infor-

39. *Melvin v. Burling*, 49 N.E. 2d 1011, 1012 (Ill. App. Ct. 1986).

40. § 652B Comment b: 'The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined."

41. Narducci v. Vill. of Bellwood, 444 F. Supp. 2d 924, 938 (N.D. Ill. 2006), *citing* Lovgren v. Citizen's Fist Nat'l Bank, 126 Ill.2d at 417, 534 N.E.2d at 989; Thomas v. Pearl, 998 F. 2d 447, 452 (7th Cir. 1993); RESTATEMENT (SECOND) OF TORTS § 652B cmt. b).

42. *See* § 2 *infra*.

43. *Melvin v. Burling*, 49 N.E.2d at 1012.

44. Second Restatement § 652B Comment d: "There is likewise 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 man would strongly object."

mation was obtained as well as what information was obtained.[45]

Baylor could argue the installation of the keylogger program on his computer is offensive to a reasonable person because the information obtained was private and could not be obtained without using this highly intrusive measure of hacker-like computer technology, or unless Baylor himself gave out his password. Thus, the deceptive and intrusive actions of Nesbit, made possible by the lack of security and safeguards at ConDevel, were improper and highly offensive to a reasonable person.

Conversely, ConDevel could argue that an employee does not have a reasonable expectation of privacy in his work computer, and therefore, the intrusion cannot reach the standard of "highly offensive to the reasonable person."[46] In *Thygeson*, a former employee sued his former employer for intrusion upon seclusion when the employer company terminated him for excessive internet usage and because sexually inappropriate e-mails were found in his personal folder on the company's network. A question raised in *Thygeson* was "whether [the company's review of its employee's e-mail and internet usage] was an intrusion on the former employee's solitude in a manner that would be highly offensive to a reasonable person." *Id.* After reviewing precedent from several jurisdictions, the court found there was no precedent to support the former employee's assertion of a reasonable expectation of privacy when using his work computer and the company's internet.[47] Similarly, here, ConDevel, like the company in *Thygeson*, should assert that Baylor can have no reasonable expectation of privacy in his work computer, and especially has no reasonable expectation of privacy in his work files.

3. *Private Matter*

The third requirement for intrusion upon seclusion is that the matter intruded upon must be private. This third element is "the predicate for the other three," because "[w]ithout private facts, the other three elements of the tort need not be reached."[48]

Here, Baylor should argue that Nesbit intruded upon a private matter because he improperly entered Baylor's office, pried into Baylor's computer, and thereby stole confidential passwords and employment information about Baylor. These files include employment data not otherwise accessible by Nesbit or other employees at Nesbit's level. For instance, in *Acosta v. Scott Labor, LLC*, the court noted that "Factors affecting an employee's expectation of privacy in a given area of the office include: 'whether the area was given over to an employee's exclusive

45. Tobin v. Mich. Civil Service Comm., 331 N.W.2d 184 (Mich. 1982).

46. Thygeson v. U.S. Bancorp, 2004 U.S. Dist. LEXIS 18863, *61 (D.C. Or. 2004)

47. *Id.* at 74.

48. Busse v. Motorola, Inc., 351 Ill. App. 3d 67, 72 (Ill. App. Ct. 2004).

use, . . .[and] the extent to which others had access to the work space. . . ."[49]

Baylor should concede that "matters of public record" are not private. For instance, in *Busse*, the First District of Illinois stated that, "Matters of public record—name, address, date of birth and fact of marriage—have been held not to be private facts."[50] However, even if matters of public record are not found to be private facts, Baylor should argue that his confidential employment file contained more than merely matters of public record and that the other employment and benefits information in the file constitute his private employee information. Notably, the confidential employment files that Nesbit obtained by way of his intrusion contained "employee performance evaluations, employee salary data, employee benefits information, employee awards. . .and other personal data."[51]

ConDevel, on the other hand, can reiterate many of its arguments under the first element—unauthorized intrusion or prying. Specifically, ConDevel should argue that information obtained through the intrusion was not private as to ConDevel. Some jurisdictions have found that the use of password protection and personal folders on a company's intranet system did not create a reasonable expectation of privacy.[52] Therefore, even if Baylor may have created and used his own passwords, that does not cloak his work computer or the company's files with the requisite privacy for this element.

4. *Anguish and Suffering*

The fourth and crucial for Appellant, Ron Baylor, requirement for intrusion upon seclusion is that the intrusion must cause anguish and suffering. In *Thomas v. Pearl*, the Seventh Circuit stated that: "The tort of intruding upon the seclusion of another is aimed at discomfort caused by *the intrusion itself*—for example, [the discomfort caused if] someone enters your bedroom, opens your mail, or makes repeated and unwanted telephone calls to you."[53] The appellate court's order states that Baylor has failed to establish the "anguish and suffering" element. As such, both parties should focus on this element.

In *Schmidt v. Ameritech Illinois*, the court stated that a plaintiff could prove anguish and suffering by establishing actual injury "in the form of, for example, medical care, an inability to sleep or work, or a loss

49. 377 F. Supp. 2d 647, 651 (N.D. Ill. 2005) (internal citations omitted).

50. 351 Ill. App. 3d at 72.

51. R. at 2.

52. Garrity v. John Hancock Mut. Life Ins. Co., 2002 U.S. Dist. LEXIS 8343, 2002 WL 974676, *2 (D. Mass. 2002); McLaren v. Microsoft Corp, 199 Tex. App. LEXIS 4103, 1999 WL 339015 at *4 (Tex. Ct. App. 1999).

53. 998 F.2d 447, 452 (7th Cir. 1993) (emphasis added) (internal citations omitted).

of reputation and integrity in the community."[54] Accordingly, the *Schmidt* court found there was sufficient evidence to support the requisite anguish and suffering for one of the co-plaintiffs in that case—a business owner whose telephone records were reviewed by Ameritech officials as part of Ameritech's investigation into another co-plaintiff's whereabouts during his disability leave. The court noted that the evidence demonstrated "[the business owner] was infuriated and emotionally upset because Ameritech had broken the trust she placed in the company."[55] Ultimately, the court found there was sufficient evidence to support a finding of anguish and suffering from the intrusion itself. The court made this finding despite the fact that this co-plaintiff never sought medical or psychological assistance for her anguish or suffering.[56]

Here, Baylor could assert that when he discovered the unauthorized intrusion into his computer he became infuriated and now experiences anguish and suffering when using computers at work or at home. Consequently, Baylor could argue that there is at least a question as to whether he has experienced enough anguish and suffering as to prove actual injury, for example, "an inability to sleep or work."[57]

Additionally, Baylor could argue that the intrusion caused him anguish and suffering because he is experiencing "a loss of reputation and integrity in the community" as a result of the intrusion.[58] For instance, Baylor could assert that the intrusion has already had the effect of putting him on a statewide "blacklist" for the State's most elite private social clubs, in which he otherwise could have enjoyed VIP membership status if he chose to do so. He could assert that as a result of the intrusion he unjustly obtained the reputation of being a "drunk and troublemaker"[59] marring his image of a hardworking family man which he earned through the years. In sum, this placement on the Marshall blacklist, and Nesbit's actions leading to Baylor's placement on the blacklist beginning with the intrusion on Baylor's computer, has damaged Baylor's "reputation and integrity in the community."

If challenged and forced to concede that only anguish and suffering as a result of the intrusion itself should be considered for this tort,[60] Baylor could attempt to overcome this counter-argument by asserting that the intrusion on his computer was the proximate cause for the theft of his personal information and employee benefits, placement on the Marshall blacklist, and loss of "reputation and integrity in the commu-

54. 329 Ill. App. 3d 1020, 1035 (1st Dist. 2002).
55. *Id.*
56. *Id.*
57. *See Id.*
58. *See Id.*
59. *See* R. at 5.
60. *See Thomas*, 998 F.2d at 452.

nity," all of which, caused him anguish and suffering. In *Schmidt*, the court did not find anguish and suffering as to two of the three co-plaintiffs because the record did not reflect their suffering was proximately caused by the intrusion itself.[61] Instead, the *Schmidt* court found that the loss of co-plaintiff's job, rather than the allegedly unauthorized intrusion into phone records, caused his suffering, and that he would have lost his job even if Ameritech had not reviewed the relevant phone records. Baylor can argue that, unlike in *Schmidt*, here the evidence shows that the intrusion into his computer did proximately cause his anguish and suffering because it resulted in the misuse his personal information and subsequent injuries. The misuse of Baylor's personal data and his placement on Marshall's blacklist would not have occurred if not for the intrusion on his computer. This "but for" relationship was not present in *Schmidt*, and thus, is distinguishable from the case at bar.

On the other hand, ConDevel can argue that the intrusion itself caused Baylor no anguish or suffering: "Baylor did not begin to suspect that his personal information had been misused until he tried to take some friends to play golf at Shady Links, a local private course, on June 1, 2005."[62] This was more than a month after the April 25 intrusion into Baylor's work computer.[63] Consequently, ConDevel could argue that Baylor's anguish and suffering, if any, as a result of Nesbit's subsequent use of information obtained from the intrusion, is not relevant to this cause of action because it is separate from the intrusion itself. ConDevel could analogize this case to *Thomas*, where a college basketball coach surreptitiously recorded conversations with a potential recruit, and then played the recordings to several people in order to establish that another college basketball coach was making improper offers to recruit Thomas. The court found that "Thomas was harmed if at all not by the telephone calls themselves (since he was a willing party) or even by the recording, but by the publication of what he said in the conversations."[64] Here, ConDevel can argue that the court must separate the intrusion from the subsequent use of information, just as *Thomas* separated the intrusion of surreptitiously recording one's telephone conversations and the subsequent use of the recording by "publication."

ConDevel could also argue that Baylor's anguish and suffering arose from his own actions, including leaving his office space and computer open and unprotected. Moreover, ConDevel could reiterate its prior arguments that Baylor has no reasonable expectation in his work computer and work files, and thus any anguish and suffering actually resulting

61. 329 Ill. App. 3d at 1036.

62. R. at 4.

63. R. at 3.

64. 998 F.2d at 452.

from the "discomfort caused by the intrusion itself" is not an actual injury because he has no privacy right in his work computer. If he has no privacy in his work computer and files, then any discomfort caused by his later discovery of the intrusion cannot constitute an actual injury.

D. BREACH OF THE MARSHALL DATA PROTECTION ACT (17 MARSHALL CODE SECTION 105 (2006))

1. *General: Scope of the Data Protection Act*

The Marshall Data Protection Act represents one of the many newly enacted state statutes that deal with the loss of personal information by data collectors. Similarly to other state data breach notification statutes,[65] the Marshall Data Protection Act is an attempt to balance several competing interests including the interest of an individual in being aware of who possesses information about that him or her; the business interest in efficiency and modern necessity of information exchange (including the widespread use of data bases and data mining technologies); the public interest in protecting the consumers and enhancing the security of personal information; and shielding compliant companies from liability.

California was the first state to enact a breach notification statute in 2003.[66] Other states' statutes, including Marshall's, to a large degree, resemble the California statute's language and provisions. California's Office of Privacy Protection has published recommendations to help businesses ascertain a better understanding of the law and assist them "in managing personal information in ways that promote and protect individual privacy interests.[67] These "best practices" recommendations can serve as guidelines for organizations and "are intended to assist organizations in supplementing their information security programs".[68] They do not constitute regulations or binding authority[69] but they are persuasive authority and will likely be used by both parties in their arguments.

The Marshall Data Protection Act creates an affirmative duty for organizations that collect data on individuals to notify that individual (the data subject) in the event of a data breach or unauthorized disclosure of data. The Marshall Data Protection Act provides a private cause of action for individuals when there has been an unauthorized disclosure of the individual's personal data and the collecting organization failed to

65. *See,* e.g., Illinois (815 ILCS 530/10),California Civil Code Section 1798.29

66. *See* California Civil Code § 1798.29

67. *See* CA DEP'T OF CONSUMER AFFAIRS, OFFICE OF PRIVACY PROTECTION, *Recommended Practices on Notice of Security Breach Involving Personal Information (2007),* http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf.

68. *See Id.* p.8.

69. *Id.*

notify or unreasonably delayed notification about the unauthorized disclosure.[70] An unauthorized disclosure resulting from a breach of security may be due to unauthorized individuals or employees utilizing any personal data in a manner not consistent with the purposes designated by the organization.[71] The Marshall Data Protection Act also creates an affirmative duty to report unauthorized disclosures that occur from external as well as internal sources.[72]

In order to prevail on a claim under the Marshall Data Protection Act, a plaintiff must demonstrate that: (1) an agency collected the personal data of individuals; (2) the personal data was acquired by unauthorized persons; (3) the unauthorized access was discovered by the agency; and (4) the agency failed to notify, or unreasonably delayed notification to the data subject individuals that their personal information had been obtained by unauthorized persons.[73]

Neither "personal data" nor "acquisition" is defined in Marshall's statute. However, since the definition of "personal information" is substantially similar in all the data breach notification statutes, it is likely

---

70. Marshall Data Protection Act, 17 Marshall Code § 105(g) (cited at R. 9) "Any and all data subjects within the State of Marshall shall have a civil action against any data collector that obfuscates evidence of a breach or makes an informed choice to not inform data subjects of a breach. Remedies available shall include:
1) Monetary damages not to exceed $100,000 per plaintiff. In the case of a class action, monetary damages are not to exceed $20,000,000.
2) Injunctive relief, as appropriate, to prevent further dissemination of the effected data.
3) Punitive damages not to exceed $30,000,000 for a deliberate and malicious violation of this subsection."

71. 17 Marshall Code § 105(d).

72. 17 Marshall Code § 105. The applicable sections of the statute state:
(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Marshall whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
. . .
(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency is not a breach of the security of the system, provided that the personal information is used for the purposes designated by the agency and/or is not subject to further unauthorized disclosure.

73. 17 Marshall Code § 105.

that the parties will rely on a definition of "personal data" or "personal information" that includes, but is not limited to, an individual's first name or first initial and last name in combination with a social security number, a driver's license number, or financial information with any required security code.[74] Additionally, California's Office of Privacy Protection's recommendations provide guidance to determine when acquisition of personal data has occurred, including when there is indication that the information has been downloaded or copied.[75]

2. *Determining "Good Faith" under 17 Marshall Code Section 105(d)*

A collecting agency does not have an affirmative duty to notify individuals about a breach of the security of a computer system where no unauthorized acquisition of the personal information took place. Specifically, the "good faith" acquisition of the data by employees or agents is not a "breach" provided that the personal information is being utilized in a manner that is authorized by the data collector. Under the Marshall Data Protection Act, authorized acquisition of data by an employee is based upon whether the employee had acquired the information in "good faith" while in the performance of one's duties within the purposes "designated by the agency" and/or that no further disclosure occurs.[76]

The Marshall Data Protection Act does not contain a definition of the term "good faith." Therefore, the parties will likely look to other jurisdictions for guidance. Some states have included language to clarify that good faith exception by specifying that the information obtained "is not used for a purpose unrelated to the business"[77] or "not used for an unlawful purpose."[78] Additionally, based on the legislative history of the California Notification Statute it may be argued that the purpose of such

74. 815 ILCS 530/10, California Civil Code Section 1798.29, OHIO REV. CODE ANN. § 1349.19(A)(7).

75. *See* CA DEP'T OF CONSUMER AFFAIRS, OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION (2007), http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf .
In page 11 the recommendations state:
"Acquisition
In determining whether unencrypted notice-triggering information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:
1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been downloaded or copied.
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported."

76. 17 Marshall Code § 105(d).

77. Fla. Stat. § 817.5681(4).

78. OHIO REV. CODE ANN. § 1349.19(A)(b)(i).

an addition was to exempt those who were acquiring personal information for a legitimate purpose, although in circumstances that the legislature had perhaps not contemplated.[79]

Due to the novelty of the creation of an affirmative duty upon a data collector, the liability springing from such a duty is an issue of first impression before the courts. Since there is no case law on this type of notification statute at present, the parties will need to explore other statutes from which they can draw applicable analogies. The Digital Millennium Copyright Act ("DMCA") and the Computer Fraud and Abuse Act ("CFAA") may provide appropriate analogies because they both specifically address the issue of unauthorized access to a computer system or network and provide a good faith exception.

The DMCA seeks to balance the interests of copyright holders and Internet users.[80] This balance is created through a notification scheme requiring the removal of potentially infringing material from an Internet site when the copyright holder provides notification including a statement of good faith belief stating the posted material is infringing.[81] Similarly, the CFAA employs criminal penalties to deter unauthorized access to protected computers[82] but also provides additional private cause of action[83] seeking to protect individuals from damages or loss as a result of a violation of its provisions and ultimately enhance "control by

79. Such an exception was not included in the original version of California's notification statute but was only added later *See* Official California Legislative Information, http://leginfo.public.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020823_amended_asm.html (last visited Sept. 23, 2007).

80. Rossi v. Motion Picture Ass'n of America, Inc., 391 F.3d 1000, 1004 (9th Cir. 2004).

81. 17 U.S.C. § 512(c)(3). The DMCA requires the notification contain specific elements so that Internet providers may rely upon such notifications without the need to perform their own investigations to ascertain the validity of a copyright holder's claim.

(A) To be effective under this subject, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

82. Computer Fraud and Abuse Act,18 U.S.C. § 1030(a)(4).

83. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g).

information providers."[84] Both acts have a requisite "good faith" element to which courts will look to in determining liability.[85]

It is quite possible that the parties will attempt to analogize the provisions of the DMCA and the CFAA with those similar and relevant provisions of the Marshall Data Protection Act.

3. *Acquisition in "Good Faith"*

"Good Faith" is a term the meaning of which may vary depending on the context the term is used. However, a generally accepted definition of "good faith" describes it as "[a] state of mind consisting [of] . . . honesty in belief or purpose . . . or . . . absence of intent to defraud or seek unconscionable advantage.[86]

ConDevel may argue that Nesbit acquired the data in "good faith," within the scope of the Marshall Statute because Nesbit accessed the computer system under the honest purpose of good faith testing, or correcting a security flaw or vulnerability, during the performance of his employment and he had no intention to defraud or otherwise gain unconscionable advantage. ConDevel could support its argument with the relevant provisions of DMCA.[87] The Southern District Court in New York had the opportunity to apply and analyze the relevant provisions of DMCA in *Universal City Studios v. Reimerdes*.[88] In that case, computer hackers had created a computer program that was able to circumvent the protection system to ensure motion pictures could not be copied.[89] The program had been posted on the Internet.[90] When sued by the copyright owner, the defendants claimed they fell under the good faith exception of the DMCA because they were doing encryption research.[91] The court held that the defendants' actions did not qualify under the good faith exception.[92] The court explained that a good faith exception exists when a person accesses "a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting [of a] security flaw or vulnerability, with the authorization of the owner or operator of such computer system or computer network."[93]

84. EF Cultural Travel BV v. Explorica, Inc., 318 F.3d 58, 63 (1st Cir. 2003).

85. The DMCA looks at "good faith" in two particular situations: (1) when considering liability for Internet service providers in the posting of copyrighted materials, and (2) when liability may be imposed for circumventing technological measures used to protect copyrighted materials. Digital Millennium Copyright Act, 17 U.S.C § 1201(g).

86. Black's Law Dictionary, 701 (7th ed. 1999).

87. Digital Millennium Copyright Act, 17 U.S.C. § 1201(j).

88. 111 F. Supp.2d 294 (S.D.N.Y. 2000).

89. *Id.* at 303.

90. *Id.*

91. *Id.* at 321.

92. *Id.*

93. *Id.*

In *Universal City Studios*, the record did not reflect defendants' having anything to do with testing computers or computer systems.[94] ConDevel may argue that contrary to *Universal City Studios*, in this case, Nesbit's program was created for the sole purpose to test and reveal the vulnerabilities in ConDevel's computer system. More specifically, Section 1201(j) of the DMCA provides a "good faith exception" if access to a computer system or network was done with the purpose to test or investigate the security or vulnerabilities in the system or network.[95] ConDevel could refer to Record indicating that Nesbit had repeatedly made several comments to his supervisor in person and through email, to discuss the weak security measures in place at ConDevel.[96] Nesbit specifically designed and installed the keylogger program with the sole purpose to expose the flaws in ConDevel's computer system and alert the company of the security issues. It is an undisputed fact that the intention of Nesbit was to access the system and then report to the management with his findings.[97] Indeed, Nesbit's actions did result in improving the data security system. Moreover, the information Nesbit obtained was not subject to any further unauthorized disclosures either before or after ConDevel became aware of the breach. Therefore, good faith existed on Nesbit's part from the time that the key logger program was created and it is irrelevant what he did with the information after he created the key logger program

On the other hand, Baylor based on the generally accepted definition of "good faith" as "[a] state of mind consisting [of] . . . honesty in belief or purpose . . . or . . . absence of intent to defraud or seek unconscionable advantage[98] could argue that according to the record Nesbit does satisfy the necessary requirements. He could draw an analogy from the language used by the Ninth Circuit in *Rossi v. Motion Picture Ass'n of America*, which held that 'good faith belief' is a subjective standard.[99] In that case, the defendant-infringer argued that the copyright holder's good faith belief should be held to an objective standard.[100] However, the Court cited a long tradition of using the subjective standard to interpret 'good faith' in accordance with the general definition of good faith.[101] "Good-faith" is [a] state of mind consisting [of] . . . honesty in belief or purpose.[102] The Court disagreed with the defendant's objective

94. *Id.*
95. Digital Millennium Copyright Act, 17 U.S.C. § 1201(j).
96. R. at 3.
97. R. at 4.
98. Black's Law Dictionary, 701 (7th ed. 1999).
99. *Rossi*, 391 F.3d at 1004.
100. *Id.*
101. *Id.*
102. *Id.* at 1004, in footnote 70, citing Black's Law Dictionary, 701 (7th ed. 1999).

standard of "good faith" and held that where the infringers' representations formed the impression that the materials were available for download, the copyright holders could subjectively conclude that such materials were available.[103] Even with the Court's refusal to adopt the infringer's objective standard, it did not solely apply the definition of subjective good faith. Rather, the Court's decision was based on both the representations of the infringers, in concert with the copyright holders' subjective belief in good faith that the posted materials were their property.

Baylor may argue that the record indicates that Nesbit's motives were not all that honest. Nesbit was not driven solely by the desire to demonstrate to his superiors how insufficient the security system was but he was equally, if not mostly, motivated by his aspiration to enjoy the privileges reserved to the executives[104] as well as enhance his position and reputation within the company.[105] This alone negates the "honesty in purpose" requirement or at least creates a genuine issue of material fact better left for the jury to determine.

Additionally, even if the court were to recognize "good faith testing" at the time of the installation of the "keylogger" program, Baylor could argue that ConDevel is barred from making this a good faith claim based on its actions when it discovered Nesbit's activities. The court in *Universal City Studios* relied on Section 1201(g)(3) of the DMCA to examine when a person can claim he or she is engaged in good faith research.[106] The court held that the time to determine whether research is conducted in good faith is established by whether it is communicated to the copyright owner in a timely fashion.[107] In *Universal City Studios*, the court stated that there was no evidence that the defendants made any effort to provide their results to the copyright owners.[108] Similarly, there is no sufficient evidence to show Nesbit was going to provide his results to ConDevel. To the contrary Nesbit used that information to avail himself of the benefits reserved to the high ranked officers of the company. ConDevel on its part when it discovered Nesbit's actions attempted to conceal the acquisition of the data as it has been clearly demonstrated by the communication between ConDevel's CEO and the Director of the Technology Department "as far as we know, no one knows that this ever happened. Let's keep it that way."[109] Baylor may thus argue that the state of mind required to establish good faith is lacking in either context.

103. *Id.* at 1005.
104. R. at 3
105. R. at 4
106. 111 F. Supp.2d at 321.
107. *Id.*
108. *Id.*
109. R. at 5.

4. *Use for the "purposes designated by the agency"*

The Marshall Data Protection Act Section105(d) states: ". . . .Good faith acquisition of personal information by an employee or agent of the agency is not a breach of the security of the system, provided that the personal information is used for the purposes designated by the agency and/or is not subject to further unauthorized disclosure." A proper interpretation of the Marshall Data Protection Act would look to whether there was a subjective belief that the acts where in "good faith" combined with evidence that the data was *"used for purposes designated by the agency."*

Baylor may argue that while ConDevel now claims the disclosure of personal data was acquired by Nesbit in good faith, there must be some additional showing beyond a mere statement of good faith. In order to comply with Section105(d), ConDevel must show that the acquisition was within the purposes designated by ConDevel.

Accordingly, Baylor may argue that neither ConDevel nor Nesbit could have subjectively believed that Nesbit was acquiring or using the data in accordance with the purposes designated by ConDevel as Nesbit lacked honesty in his actions. Baylor could argue that ConDevel cannot claim that Nesbit was acting within and for the purposes of the company when he hacked into the computer system and used the acquired the personal data for his own purposes, including creating false credentials for his own use. Nesbit was not assigned to the technology support department responsible for ConDevel's computer infrastructure nor in the Human Resources Department which would allow him to access and use this information.[110] Nesbit went to great lengths to obtain access of the computer system via surreptitious means and conceal the installation keylogger program on Baylor's computer, and took means to obfuscate any possible detection of the intrusion into Baylor's computer.

Additionally, Baylor could claim that there is no evidence in the Record that Nesbit had the belief that he was doing what the company wanted or using the personal data within the same scope ConDevel used the information. There is no indication that Nesbit used the data for the business purposes of his employer since he did not use the data to advance ConDevel's position in the Real Estate market. He never informed ConDevel of his acquisition of the data, nor of the manner in which he used the data. Baylor could claim that although the data stored was to be used by the executives to avail themselves of the privileges afforded by ConDevel, Nesbit's use of the personal information acquired to essentially impersonate Baylor did not comply with the *"purposes designated by the agency."* The facts strongly support the assertion that Nesbit did

110. R. at 2.

not use the information with the purposes of the company or at least create a genuine issue of material fact rendering summary judgment inappropriate.

ConDevel would likely reiterate its arguments presented under (1) namely that the when Nesbit acquired the data his sole purpose was to test the security system and force the company to fix the security flaws. He was under the honest belief that he was acting for the benefit of the company, that his actions were justified by the good cause of protecting the personal information stored in ConDevel's network. This purpose, improving network's security and thus the company's efficiency and reliability, is encompassed within the duties of a loyal employee. ConDevel will refer to the Record to show that Nesbit had the subjective belief required for good faith –acting with honesty in purpose—and that the disclosure was made in the course of Nesbit's performance of his duties with the same purposes designated by ConDevel. Although not directly authorized to perform security checking, Nesbit had the honest belief that acquisition and use of the data was in the best interest of the company therefore invoking the application of Section105(d).

5. *"No further unauthorized disclosure"*

The Marshall Data Protection Act Section 105(d) states that the data must be *"used for the purposes designated by the agency and/or that is subject to further unauthorized disclosure"*[111].

ConDevel could point to the language of the Marshall Notification Statute Section 105(d). As read an agency can invoke the "good faith" exception if it can prove that the data was used *"for the purposes designated by the agency and/or* that is subject to further unauthorized disclosure". It would probably argue that the Record indicates that no other individual or entity ever obtained access or acquired the data Nesbit downloaded to his computer. Therefore even if the court found that the data was not used in accordance with ConDevel's purposes, Section 105(d) would still apply and ConDevel should be found free of liability.

Baylor would likely counter- argue that further disclosure did take place when Nesbit first started visiting the VIP lounges and Clubs under Baylor's name and especially after demonstrating the inappropriate conduct at Shady Links Club which cause Baylor's blacklisting in all exclusive clubs in the State of Marshall. Further disclosure of his personal information has been unavoidable in order to explain the situation to the establishments involved and maintaining the "blacklist" and restore his good name.

111. Marshall Data Protection Act, 17 Marshall § 105(d).

Additionally, Baylor may argue that the Marshall Data Protection Act "good faith" exception could not have been met because Nesbit violated his duty of loyalty to ConDevel, since he did not act with honesty in purpose. Incorporated within the Marshall Data Protection Act are the concepts of "good faith" acquisition and usage of acquired information for purposes designated by the company. These principles closely mirror the agency principle of good faith where the employee is to act on behalf of the employer in the course of employment. Therefore, if the employee is not properly using the personal information acquired in the same manner designated by the employer, there is breach, because outside disclosure occurred.

This line of reasoning would necessarily lead to the following issue likely to be addressed by the parties.

Since the subjective standard of "good faith" as noted above is [a] state of mind consisting [of] . . . honesty in belief or purpose,[112] the employee must have "honesty in purpose" in the performance of one's actions in order for the employer to state that there was "good faith" acquisition. When an employee acquires adverse interests to the employer, authority to act on behalf of that employer is terminated.[113] Accordingly, the duty of loyalty has been breached when the employee has acted for one's own benefit and cannot then hold out that one is performing in "good faith."

In developing this issue of first impression, the Marshall Data Protection Act's interpretation of "good faith" acquisition could look to other statutes for guidance in determining whether "good faith" may be found when the employee has exceeded the access granted by the employer. Especially in the area of regulating access to computers, additional guidance could be offered by CFAA, a criminal statute with an additional private cause of action.[114] The CFAA criminalizes access to protected computers by persons without authorization or those whom exceed their authorization with the intent to defraud.[115] The court has interpreted the CFAA as imposing limitations upon access thereby "enhancing control by information providers"[116] similarly to the scope of the Marshall Data protection Act. The court has interpreted the limitations on access to apply to those unauthorized persons both external and internal to the employer's company.[117] Where an employee violates the duty of loyalty

112. *Rossi*, 391 F.3d at 1004. in footnote 70, citing Black's Law Dictionary, 701 (7th ed. 1999).

113. RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

114. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g).

115. 18 U.S.C. § 1030(a)(4).

116. *EF Cultural Travel BV v. Explorica, Inc.*, 318 F.3d 58, 63 (1st Cir. 2003).

117. *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006).

to the employer, the principal-agent relationship is terminated.[118] Where there is no principal-agent relationship, the good faith exception under the Marshall Data Protection Act Section105(d) cannot be applied.

Baylor may argue that Nesbit could not have been authorized under ConDevel's "Computer Use Policy" in accessing the human resources database. In *Int'l Airport Ctrs., L.L.C. v. Citrin*, defendant-employee had been given a laptop to use owned by plaintiff-company.[119] The defendant was given the laptop to use to record data identifying potential acquisitions that he collected during the course of his work.[120] The defendant decided to quit and breached his employment contract by going into business for himself using the information obtained through his work for the plaintiff.[121] Before the defendant returned the laptop, he deleted all the data on it, including data that would have revealed his improper conduct.[122] The Seventh Circuit relied on the CFAA and held that the CFAA made the distinction between "'without authorization' and 'exceeding authorized access'."[123] Exceeding authorized access is accessing a computer without authorization and using that access to obtain information that a person is not entitled to obtain.[124] On the contrary, a person without authorization violates the duty of loyalty, or fails to disclose adverse interests.[125] The Seventh Circuit found that the defendant destroyed data he knew the plaintiff had no duplicates of and therefore needed.[126] The Court found for the plaintiff, and determined that the while the employee previously had authorization to access the files on the computer, the defendant breached his duty of loyalty to the employer by destroying the plaintiff's files and therefore the defendant was without authorization and thus terminated the agency relationship.[127]

Baylor could argue that ConDevel cannot claim that Nesbit was authorized to hack into the computer system, acquire the personal data and use it for his own benefit, namely creating false credentials for his own use. Nesbit was merely a "sales associate" at ConDevel, with the responsibilities of a "sales associate."[128] Nesbit was not assigned to the technology support department responsible for ConDevel's computer infrastructure. Nesbit did not obtain approval from either his superiors or the technology support department when implementing his plan to

118. *Id.* at 421.
119. *Id* at 419.
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at 420.
124. *Id.* at 420.
125. *Id.* at 420-21.
126. *Id.* at 421.
127. *Id* at 420-21.
128. R. at 2.

place his keylogger program on Baylor's computer. Nesbit was consistently rebuked when informing ConDevel superiors about his concerns, and told to "leave technological issues to the technology support department."[129] Nesbit went to great lengths to obtain access of the computer system via surreptitious means. Nesbit did not request permission to place the keylogger program on any computer, and took means to obfuscate any possible detection of the intrusion into Baylor's computer. In utilizing his keylogger program, Nesbit intentionally set it to distribute the access passwords to an external private email address instead of an email address on ConDevel's network.[130] The facts strongly support the assertion that ConDevel would not have authorized Nesbit's actions and that ConDevel would not have believed that Nesbit was acting on ConDevel's behalf.

Additionally, Baylor may argue that even though Nesbit may have been employed by ConDevel and ostensibly authorized to do such security testing on ConDevel's computers, Nesbit subsequently lost any authorization that he may have had when he used the information from the human resources database for his own benefit. While it may be arguable that Nesbit had authorization to place the keylogger program on the computer for the purposes of conducting his security tests as he originally intended,[131] Nesbit, like the defendant in *Citrin,* lost all authority to access the personal data when he used the information he gained for his own benefit. Absent authority to access the data, and Nesbit's personal use of the information, ConDevel was the subject of a "breach of security of the system" which required disclosure by ConDevel. Baylor will argue that the lower court improperly found that ConDevel had no duty to notify individuals because there was unauthorized access and disclosure of personal information. The Marshall Data Protection Act requiring "good faith" acquisition could not have been met because Nesbit violated his duty of loyalty to ConDevel, since he did not act with honesty in purpose.

On the other hand, ConDevel may use the language of the CFAA and relevant case law to support its argument. CFAA Sections 1030(a)(1), (2), and (4) allow a company to claim a good faith exception if its computer system was used inappropriately by someone who merely exceeded authorized access.[132] ConDevel may argue that Nesbit's agency status was not terminated because he only exceeded his authority for access and therefore was not without authorization. Contrary to *Int'l Airport Ctrs., L.L.C.*, Nesbit's actions were in good faith because they

129. R. at 3.

130. R. at 3.

131. R. at 3.

132. Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(1), (2) and (4).

were in the best interests of the company since the result was an improvement in the company's computer systems. Furthermore, Nesbit had no adverse interests to ConDevel's business. Unlike the defendant in *Int'l Airport Ctrs., L.L.C.,* Nesbit was not trying to gain an advantage in the business, nor was he trying to use the information in a competing venture. Therefore, ConDevel is entitled to the benefit of the "good faith exception" because Nesbit only exceeded his access to the computer system and the information obtained was not used to compete with ConDevel.

Furthermore, in *Worldspan L.P. v. Orbitz*, the court held that it is clear from the language of the CFAA that the term "exceeding authorized access" is not encompassed by the term "accessing a computer without authorization."[133] The plaintiff-company is referred to as a computer reservations system ("CRS").[134] It processes reservations and issue tickets for airlines, hotels, car rental agencies, tour companies and cruise lines.[135] The plaintiff makes money from the airlines when it books these reservations.[136] The defendant was attempting to use a direct connect model which would not generate any revenue from the airlines for the plaintiff.[137] The plaintiff warned the defendant that it could not use the plaintiff's data in relation to its direct connect model.[138] Because the defendant only exceeded authorized access, the court dismissed that count of the complaint.[139] ConDevel and Nesbit had an employer/employee, principal/agent relationship. Similar to *Worldspan, L.P.*, ConDevel may argue that by virtue of their relationship, Nesbit only exceeded his authorized access to the computer network. Because Nesbit had authorization, his acquisition of the personal information did not constitute a breach of the computer system. Therefore, Nesbit's access of the computer system was in good faith and not a violation of the statute.

ConDevel may also argue that because the issue of good faith acquisition is an issue of first impression and no definition is provided by the statute, the business judgment rule and its interpretation of good faith should apply. Although Nesbit was not a corporate director, ConDevel may argue that employees acting in good faith are similar to directors acting in good faith. A regular employee does not have the fiduciary responsibilities of a corporate director, but is an agent of the corporation nonetheless, thus the Marshall Data Protection Act Section 105(d) should apply to the actions of corporate employees and corporate direc-

133. *Worldspan L.P. v. Orbit*, 2006 U.S. Dist. LEXIS 26153 at *14.
134. *Id* at 2.
135. *Id.*
136. *Id.*
137. *Id.* at 4.
138. *Id.*
139. *Id.*

tors. The business judgment rule is generally a *laissez faire* approach to judging the decisions of corporate directors but it allows courts to analyze the "content of [the directors'] 'judgment' and . . . the information on which it was based."[140] This evaluation of the decisions of corporate directors is used to analyze whether their actions were in good faith. The business judgment rule states that courts will not analyze the decisions of corporate directors if those actions are "taken in good faith and in the exercise of honest judgment in the lawful and legitimate furtherance of corporate purposes."[141]

Applying this standard to Nesbit's actions, ConDevel will argue that Nesbit's unauthorized security audit was an honest, good faith action, taken to further the corporation's interest in better network security. Nesbit thought that by exposing flaws in the network's security, he would help the company as a whole. As such, he had a good faith intent when acting, thus triggering the exception to the Marshall Data Protection Act. ConDevel may also argue that although Nesbit ultimately used the information he obtained for his own purposes, this subsequent use did not invalidate the good faith intent of his original data acquisition. This later use of the information did not rise to the level of bad faith, which requires behavior that is driven by "some interested or sinister motive."[142] ConDevel might argue that since Nesbit did not decide to use Baylor's VIP club access until after acquiring the employee files, the initial breach itself was not made in bad faith. Furthermore, ConDevel may argue that even if Nesbit did have the intention of using Baylor's VIP status when he committed the breach, it did not rise to the level of bad faith because his actions were not inherently sinister. Had Nesbit obtained the employee data solely to discredit Baylor within the State of Marshall by abusing his VIP status, then, Nesbit's actions would have been completely outside the scope of his employment, and not a good faith acquisition within the meaning of the statute. In the case at bar, Nesbit simply thought it would be fun to see how Marshall's wealthy elite lived. His curiosity cannot be described as inherently sinister because his intention was not to harm Baylor.

ConDevel may further argue that even if Nesbit was not technically authorized to audit electronic security, he was under the "honest, though mistaken, belief that . . . [he] had good cause" for his action, which would negate the element of bad faith.[143] Nesbit was aware that the network security was lacking and that ConDevel had not prioritized fixing the

140. RSL Communs. PLC v. Bildirici, 2006 U.S. Dist. LEXIS 67548, at *17 (S.D.N.Y. 2006).

141. Scheuer Family Foundation, Inc. v. 61 Associates Corp, 179 A.D.2d 65, 69 (N.Y. App. 1992); *see also* Stein v. Bailey, 531 F.Supp. 684, 690 (S.D.N.Y. 1982).

142. Pugh v. Sees Candies, 203 Cal.App.3d 743, 764 (1988).

143. *Id.* at 770.

critical security flaws. Since his personal information and that of all other employees was stored on the network, he mistakenly believed that his actions were justified by the good cause of protecting himself and his coworkers. Improving network security would prevent a malicious intruder from using employee data for identity theft, and would protect sensitive customer data as well. Moreover, since the Pugh court applied elements of the business judgment rule to an employment contract case, ConDevel may argue that the business judgment rule is therefore applicable when interpreting good faith in other situations involving corporate employees and their actions.