

IN THE SUPREME COURT OF THE STATE OF MARSHALL

---

**Ron Baylor,**  
**Plaintiff—Appellant,**

**v.**

**ConDevel, Inc.**  
**Defendant—Appellee.**

---

ON APPEAL FROM THE FOURTH CIRCUIT COURT OF APPEALS OF THE STATE OF  
MARSHALL

---

BRIEF FOR THE APPELLANT

---

## QUESTIONS PRESENTED

- I. Did the appellate court err in holding that the surreptitious installation of a “keylogger on Baylor’s computer did not state a claim for a recognized claim of invasion of privacy under the theory of intrusion upon seclusion where the computer was kept in a personal office, where Nesbit did not have authority to access Baylor’s personal information, and where Baylor was humiliated as a result?
  
- II. Did the appellate court err in ruling that ConDevel was exempt from the notification provision of the Marshall Data Protection Act, 17 Marshall Code § 105 (2006) where ConDevel’s employee stole the personal information of the company in disobedience of explicit supervisory instructions, where he used the information to imposter a VIP executive and access exclusive clubs, and where ConDevel did not provide investigation details, credit reporting or notification after the breach?

## TABLE OF CONTENTS

QUESTIONS PRESENTED.....	i
TABLE OF CONTENTS.....	ii
TABLE OF AUTHORITIES .....	v
STATEMENT OF THE CASE.....	1
SUMMARY OF ARGUMENT .....	4
ARGUMENT.....	6
I. THE APPELLATE COURT ERRED IN RULING THAT BAYLOR DID NOT STATE A CLAIM FOR INTRUSION UPON SECLUSION BECAUSE MARSHALL SHOULD RECOGNIZE A CLAIM FOR INTRUSION UPON SECLUSION AND BECAUSE NESBIT COMMITTED AN INTRUSION UPON BAYLOR’S SECLUSION WHEN HE SURREPTITIOUSLY INSTALLED A KEYLOGGER ON BAYLOR’S COMPUTER AND ACCESSED HIS PERSONAL INFORMATION.....	7
A. The State of Marshall should recognize a cause of action for intrusion upon seclusion because doing so will provide a remedy for injured Marshall citizens and because doing so will provide incentive for people to avoid invading each other’s privacy .....	7
B. The appellate court erred in ruling that Baylor did not state a claim for intrusion upon seclusion when Nesbit secretly installed a keylogger program on Baylor’s computer which he kept in his personal office and protected with passwords and when Nesbit accessed Baylor’s personal information which Nesbit did not have authority to access.....	10
1. The installation of the keylogger program and subsequent access of Baylor’s file was an intentional, unauthorized intrusion because ConDevel ignored warnings about lax company security, because Nesbit installed the keylogger program in secret and because Nesbit was merely a low-level employee.....	10
2. The intrusion would be offensive or objectionable to a reasonable person because Nesbit recorded Baylor’s computer keystrokes and because Baylor’s file contained personal information.....	12

3. Baylor had a zone of solitude in his work computer because his computer was located in his personal office, because he protected at least some of his computer files with passwords and because ConDevel had no company policy about monitoring employee computer use .....13
4. Baylor had a zone of solitude as to the disclosure of his personal information to an unauthorized person because the information was not available to unauthorized employees such as Nesbit, because the information was only obtainable by surreptitiously installing a keylogger program on Baylor’s work computer and because of the sensitive nature of the information .....16
5. The State of Marshall should decline to adopt a formulation of intrusion upon seclusion which would require a plaintiff to show that the intrusion caused anguish and suffering because such a formulation will not adequately protect the privacy of the citizens of Marshall .....21
6. Assuming arguendo that Marshall does require an element of anguish and suffering, Nesbit’s intrusion caused Baylor anguish and suffering because he was deeply embarrassed when he was informed in front of his friends that his membership had been revoked at Shady Links golf course, because the manager of Les Deux Pommes shouted at him, “we do not want drunks and troublemakers in our restaurant” and because a reasonable person would have suffered anxiety knowing that someone had recorded their computer’s keystrokes and accessed their personnel file .....23

**II. THE APPELLATE COURT ERRED IN EXCUSING CONDEVEL FROM ITS AFFIRMATIVE DUTY TO NOTIFY UNDER THE NOTIFICATION PROVISION OF THE DATA PROTECTION ACT SINCE NESBIT USED THE PERSONAL INFORMATION HE STOLE TO IMPERSONATE AN EXECUTIVE AND GAIN ACCESS TO EXCLUSIVE CLUBS, AND SINCE HE FURTHER USED THE STOLEN CONFIDENTIAL INFORMATION IN DISOBEDIENCE OF COMPANY INSTRUCTIONS TO PURSUE HIS DESIRE TO ENJOY EXECUTIVE BENEFITS .....26**

- A. ConDevel is not exempt from the Marshall Code Data Protection Act on the basis of discretion to notify since Nesbit’s use of the confidential information was not within compliance of ConDevel’s corporate scopes and purposes, and to allow ConDevel such discretion to notify of security breaches would starkly contrast the purpose intended by the Marshall Data Protection Act and others like it .....27
  1. Acquisition of the personal information, subject to the unauthorized disclosure, was not used in compliance with ConDevel’s scopes and purposes since it was used by Nesbit to gain access to ConDevel’s

confidential VIP benefit system, to fraudulently use it to imposter an executive, to gain access to exclusive clubs and thereafter partake in a fight with a prominent member of the club .....	28
2. Granting discretion to notify of security breaches to ConDevel would starkly contrast with the underlying policies and purposes of Data Protection Acts since ConDevel did not inform anyone about the incident, did not offer any investigation details, and did not provide proof of any curative efforts such as those promoted by the Marshall Data Protection Act .....	30
B. ConDevel is not exempt from the Marshall Code Data Protection Act on the basis of the § 105(d) “good faith acquisition” exception since ConDevel’s former employee surreptitiously installed the keylogger after his supervisor consistently told him to “mind his own business and leave technological issues to the technology support department” and since after the breach ConDevel did not inform any one and did not offer any investigation details to remedy effects of the breach .....	32
1. The secretive installation of a keylogger and subsequent theft of personal VIP information filtered to the personal computer of ConDevel’s former employee despite continuous supervisory directions to leave the security issue alone does not constitute “good faith acquisition” under § 105(d) of the Marshall Code Data Protection Act .....	33
2. The breach of security of the system by ConDevel’s former employee does not satisfy the second requirement necessary to constitute an exemption under 105(d) since Nesbit’s filtering of human resource database files through installation of a hidden keylogger resulted in unauthorized acquisition of personal information that, by enabling the Nesbit to create a VIP alias and frequent upscale VIP venues, was used for purposes not designated by the agency .....	34
3. The failure of ConDevel, a company paranoid of having its inadequate security system revealed, to institute credit report checks, investigation, or other reasonable remedial actions following the unauthorized breach of security and firing of the breaching employee support a strong likelihood that further unauthorized disclosure may have resulted.....	38
CONCLUSION.....	41

## TABLE OF AUTHORITIES<sup>1</sup>

### CASES

<i>Anderson v. Mergenhagen</i> , 283 Ga. App. 546, 549 (1966) .....	24
<i>Aronson v. Sprint Spectrum, L.P.</i> , 767 A.2d 564, 568 (Pa. Super. 2001).....	24
<i>Bassiouni v. FBI</i> , 436 F.3d 712, 738 (7th Cir. 2006).....	27
<i>Busse v. Motorala, Inc.</i> , 351 Ill. App. 3d 67, 73 (1 Dist. 2004) .....	20, 21
<i>Butera &amp; Andrews v. IBM, Corp.</i> , 2006 U.S. Dist. LEXIS 75318 *3 (D.C. Oct. 18, 2006) .....	35
<i>Calyon v. Mizuho Securities USA, Inc.</i> , 2007 U.S. Dist. LEXIS 66051 *3 (S.D.N.Y. July 24, 2007).....	35, 36-37, 38
<i>Daily Times Democrat v. Graham</i> , 276 Ala. 380, 382 (1964).....	21
<i>Doe v. High-Tech Institute, Inc.</i> , 972 P.2d 1060, 1067 (Colo. App. Div. III 1998).....	
.....	8, 13, 17-18, 20, 22
<i>Dudick v. Vaccarro</i> , 2007 U.S. Dist. LEXIS 45953 *3 (M.D. Pa. June 25, 2007).....	35, 36, 37-38
<i>FBI v. Doe</i> , 936 F.2d 1346, 1357 (App. D.C. 1991).....	27-28
<i>Forbes v. Wells Fargo Bank, N.A.</i> , 420 F. Supp. 2d 1018 (D. Minn. 2006).....	40-41
<i>Giordano v. Wachovia Securities, LLC</i> , 2006 U.S. Dist. LEXIS 52266 * 3 (D.N. J. July 31, 2006).....	40-41
<i>Greywolf v. Carrol</i> , 151 P.3d 1234, 1246 (Alaska 2007) .....	13, 15, 16
<i>Frees, Inc. v. McMillian</i> , 2007 U.S. Dist. LEXIS 57211 *6 (W.D. La. August 6, 2007) .....	33
<i>Int'l Airport Centers, LLC v. Citrin</i> , 440 F.3d 418, 419 (7th Cir. 2005).....	35
<i>Johnson v. K-Mart Corp.</i> , 311 Ill. App. 3d 573, 577 (Ill. App. 1st Dist. 2000). .....	6, 11
<i>LaCrone v. Ohio Bell Tel. Co.</i> , 114 Ohio App. 299 (10th Dist. 1961).....	9
<i>Lewis v. LeGrow</i> , 258 Mich. App. 175, 193 (2003) .....	12, 14
<i>Leventhal v. Knappek</i> , 266 F.3d 64, 74 (2nd Cir. 2001).....	14, 15

---

<sup>1</sup> This brief uses ALWD.

<i>Luce v. First Equip. Leasing Corp.</i> , 960 F.2d 1277, 1278 (5th Cir. 1992).....	28-29
<i>Melvin v. Burling</i> , 141 Ill. App. 3d 786, 789 (3rd Dist. 1986). ....	7, 24, 25
<i>Miller v. National Broad. Co.</i> , 187 Cal. App. 3d 1463 (2nd Dist. 1986) .....	9
<i>Monroe v. Darr</i> , 221 Kan. 281, 286 (1977).....	24
<i>Mucklow v. John Marshall Law School</i> , 176 Ill. App. 3d 886, 894 (1st Dist. 1988) .....	11, 12
<i>Muick v. Glenayre Elec.</i> , 280 F.3d 741, 743 (7th Cir. 2002).....	14, 15
<i>Pavesich v. New England Life Ins. Co.</i> , 102 Ga. 190, 194 (1905).....	7
<i>Relief Fire Insur. Co. of N.Y. v. Shaw</i> , 94 U.S. 574, 576 (1877) .....	28-29
<i>Remsburg v Docusearch, Inc.</i> , 816 A.2d 1001 .....	39
<i>Roth v. J.N. Roth Corp.</i> , 363 Mo. 767, 777 (Mo. 1952) .....	28-29, 30
<i>Sabrina W. v. Willman</i> , 4 Neb. App. 149, 159 (1995) .....	22
<i>Sanders v. American Broadcasting Companies, Inc.</i> , 20 Cal.4th 907, 915 (1999) .....	13, 17, 18, 19
<i>Smith v. Doss</i> , 251 Ala. 250, 253 (1948) .....	24
<i>Shulman v. Group W. Prod., Inc.</i> , 18 Cal. 4th 200, 243 (1998).....	9
<i>Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.</i> , 119 F. Supp. 2d 1121, 1123 (W.D. Wa. 2000) .....	33
<i>Snakenberg v. Hartford Casualty Ins. Co., Inc.</i> , 299 S.C. 164, 169 (App. 1989) .....	7, 22
<i>State of Ohio v. Grays</i> , 2001 Ohio App. LEXIS 5397 *12 (8th Dist. Dec. 6, 2001).....	33-34
<i>Sussman v. U.S.</i> , 2006 U.S. Dist. LEXIS * 39 (E.D.N.Y. Sept. 30, 2007).....	27
<i>Toomer v. Garrett</i> , 155 N.C. App. 462, 479 (2002) .....	11, 12, 13, 17, 18, 19
<i>Trustmark Life Insur. Co. v. The U. of Chicago Hosp.</i> , 207 F.3d 876, 883 (7th Cir. 2000)....	33-34
<i>U.S. v. Simons</i> , 206 F.3d 392, 398 (4th Cir. 2000) .....	14
<i>White v. White</i> , 344 N.J. Super 211, 223 (2001).....	14
<i>Yoeckel v. Samonig</i> , 272 Wis. 430 (1956) .....	8

## STATUTES

17 Marshall Code § 105 (2006). ....	6, 26-27, 31-33, 38-39
-------------------------------------	------------------------

Marshall R. Civ. P., Rule 56(c).....6

**SECONDARY SOURCES**

*Black’s Law Dictionary* 307 (Bryan A. Garner ed., 2d pocket ed., West 2001) .....33, 34

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 973-74 (1964) .....8, 22

Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security*, 43 Hous. L. Rev. 1597, 1599 (2007).....31, 39

Matthew Bender, *1-2 Law of the Internet* § 2.03 (LexisNexis 2005) .....31

*Restatement (Second) of Torts* § 652B (1977)..... 6, 7, 10, 22-23

R.T. Kimbrough, *Right of Privacy*, 138 A.L.R. 22, 25 (1942) .....24

Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C.L. Rev. 255, 286 (2005).....39

William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 423 (1960)..... 22, 24-25

## STATEMENT OF CASE

Plaintiff/Appellant Ron Baylor brought this suit against Defendant/Appellee ConDevel, Inc. in 2005 in the State of Marshall. Baylor claims that ConDevel intruded upon his seclusion when ConDevel's employee, Nesbit, surreptitiously installed a keylogger program on his work computer and subsequently accessed his employee personnel file. Baylor also claims that ConDevel violated the Marshall Data Protection Act when he failed to notify him of a personal data security breach. The trial court granted summary judgment for ConDevel. The court ruled that Marshall does not recognize a cause of action for intrusion upon seclusion and, even if it did, Baylor had not stated a claim. The trial court also ruled that ConDevel was exempt from the notification statute.

Baylor was a vice president at ConDevel. (R. 2.) ConDevel had repeatedly ignored warnings regarding their lack of security. (R. 3.) Nesbit, who was a low-level employee at ConDevel, surreptitiously installed a keylogger program on Baylor's work computer. (R. 2-3.) Nesbit subsequently accessed Baylor's employee personnel file and used Baylor's personal information to impersonate him at an exclusive club where he was thrown out for drunken fighting. (R. 4.) As a result of Nesbit's impersonation, Baylor was humiliated by being blacklisted from exclusive clubs. (R. 4-5.) Baylor reported the impersonation to ConDevel and although ConDevel fired Nesbit, it did not investigate the incident nor offer any assistance to Baylor. (R. 5.)

Ron Baylor is an executive vice president at ConDevel who is responsible for the human resource department. (R. 2.) By virtue of that position he has access to all employees' electronic personnel files which "contain employee contact information, social security numbers, driver license numbers, employee performance evaluations, employee salary data, employee benefits

information, employee awards and honors, and other personal data.” (R. 2.)

Nesbit worked for ConDevel as a sales associate. (R. 2.) He wanted to take a “quick ladder” to the executive ranks of the company. (R. 2.) Because of his disappointment at not being able to enjoy the benefits reserved for high-level employees, he had been heard to say, “I wonder if there is another way to enjoy the good life reserved to the executives.” (R. 2.)

Recently ConDevel has struggled financially. (R. 1.) As a result, no computer upgrades have been made and the technical support department is short-staffed. (R. 2.) Few resources have been devoted to corporate information security. (R. 2.)

ConDevel has a policy which states “employees are responsible for safeguarding all equipment and software provided by the company.” (R. 2.) But employees have been given no guidance as to what would be “appropriate safeguard measures.” (R. 2.) ConDevel has no policy of monitoring employee computer use. (R. 2.)

Nesbit commented multiple times to his supervisor that ConDevel had minimal security and that “ConDevel was a data breach waiting to happen.” (R. 3.) However, ConDevel did not act on Nesbit’s complaints. (R. 3.) Instead the supervisor consistently told Nesbit to “mind his own business and leave technological issues to the technology department.” (R. 3.) Nesbit “devised a plan to raise upper management’s awareness of the company’s technological vulnerabilities.” (R. 3.) He created a keylogger program which he could install on another computer and which would “record keystrokes made on the target computer” and then email the record of those keystrokes back to Nesbit. (R. 3.)

One day Nesbit passed Baylor’s office and realized that Baylor would immediately be leaving for a meeting. (R. 3.) Realizing that no other employees were nearby, Nesbit entered Baylor’s office when Baylor left for the meeting. (R. 3.) Baylor’s computer was turned on and

Nesbit installed the keylogger program on Baylor's computer. (R. 3.)

From the subsequent emails sent to Nesbit from Baylor's computer, Nesbit learned "Baylor's login and passwords used to access many company files including the human resources database that contained the electronic employee personnel files" and "the benefit system and 'VIP Program' files used for setting up memberships at various exclusive clubs." (R. 4.) Although Nesbit intended to report his findings to management, once he used Baylor's login information to access the personnel files he "had a change of heart." (R. 4.) He realized that he could use his new access to the executive's benefits system for his own enjoyment and subsequently had several VIP club and restaurant memberships issued in Baylor's name. (R. 4.)

Nesbit began frequenting these establishments by gaining entry in Baylor's name. (R. 4.) On one such visit at the Marshall League Club, "Nesbit became seriously intoxicated and got into a fight with a prominent member of the club." (R. 4.) He was physically removed from the premises. (R. 4.) After the incident Baylor's name was added to a "blacklist" which is shared by many exclusive clubs and restaurants. (R. 4.)

Baylor was unaware of Nesbit's behavior and the subsequent blacklisting until he took some friends to play golf at a private course and was told "that his membership had been revoked due to his behavior at the Marshall League Club." (R. 4.) "Baylor was deeply embarrassed." (R. 4.) The next week Baylor took his family to an upscale restaurant but was denied service. (R. 5.) When Baylor demanded to see the manager the conversation became heated and the manager shouted, "We do not want drunks and troublemakers in our restaurant!" (R. 5.)

After these embarrassing incidents, Baylor realized that someone had accessed the human resources system and had had memberships issued in Baylor's name. (R. 5.) One of the few ConDevel technology experts assisted Baylor by examining Baylor's computer. (R. 5.) He

discovered the keylogger program and was then able to trace the program to Nesbit. (R. 5.)

When ConDevel's management became aware of what had happened Nesbit was fired. (R. 5.) However, management concluded that "no one outside the company accessed the files, thus no true data breach had occurred." (R. 5.) Fearing harm to ConDevel's reputation the company's chief operating officer told the technology expert who had assisted Baylor "as far as we know no one knows that this ever happened. Let's keep it that way." (R. 5.)

Following this incident the "technology support department tightened security." (R. 5.) No one was informed of the incident and ConDevel offered no investigation details to Baylor. (R. 5.) Nor did ConDevel "assist Baylor in rebuilding his good name." (R. 5.)

Based on these facts the Court should reverse the granting of summary judgment.

### **SUMMARY OF ARGUMENT**

The appellate court erred by ruling that Nesbit did not intrude upon Baylor's seclusion when he installed a keylogger program on Baylor's computer and subsequently accessed Baylor's personal information, and by ruling that ConDevel was exempt from the notification provision of the Marshall Data Protection Act.

An intrusion upon seclusion is an unauthorized intrusion which would be offensive or objectionable to a reasonable person into an area which the plaintiff had a zone of solitude. Some courts have also required the intrusion to cause anguish and suffering.

Marshall should recognize this cause of action because it will protect the privacy interests of the citizens of Marshall.

Nesbit's actions constituted an unauthorized intrusion because he was a low-level employee who surreptitiously installed a keylogger program on Baylor's computer and accessed his personal information. A reasonable person would be offended by the intrusion because

Nesbit recorded Baylor's keystrokes and accessed personal information. Baylor had a zone of solitude in his work computer because it was in his personal office and he had passwords on it. Baylor had a zone of solitude as to the disclosure of his personal information to an unauthorized person because of the sensitive nature of the information and because Nesbit was not authorized to access the information. This Court should not require a showing of anguish and suffering because doing so will not protect the privacy interests of the citizens of Marshall. Even if this Court does require such a showing, the intrusion caused anguish and suffering because Baylor was embarrassed and humiliated when the managers at the golf club and restaurant told him he was banned.

To be exempt from the notification provision of the Marshall Data Protection Act, an agency must prove that the personal information breached was actually a "good faith acquisition of personal information by an employee or agent of the agency" and was used for purposes designated by the agency and/or was not subject to further unauthorized disclosure. The appellate court also recognized an exemption based on discretion to notify. Discretion should be given only where the agency utilizing discretion promulgates substitute procedures and proves that they promote the underlying purposes of the statute.

ConDevel did not meet the burden of proof since Nesbit's secret installation of a keylogger program and filtering thereof to his personal computer did not constitute good faith acquisition, Nesbit's use of the information to impersonate Baylor and obtain access to exclusive clubs was not a use for purposes designated by ConDevel, and ConDevel's failure to take any measures to determine the scope of the breach or to notify anyone do not satisfy a conclusion that the information was not subject to further unauthorized disclosure.

ConDevel is not entitled to discretion to notify since ConDevel failed to provide any

proof of substitute procedures, and since ConDevel did not notify anyone, but instead sought ways to keep the breach undisclosed.

This court should reverse because Nesbit intruded upon Baylor's seclusion and because ConDevel is not exempt from the notification provision of the Marshall Data Protection Act.

### **ARGUMENT**

The Appellate Court erred in holding that Baylor did not state a recognized claim of invasion of privacy under the theory of intrusion upon seclusion and that ConDevel was exempt from the notification provision of the Marshall Data Protection Act, 17 Marshall Code § 105 (2006). According to the Restatement, as adopted by Marshall courts, "[o]ne 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." *Restatement (Second) of Torts* § 652B (1977).

According to the Marshall Data Protection Act, an agency is exempt from its notification provisions where there is "good faith acquisition of personal information by an employee or agent of the agency" which is "not a breach of 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." 17 Marshall Code § 105(d) (2006).

This Court should reverse the erroneous holding by ruling first, that Baylor has stated a claim of intrusion upon seclusion, and second that ConDevel is not exempt from the notification provision of the Marshall Data Protection Act.

A court that reviews a grant of summary judgment should apply the same test utilized by the trial court, asking whether the evidence demonstrates that there is a genuine issue as to any material fact and if the moving party is entitled to judgment as a matter of law. Marshall R. Civ.

P., Rule 56(c). In summary judgment cases, a reviewing court conducts a *de novo* review of the evidence. *Johnson v. K-Mart Corp.*, 311 Ill. App. 3d 573, 577 (1st Dist. 2000).

**I. THE APPELLATE COURT ERRED IN RULING THAT BAYLOR DID NOT STATE A CLAIM FOR INTRUSION UPON SECLUSION BECAUSE MARSHALL SHOULD RECOGNIZE A CLAIM FOR INTRUSION UPON SECLUSION AND BECAUSE NESBIT COMMITTED AN INTRUSION UPON BAYLOR'S SECLUSION WHEN HE SURREPTITIOUSLY INSTALLED A KEYLOGGER ON BAYLOR'S COMPUTER AND ACCESSED HIS PERSONAL INFORMATION.**

The appellate court erred by ruling that the State of Marshall does not recognize a cause of action for intrusion upon seclusion and that even if it did, Baylor had not stated a claim for intrusion upon seclusion.

According to the Restatement, as adopted by Marshall courts, “[o]ne 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.” *Restatement (Second) of Torts* § 652B (1977).

This Court should reverse the appellate court by ruling that the State of Marshall does recognize a cause of action for intrusion upon seclusion, and that Baylor has met the requirements to state a claim for intrusion upon seclusion.

**A. The State of Marshall should recognize a cause of action for intrusion upon seclusion because doing so will provide a remedy for injured Marshall citizens and because doing so will provide incentive for people to avoid invading each other's privacy.**

The State of Marshall should recognize the invasion of privacy sub-tort intrusion upon seclusion. “A right of privacy in matters purely private is . . . derived from natural law.” *Pavesich v. New England Life Ins. Co.*, 102 Ga. 190, 194 (1905). “This interest in ‘privacy’ is a distinct aspect of human dignity and moral autonomy.” *Snakenberg v. Hartford Casualty Ins. Co., Inc.*, 299 S.C. 164, 169 (App. 1989). “Privacy is one of the sensitive and necessary human

values and undeniably there are circumstances under which it should enjoy the protection of law.” *Melvin v. Burling*, 141 Ill. App. 3d 786, 789 (3rd Dist. 1986).

The State of Marshall has already determined that its citizens have a right to privacy and that it is the judiciary’s duty to protect that right, because Marshall has already recognized the other forms of invasion of privacy. “[T]he vast majority of courts in other jurisdictions which have recognized other types of common law privacy claims” have also recognized a claim for intrusion upon seclusion. *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060, 1067 (Colo. App. Div. III 1998).

Writing on the tort of intrusion upon seclusion in 1964, New York University law professor Edward Bloustein stated:

[O]ur Western culture defines individuality as including the right to be free from certain types of intrusion. This measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by these concepts. A man whose home may be entered at the will of another, whose conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account.

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 973-74 (1964).

By recognizing this cause of action, this Court will provide a way for Marshall citizens to redress injuries to their privacy. Furthermore, recognizing this tort will prevent such injuries by deterring citizens from conduct which would infringe on another’s privacy.

A brief survey of cases involving intrusion upon seclusion demonstrates the types of injuries that can be both redressed and avoided by recognizing the tort in this state:

A tavern owner was in the habit of photographing women as they used the women’s restroom. *Yoeckel v. Samonig*, 272 Wis. 430, 431 (1956). The court refused to hold the tavern

owner liable because it would not recognize a cause of action for intrusion upon seclusion. *Id.* at 434. The injury to the women’s privacy was not recognized and no doubt the tavern owner continued taking pictures.

A television camera crew followed a team of paramedics into the home of a husband and wife, without permission, and filmed the husband as he lay dying from a heart attack. *Miller v. National Broad. Co.*, 187 Cal. App. 3d 1463, 1469 (2nd Dist. 1986). The court held that the wife stated a cause of action for intrusion upon seclusion. *Id.* at 1484. This holding not only recognized the wife’s right to privacy in her terrible hour, but it also sent a message regarding future conduct by overzealous camera-crews.

A telephone company tapped a woman’s phone line and listened to her private conversations. *LaCrone v. Ohio Bell Tel. Co.*, 114 Ohio App. 299, 299 (10th Dist. 1961). The court ruled that the woman had stated a cause of action for intrusion upon seclusion. *Id.* at 300-302. This holding recognized the damage caused to the woman’s privacy and encouraged phone companies to wield their power responsibly.

Each case is a clear demonstration of an instance where the plaintiff’s right to seclusion was violated. In none of these cases would a separate branch of privacy law have recognized the harm done to the plaintiff.

Furthermore, a changing world requires an adaptable legal system. As one justice noted, “In an earlier age, privacy was more easily maintained . . . . Not so today, when the social and physical barriers that formerly protected our privacy are dissolving in the face of technological” change. *Shulman v. Group W. Prod., Inc.*, 18 Cal. 4th 200, 243 (1998) (Kennard, J., concurring). In the case at bar, modern technology has been used to cause harm to the privacy of a Marshall citizen. Particularly because of the heightened potential for invasions of privacy by using

modern technology to intrude on the seclusion of another, this court should now recognize that this tort exists, and thus provide redress and protection for the privacy of Marshall citizens.

This Court should reverse the ruling of the appellate court by holding that the State of Marshall does recognize a cause of action for intrusion upon seclusion.

**B. The appellate court erred in ruling that Baylor did not state a claim for intrusion upon seclusion when Nesbit secretly installed a keylogger program on Baylor's computer which he kept in his personal office and protected with passwords and when Nesbit accessed Baylor's personal information which Nesbit did not have authority to access.**

This Court should rule that Nesbit's installation of the keylogger program and subsequent access of personal files constituted an intrusion upon Baylor's seclusion. According to the Restatement, as adopted by Marshall courts, "[o]ne 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." *Restatement (Second) of Torts* § 652B (1977). Appellate courts in Marshall have also required that the intrusion have caused "anguish and suffering." (R.7.) This Court should rule that the installation of the keylogger program and subsequent access of Baylor's personal files was an intentional, unauthorized intrusion, that the intrusion would have been highly offensive to a reasonable person and that Baylor had a zone of solitude in both his computer and his personal files. This Court should also rule that Marshall does not require a showing of anguish and suffering, or in the alternative, that the intrusion did cause anguish and suffering.

**1. The installation of the keylogger program and subsequent access of Baylor's file was an intentional, unauthorized intrusion because ConDevel ignored warnings about lax company security, because Nesbit installed the keylogger program in secret and because Nesbit was merely a low-level employee.**

Nesbit's actions constituted an intentional, unauthorized intrusion. In order to make a claim for intrusion upon seclusion, the plaintiff must show an "unauthorized intrusion or prying into the plaintiff's seclusion." *Johnson v. K Mart Corp.*, 311 Ill. App. 3d 573, 595 (1st Dist. 2000); *Mucklow v. John Marshall Law School*, 176 Ill. App. 3d 886, 894 (1st Dist. 1988). The intrusion must be intentional. *Toomer v. Garrett*, 155 N.C. App. 462, 479 (2002).

In *Mucklow*, the court held that there had been no intrusion upon seclusion where a professor accessed a student's "student record book." 176 Ill. App. 3d at 889. The court focused on the required element of an "unauthorized intrusion," reasoning that the professor was acting in the capacity of the student's "teacher, supervisor or within some other proper capacity with respect to plaintiff when he viewed plaintiff's file," and thus no unauthorized intrusion into the student's file occurred. *Id.* at 894.

The court in *Toomer* held that an employee had stated a cause of action for intrusion upon seclusion against his employer where the employer maintained a personnel file on the employee, where the employer kept the employee's file "separate from those of other state employees so as to facilitate access to them," and where the employer "allowed unauthorized persons to go through the records." 155 N.C. App. at 467. The court reasoned that such conduct was an intentional intrusion. *Id.* at 480.

Unlike the professor in *Mucklow*, who was acting in a "proper capacity with respect" to the student, in this case Nesbit was not acting in any proper capacity with respect to Baylor. While Baylor was a vice-president, Nesbit was merely a new sales associate. Nesbit only went into Baylor's office because he realized no one was looking and as soon as ConDevel found out what Nesbit had done, they fired him. These facts clearly indicate that Nesbit, although an employee of ConDevel, was not authorized to install a keylogger on Baylor's computer to access

his personnel file. Furthermore, Nesbit's actions were clearly done intentionally. Thus, unlike the court in *Mucklow* held that the professor had not intruded because he was authorized to view the student's file, the Court here should hold that Nesbit did intentionally intrude because he was not authorized to install the program on Baylor's computer to access his file.

But like the employer in *Toomer*, who made the employers records available to unauthorized persons, ConDevel here made unwarranted access to Baylor's files by ignoring complaints about the lack of company security and by not providing guidance to its employees on how to secure their computers. Thus, like the Court in *Toomer* held that the employer had made an intentional intrusion, the Court here should rule that ConDevel made an intentional intrusion.

Therefore, this court should reverse the appellate court by ruling that Nesbit's and ConDevel's actions constituted an intentional, unauthorized intrusion.

**2. The intrusion would be offensive or objectionable to a reasonable person because Nesbit recorded Baylor's computer keystrokes and because Baylor's file contained personal information.**

The intrusion would be offensive or objectionable to a reasonable person. To establish a claim for intrusion upon seclusion, courts generally require that a reasonable person would find the intrusion offensive or objectionable. *Toomer v. Garrett*, 155 N.C. App. 462, 480 (2002); *Lewis v. LeGrow*, 258 Mich. App. 175, 193 (2003).

The court in *Toomer* held that an employee had stated a cause of action for intrusion upon seclusion against his employer where the employer allowed unauthorized access to the employee's personnel file which contained the employee's home address, social security number, personnel history and other "confidential, personal and private information." 155 N.C. App. at 467. The court reasoned that because of the sensitive nature of the information involved,

examining a person's personnel file would make the intrusion "highly offensive to a reasonable person." *Id.* at 480.

Like the employee personnel file in *Toomer* contained the employee's home address, social security Number, personnel history and other personal information, Baylor's personnel file contained his contact information, social security Number, personnel history, and other personal information. Based on the sensitive and private nature of this information, the Court here should rule, as the court in *Toomer* did, that Nesbit's intrusion would be offensive or objectionable to a reasonable person.

Furthermore, a person's keystrokes can reveal their private thoughts. Any reasonable person would find it highly offensive to have their private thoughts recorded.

Therefore, this Court should reverse the appellate court because Nesbit's intrusion would be offensive or objectionable to a reasonable person.

**3. Baylor had a zone of solitude in his work computer because his computer was located in his personal office, because he protected at least some of his computer files with passwords and because ConDevel had no company policy about monitoring employee computer use.**

Baylor had a zone of solitude in his work computer. A person has a right to seclusion—or as the trial court put it, a "zone of solitude"—in a "place, conversation or data source" for which he has a reasonable expectation of privacy. *Sanders v. American Broadcasting Companies, Inc.*, 20 Cal. 4th 907, 915 (1999); *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060, 1068 (Colo. App. Div. III 1998). One "factor commonly considered in determining whether a person's expectation of privacy was reasonable" is whether the person had a "right to exclude others." *Greywolf v. Carrol*, 151 P.3d 1234, 1246 (Alaska 2007). An employee generally does not have a reasonable expectation of privacy where an employer advises its employees that it

will monitor computer use. *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002); *U.S. v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000); see also *Leventhal v. Knapek*, 266 F.3d 64, 74 (2nd Cir. 2001).

Because most of the cases which deal with employee computer privacy arise in the context of police searches and seizures, it is important to note that although it would be incorrect to “blindly import Fourth Amendment analysis into the analogous common-law tort of invasion of privacy,” *Lewis v. LeGrow*, 258 Mich. App. 175, 187 (2003), such an analysis asks, as does a tort claim for invasion of privacy, whether society would say that a person had a reasonable expectation of privacy in some thing or area. Thus, a case dealing with a Fourth Amendment expectation of privacy can be helpful in determining whether a reasonable expectation exists when the plaintiff claims a zone of solitude. *White v. White*, 344 N.J. Super 211, 223 (2001).

The court in *Muick* held that an employee had no reasonable expectation of privacy for his work laptop computer because his employer had specifically “announced that it could inspect the laptops that it furnished for its employees.” 280 F.3d at 743. The court reasoned that although there is no *per se* rule against a right to privacy in equipment furnished by an employer to its employee, this announcement destroyed any reasonable expectation of privacy that the employee may have had. *Id.*

In *Leventhal*, the employer had an anti-theft policy which prohibited use of its computers for “personal business.” 266 F.3d at 74. However, the policy failed to define exactly what was meant by “personal business.” *Id.* at 74. Furthermore, the employee in question kept his computer in a private office and had “exclusive use” of the computer. *Id.* at 73. He also protected some of his computer files with a password. *Id.* at 76. Despite some occasional access to the computer by the employer, there was no “extensive” policy of computer monitoring or

access. *Id.* at 74. In holding that the employee did have a reasonable expectation of privacy, the court reasoned that there was nothing that would have put the employee “on notice that he should have no expectation of privacy in the contents of his office computer.” *Id.*

In *Greywolf*, the court held that a hospital patient did not have a claim for intrusion upon seclusion when she was arrested in her room in the mental health unit. 151 P. 3d at 1236. The court reasoned that because she did “show that she had the right to exclude others from her room,” she could not have had a reasonable expectation of privacy. *Id.* at 1246.

Unlike *Muick*, where the employers each had a policy of monitoring computer use, neither the employer in *Leventhal* nor ConDevel had a policy of monitoring computer use. However, both Baylor and the employee in *Leventhal* kept their computers in their personal offices and protected at least some of their files with passwords. These facts were enough to maintain a reasonable expectation of privacy in spite of the *Leventhal* employer’s policy that no company equipment was to be used for personal business, and they should also be enough to maintain a reasonable expectation of privacy in this case despite the trial court’s statement that Baylor’s computer “was not to be used for private matters.” Thus, whereas the courts in *Muick* held that the expectation of privacy for the employees in those cases was destroyed by the employer policy of computer monitoring, this Court should hold, as the court in *Leventhal* did, that since ConDevel did not have any such policy, Baylor maintained a reasonable expectation of privacy in his work computer.

Furthermore, unlike the mental health patient in *Greywolf*, who could not exclude others from her room, Baylor had the right to exclude others from his computer. Although the record does not reflect whether Baylor had protected general access to his computer with a password, his right to exclude others from his computer is still established by the facts that his computer

was in his personal office and that he had passwords protecting at least some of his files. And even though Baylor left his computer on and the door to his office open, Nesbit still recognized that he was excluded from Baylor's computer because he only entered the office and used the computer after making sure that he was not being watched. Employees generally expect that they have the right to exclude other co-workers from using their computer, and this is especially true when taken in the context that Baylor was a vice-president of ConDevel and Nesbit was a low-level subordinate. Therefore, unlike the court in *Greywolf* held that there was no reasonable expectation of privacy in the patient's hospital room because she could not exclude others, the Court here should find that Baylor had a reasonable expectation of privacy for his computer because he could exclude others.

Finally, even though ConDevel had a policy which stated that "employees are responsible for safeguarding all equipment and software provided by the company," in the absence of guidance as to what were appropriate safeguard measures, Baylor's enabling of passwords was sufficient to maintain a reasonable expectation of privacy.

Therefore, because Baylor had a reasonable expectation of privacy in his computer, this Court should reverse the appellate court by ruling that Baylor had a zone of solitude in his work computer.

- 4. Baylor had a zone of solitude as to the disclosure of his personal information to an unauthorized person because the information was not available to unauthorized employees such as Nesbit, because the information was only obtainable by surreptitiously installing a keylogger program on Baylor's work computer and because of the sensitive nature of the information.**

Baylor had a zone of solitude as to the disclosure of his personal information to an unauthorized person. A person has a right to seclusion—or as the trial court put it, a "zone of

solitude”—in a “place, conversation or data source” for which he has a reasonable expectation of privacy. *Sanders v. American Broadcasting Companies, Inc.*, 20 Cal. 4th 907, 915 (Cal. 1999); *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060, 1068 (Colo. App. Div. III 1998). Whether the expectation of privacy is reasonable can be analyzed by examining the “identity of the...intruder and the nature of the intrusion.” *Sanders*, 20 Cal. 4th at 918. Furthermore, “the seclusion referred to need not be absolute,” but rather can be established by degrees. *Id.* at 916. Specifically, an employer who allows unauthorized access to an employee’s file containing private information can be liable for an intrusion upon the employee’s seclusion. *Toomer v. Garrett*, 155 N.C. App. 462, 480 (N.C. App. 2002).

The court in *Toomer* held that an employee had stated a cause of action for intrusion upon seclusion against his employer where the employer maintained a personnel file on the employee which contained the employee’s home address, social security number, personnel history and other “confidential, personal and private information.” *Id.* at 467. Because the employee could not have stated a claim for intrusion upon the seclusion of his information if he had not had a reasonable expectation of privacy in that information, the court’s holding implicitly recognized that there is a reasonable expectation of privacy for personal information contained in an employee personnel file.

In *Sanders*, the court held that an employee in a psychic hotline company could state a claim for intrusion upon seclusion against an investigative reporter, working at the psychic company undercover, who used a small “hat-cam” to secretly record conversations with the employee, even though conversations in the employees’ cubicles could be easily overheard by employees sitting in surrounding cubicles. 20 Cal. 4th at 912-13. The court focused on the nature of the intrusion (the secretive use of the hat-cam) and the identity of the intruder (an

undercover reporter) in reasoning that although the employee may not have had an absolute expectation of privacy for these conversations, he still had a reasonable expectation that the conversations would not be secretly recorded by an undercover reporter. *Id.* at 923.

In *Doe*, the court held that the plaintiff had stated a claim for intrusion upon seclusion where a student in a medical training program who gave consent for his school to test his blood for rubella sued the school when the school performed an additional test which indicated that the student had the human immunodeficiency virus (HIV). 972 P.2d at 1064. In holding that a person has a reasonable expectation of privacy in his blood and the information that can be obtained from it, the court reasoned that the student's privacy interest did not end once his blood had been removed from his body because private medical information could be obtained by conducting further tests on the blood. *Id.* at 1068.

Similar to *Toomer*, where the employer maintained a personnel file of the employee's personal information, including his home address and social security number, ConDevel maintained an electronic, human resources personnel file of Baylor's personal information, including "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." The trial court thought that by giving personal information to ConDevel, Baylor could not have any reasonable expectation of privacy in that information. However, the trial court's blanket all-or-nothing rule would completely strip the right of employees to expect their employers to handle their private information responsibly. Because of the sensitive nature of this information, and the potential for misuse of or embarrassment from this information, Baylor and other ConDevel employees had a right to expect that ConDevel would keep the information private. ConDevel itself must have

recognized this right because it limited access to the information, i.e. Baylor only had access to the information by virtue of his position with the company. Thus, like the court in *Toomer* implicitly held that the employee had a reasonable expectation of privacy for information contained in his personnel file, the Court here should hold that Baylor had a reasonable expectation of privacy in the information contained in his personnel file.

Assuming that Baylor no longer had an *absolute* expectation of privacy in the information once he gave it to ConDevel, this case is like *Sanders*, where the plaintiff did not have an absolute expectation of privacy but maintained one of degrees. Applying the two part test from *Sanders*, first we can look at the identity of the intruder. Nesbit was a subordinate employee, who was not authorized to access the human resources information contained on Baylor's computer. Looking next to the nature of the intrusion, Nesbit surreptitiously installed a keylogger program on Baylor's computer, recorded Baylor's logins and passwords and used them to access Baylor's personal information. Under these circumstances, and due to the potential for misuse of or embarrassment from the personal information, Baylor could have reasonably expected that the information which he provided to ConDevel would have remained private. Therefore, like the court in *Sanders* held that although the employee did not have an absolute expectation of privacy, he did have a reasonable expectation that his conversations would not be secretly recorded by an undercover reporter, the Court here should rule that although Baylor did not have an absolute expectation of privacy, he did have a reasonable expectation of privacy that an unauthorized ConDevel employee would not secretly install a keylogger program to steal his personal information.

Finally, this case can be analogized to *Doe*, where the court held that although the plaintiff had given his blood to the defendant and consented to a test for rubella, the plaintiff

retained a reasonable expectation of privacy that the defendant would not go beyond that consent by testing the blood for HIV. Baylor voluntarily gave certain personal information to ConDevel, but when an employee provides private information to an employer, there is an understanding that the employer is only to use the information for purposes related to employment. If workers thought that by giving personal information to their employers they would be consenting to *any* employee of the company accessing it, then they would not be willing to provide it. Thus, Baylor's consent for ConDevel to use his private information for purposes related to employment cannot be seen as giving ConDevel *carte blanche* to do with the information as it pleased. Nesbit's surreptitious acquisition of Baylor's private information cannot be seen as having been consented to by Baylor. Therefore, just as the court in *Doe* ruled that the plaintiff retained a reasonable expectation of privacy in not having his blood tested for HIV despite having given the blood to the defendant, this Court should rule that Baylor retained a reasonable expectation of privacy in his information not being accessed by an unauthorized employee, despite having provided that information to ConDevel.

Although a few courts have held that social security numbers are not considered private information for purposes of this tort, see *Busse v. Motorola, Inc.*, 351 Ill. App. 3d 67, 73 (1 Dist. 2004), such a rule is clearly not consistent with protecting a person's right to privacy. A social security number can be used to glean private information about a person or can be used for identity theft. The judiciary should interpret laws in a way that is consistent with this strong interest in keeping social security numbers confidential.

Furthermore, Nesbit not only accessed Baylor's social security number and driver's license information, but also his employment history including evaluations and salary information (both of which a reasonable person would want his employer to keep from other

employees, especially subordinates), club membership information (which would let Nesbit know about ways that Baylor spends his private time) and other “personal information.” Thus, the Court here should rule that based on the extensive amount of personal information contained in the file, Baylor had a reasonable expectation of privacy in his personal information.

Therefore, because Baylor had a reasonable expectation of privacy in the personal information contained in his human resources file, this Court should reverse the appellate court by ruling that he had a zone of solitude in that information.

**5. The State of Marshall should decline to adopt a formulation of intrusion upon seclusion which would require a plaintiff to show that the intrusion caused anguish and suffering because such a formulation will not adequately protect the privacy of the citizens of Marshall.**

The State of Marshall should decline to adopt a formulation of intrusion upon seclusion which would require a plaintiff to show that the intrusion caused anguish and suffering. Courts have taken different approaches as to whether a plaintiff is required to prove damages for an intrusion upon seclusion claim.

One approach is to require a showing of some form of mental suffering, humiliation, or mental anguish. *Daily Times Democrat v. Graham*, 276 Ala. 380, 382 (1964); *Busse v. Motorola, Inc.*, 351 Ill. App. 3d 67, 71 (1 Dist. 2004).

This approach is clearly intended to prevent frivolous lawsuits from clogging the courts. The apparent perception is that by allowing a claim for intrusion upon seclusion, there is a risk of litigation from citizens who have suffered some minor inconvenience.

However, the approach taken by many other courts is that “the damage consists of the unwanted exposure resulting from the intrusion. Thus, if the plaintiff proves the . . . elements needed to establish his cause of action, the fact of damage is established as a matter of law.”

*Snakenberg v. Hartford Casualty Ins. Co., Inc.*, 299 S.C. 164, 172 (App. 1989). Some jurisdictions expressly allow recovery for nominal damages. *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1066 (Colo. App. 1998); *Sabrina W. v. Willman*, 4 Neb. App. 149, 159 (1995).

Showcasing the contrast between these two approaches, Dean Prosser believed that “the gist of the wrong is clearly the intentional infliction of mental distress,” William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 423 (1960), whereas Prof. Bloustein contended “that the gist of the wrong in the intrusion cases is not the intentional infliction of mental distress but rather a blow to human dignity, an assault on human personality.” Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 974 (1964).

Of these two approaches, the “damages as a matter of law” rule will better protect the privacy interests of the citizens of Marshall. The right to privacy protects that sphere surrounding a person in which they have a “dignitary interest,” a privilege to be free from unwanted intrusions. *Snakenberg*, 299 S.C. at 169 (App. 1989). Penetration of that sphere is injury in itself, and as such should be subject to redress as a matter of law. Requiring a showing of “anguish and suffering” denies that penetration of that sphere is a violation of a right, effectually denying that there is a right to privacy.

Furthermore, the Restatement suggests a formulation of the tort not requiring an element of “anguish and suffering.” Although the appellate court stated that Marshall courts have followed the Restatement formulation, the Restatement only requires 1) an intentional intrusion, 2) upon the solitude of another, 3) if it would be highly offensive to a reasonable person. *Restatement (Second) of Torts* § 652B (1977). This formulation makes no reference to “anguish and suffering.”

In addition, the section of the Restatement dealing with damages that are available as a remedy for invasion of privacy also suggests that no “anguish and suffering” need be established. *Restatement (Second) of Torts* § 652H makes damages available to compensate 1) harm suffered to the plaintiff’s interest in his privacy, 2) mental distress suffered and 3) special damages. This section clearly indicates that “mental distress” is only one form of injury that may result from the intrusion upon seclusion. The first category of damages clearly makes a remedy available when the only injury suffered is to the plaintiff’s privacy.

Thus, those jurisdictions that have claimed to adopt the Restatement version of the tort, but which have also required a showing of “anguish and suffering,” have gone beyond the scope of the Restatement. Those jurisdictions have also implicitly rejected a person’s right to privacy, thus making it more difficult for their citizens to obtain a remedy in the courts and failing to efficiently deter further invasion of privacy claims.

Therefore, the Court should reverse the appellate court by ruling that the State of Marshall does not require a plaintiff to show “anguish and suffering” in order to recover for intrusion upon seclusion.

6. **Assuming arguendo that Marshall does require an element of anguish and suffering, Nesbit’s intrusion caused Baylor anguish and suffering because he was deeply embarrassed when he was informed in front of his friends that his membership had been revoked at Shady Links golf course, because the manager of Les Deux Pommes shouted at him, “we do not want drunks and troublemakers in our restaurant” and because a reasonable person would have suffered anxiety knowing that someone had recorded their computer’s keystrokes and accessed their personnel file.**

Nesbit’s intrusion caused Baylor anguish and suffering. The formulation of intrusion upon seclusion that requires “anguish and suffering” has its roots in an American Law Reports annotation published in 1942, where the author proposed a definition for invasion of privacy

requiring that the invasion “cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.” R.T. Kimbrough, *Right of Privacy*, 138 A.L.R. 22, 25 (1942).

This exact definition was eventually adopted by several jurisdictions, which now require that an intrusion upon seclusion cause “mental suffering, shame, or humiliation.” *Smith v. Doss*, 251 Ala. 250, 253 (1948); *Anderson v. Mergenhagen*, 283 Ga. App. 546, 549 (1966); *Aronson v. Sprint Spectrum, L.P.*, 767 A.2d 564, 568 (Pa. Super. 2001). Other courts have adopted a similar rule, such as a requirement that a plaintiff have “suffered anxiety, embarrassment, or some other form of mental anguish.” *Monroe v. Darr*, 221 Kan. 281, 286 (1977). Although these courts allow “mental suffering” or “mental anguish” to establish the tort, similar to the appellate court’s formulation, these courts also make room for “humiliation,” “anxiety” or “embarrassment.”

The rule that is most similar to the appellate court’s formulation is that used in Illinois. Illinois courts have required that “the intrusion causes anguish and suffering,” as first stated in *Melvin v. Burling*, 141 Ill. App. 3d 786, 789 (3rd Dist. 1986).

Although the *Melvin* court does not make clear its authority for adopting this requirement, it seems probable that the court was influenced by the courts adopting the American Law Report annotation. This suggests that humiliation, anxiety or embarrassment is sufficient to qualify as forms of anguish and suffering.

Even Dean Prosser, who believed that “the gist of [intrusion upon seclusion] is clearly the intentional infliction of mental distress,” went on to say that the indication is that an invasion of privacy claim does not require “extreme outrage” or “serious mental harm.” William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 423 (1960).

In *Melvin*, the plaintiffs had received “numerous items through the mail” which they had not ordered and later received “demands for payment.” 141 Ill. App. 3d at 786. They “alleged

that these items had in fact been intentionally ordered by the defendant who had used the plaintiff's names without authority when ordering the items." *Id.* In holding that the plaintiffs had stated a claim for intrusion upon seclusion, the court reasoned that "[t]he facts also support the elements of anguish and suffering including as they do the difficulties of returning unauthorized merchandise and dealing with irate creditors." *Id.* at 789-790.

The *Melvin* reasoning can be applied to the case at bar. In finding anguish and suffering, the *Melvin* court cited the fact that the plaintiffs would have difficulties returning the merchandise and dealing with irate creditors. These problems were not actual intrusions by the defendants, but consequences of the intrusion. In this case, Nesbit's intentional acts of intrusion were installing the keylogger and accessing Baylor's private information. The Court here can look to the consequences of those actions, just as the court did in *Melvin*, to determine whether Baylor suffered anguish and suffering. Given the rules cited from other jurisdictions that suggest humiliation, embarrassment or anxiety can satisfy the requirement for anguish and suffering, a reasonable person would be deeply humiliated by a restaurant manager shouting at him, "We do not want drunks and trouble makers in our restaurant," and the record states that Baylor was "deeply embarrassed" following his ban from the golf club. It also seems apparent that Baylor would have suffered some level of anxiety following these incidents and in his subsequent discovery that a person was impersonating him in such an outrageous manner.

Even if the Court elects to focus on the anguish and suffering that Baylor would have suffered if Nesbit had only installed the keylogger program and accessed Baylor's files, it still follows that a reasonable person would be embarrassed and suffer some anxiety from knowing that their personal information had been accessed, as well as knowing that a person had been

keeping track of their computer keystrokes, since a person's keystrokes can reflect the private thoughts of the individual typing.

Therefore, because Baylor has suffered humiliation, embarrassment and anxiety, this Court should reverse the appellate court by ruling that the intrusion caused "anguish and suffering."

**II. THE APPELLATE COURT ERRED IN EXCUSING CONDEVEL FROM ITS AFFIRMATIVE DUTY TO NOTIFY UNDER THE NOTIFICATION PROVISION OF THE DATA PROTECTION ACT SINCE NESBIT USED THE PERSONAL INFORMATION HE STOLE TO IMPERSONATE AN EXECUTIVE AND GAIN ACCESS TO EXCLUSIVE CLUBS, AND SINCE HE FURTHER USED THE STOLEN CONFIDENTIAL INFORMATION IN DISOBEDIENCE OF COMPANY INSTRUCTIONS TO PURSUE HIS DESIRE TO ENJOY EXECUTIVE BENEFITS.**

The Appellate Court erroneously held that ConDevel was exempt from the notification provisions of the Data Protection Act, first, when it held that the ConDevel had discretion whether to notify or not and second, when it held that ConDevel qualified for the "good faith acquisition" exemption in § 105(d) of the statute.

The Marshall Data Protection Act, requires any agency that owns or licenses computerized data that includes personal information to disclose any "breach of the security of the system," following discovery or notification of the breach, to any resident of Marshall whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. 17 Marshall Code § 105. To be exempt from this affirmative duty to disclose any breach of the security system, the agency who owns or licenses the computerized data must prove that the breach qualifies as a good faith acquisition in § 105(d) of the Marshall Code Data Protection Act, or in the alternative created by the Appellate Court, prove that notification is not necessary based on the company's structure and policies.

This Court should reverse the Appellate Court's holding that ConDevel was exempt from

the provisions of the Data Protection Act. ConDevel does not qualify for either of the exceptions since the personal information stolen was maintained confidentially by ConDevel for the purpose of safeguarding the system and since deceitful acquisition of it by Nesbit was for his personal acquisition of exclusive VIP benefits that he was not entitled to enjoy.

A. **ConDevel is not exempt from the Marshall Code Data Protection Act on the basis of discretion to notify since Nesbit's use of the confidential information was not within compliance of ConDevel's corporate scopes and purposes, and to allow ConDevel such discretion to notify of security breaches would starkly contrast the purpose intended by the Marshall Data Protection Act and others like it.**

The Appellate Court erred in granting ConDevel discretion and, as a result, exempting ConDevel from the affirmative duty to notify of the breach of its security system. Courts have granted discretion to agencies and companies in lieu of statutory compliance where the agencies promulgate their substitute procedures in accordance with rulemaking provisions of the statute, provide statements of their reasons for exercising the discretion to do so, and/or prove that the substitute procedures promote the underlying purposes of the statute. *FBI v. Doe*, 936 F.2d 1346, 1357 (App. D.C. 1991); *Bassiouni v. FBI*, 436 F.3d 712, 738 (7th Cir. 2006); *Sussman v. U.S.*, 2006 U.S. Dist. LEXIS \* 39 (E.D.N.Y. Sept. 30, 2007).

In *FBI v. Doe*, the court remanded for further determination as to whether an exemption to a privacy statute should apply. 936 F.2d at 1361. In seeking to be exempt from particular record correction requirements in the statute, the plaintiff provided explanations, such as the justification that adhering to the statutory Act would impose a large burden on the plaintiff to retrograde all of its investigations to resolve questions of accuracies. *Id.* at 1359. The plaintiff further offered proof tending to show that subjecting particular records to the provisions of the Act was not as clearly necessary to effectuate the purposes behind the Act. *Id.* Given plaintiff's proof and reasons, the court concluded an issue of genuine fact still remained and thus

remanded the case for further decisions on the matter. *Id.* at 1361.

This Court should reverse the Appellate Court's erroneous grant of discretion since ConDevel did not provide any reasons or proof, such as the defendant in *FBI*, that its alternative processes were in furtherance of the Act. The only reason provided by ConDevel is that the disclosure was within its scopes and purposes, which is a reason not substantially supported by the facts. Furthermore, granting ConDevel discretion to notify starkly contrasts with the underlying purpose and policy of the Marshall Data Protection Act.

- 1. Acquisition of the personal information, subject to the unauthorized disclosure, was not used in compliance with ConDevel's scopes and purposes since it was used by Nesbit to gain access to ConDevel's confidential VIP benefit system, to fraudulently use it to imposter an executive, to gain access to exclusive clubs and thereafter partake in a fight with a prominent member of the club.**

The Appellate Court erroneously held that the information obtained by Nesbit was within, or in compliance with, ConDevel's scopes and purposes and therefore erred in granting ConDevel discretion to notify its employees. Whether the actions of an employee are within the scopes and purposes of his employer is determined based on the corporate charter, the facts at hand and the inferences that can be drawn from both. *Relief Fire Insur. Co. of N.Y. v. Shaw*, 94 U.S. 574, 576 (1877); *Luce v. First Equip. Leasing Corp.*, 960 F.2d 1277, 1278 (5th Cir. 1992); *Roth v. J.N. Roth Corp.*, 363 Mo. 767, 777 (Mo. 1952). An employee is not acting within, or in compliance with, the scopes and purposes of his company if his actions are inconsistent with the scopes and purposes as defined and reasonably inferred from the company and its ordinary business, if he does not act in furtherance of said scopes and purposes, or if his actions cannot be fairly said to have been authorized by the company. *Relief Fire Insur. Co. of N.Y.*, 94 U.S. at 576; *Luce*, 960 F.2d at 1278; *Roth*, 363 Mo. at 777.

In *Roth*, the court reversed a judgment against the defendant, a corporation whose employee committed the acts complained about in the lawsuit. *Roth*, 363 Mo. at 779. The defendant was a corporation in the business of selling hospital and hotel furniture and supplies. *Id.* at 770. The defendant's employee was driving the plaintiff in defendant's car when he was involved in an accident and the plaintiff was injured. *Id.* The plaintiff asserted that because the employee was driving the corporate car, he was acting within the scope and purposes of the defendant. *Id.* at 772. The court disagreed and concluded that the scope and purpose of a company are limited to its ordinary course of business, and the usual or ordinary course of business cannot extend beyond the scope of the corporation's business nor include acts which are beyond the corporate objects and purposes. *Id.* at 775. In reversing the lower court's holding for the plaintiff, the court held that in some circumstances operating an automobile may fall within the scopes and purposes of a business, driving a passenger to lunch does not. *Id.* at 778. The court further held that the scopes and purposes of the defendant's corporation were to sell hospital and hotel furniture and supplies, not to transport guests. *Id.*

Similarly to *Roth*, Nesbit was not acting within compliance of ConDevel's scopes and purposes and thus ConDevel is not entitled to notify per its own discretion. Although, the record does not explicitly state ConDevel's scopes and purposes, it is clearly stated that ConDevel is a real estate construction company. While a subset purpose might be termed "safeguarding all equipment and software" based on the Computer Usage Policy, this is comparable to terming transportation as a subset purpose of the defendant corporation in *Roth*. Although safeguarding the equipment and software may be a task completed by ConDevel and its employees, doing so by testing the system secretly, invasively and from a private home computer is not.

Furthermore, ConDevel's assertion that safeguarding and testing the security system is its

purpose is weak since the Computer Usage Policy's were not accompanied by any guidance for employees as to what constituted safeguard measures. Additionally, due to ConDevel's financial hardships its main scope and purpose is focused on "appeas[ing] its shareholders" while keeping the VIP Program intact. Nesbit's actions contradict both of these purposes. Even if ConDevel's purpose was to "test the security system," Nesbit's use of the personal information to fraudulently obtain executive status as "Mr. Baylor" and frequent upscale clubs is not in furtherance of this purpose. Nesbit's actions were not within compliance of ConDevel's scopes and purposes and thus ConDevel should not be granted discretion to notify.

**2. Granting discretion to notify of security breaches to ConDevel would starkly contrast with the underlying policies and purposes of Data Protection Acts since ConDevel did not inform anyone about the incident, did not offer any investigation details, and did not provide proof of any curative efforts such as those promoted by the Marshall Data Protection Act.**

The Appellate Court erred in granting ConDevel discretion to notify of the breach of security in the system since doing so starkly contrasts with the policy and underlying purposes of the Marshall Data Protection Act. While the purposes of the Marshall Data Protection Act are not explicitly stated in the facts, the protection of consumers and security of personal information can be inferred as purposes from various similar data protection acts as well as the language of the Marshall statute itself.

First, the common underlying theme of data protection acts is to protect consumers and their personal information by way of prompt notification. Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security*, 43 Hous. L. Rev. 1597, 1599 (2007). Notification of any breach enables consumers to take curative actions. *Id.* With network breaches and identity theft on the rise, these notification statutes are a necessary means to prevent and remedy any resulting harm. *Id.* at 1609. One of

the data protection acts comparable to Marshall's is the California Data Protection Act. The California Act forces companies to "fess up to breaches" and "warn customers when a hacker" has obtained personal information. Matthew Bender, *1-2 Law of the Internet* § 2.03 (LexisNexis 2005). At least thirty-five states have similar statutes and all of them require some form of notification. Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security*, 43 Hous. L. Rev. 1597, 1605 (2007). (citing Nat'l Conference of State Legislatures, 2005 Breach of Information Legislation, <http://www.ncsl.org/programs/lis/cip/priv/breach05.htm> (last visited Jan. 10, 2007) (listing security breach disclosure legislation by state)). Therefore notification is the main underlying component of data notification provisions in furtherance of their purposes.

Secondly, the importance of the notification scheme is evident in the language of the Marshall Data Protection Act. Although some provisions of the statute allow for alternative forms of notification, such as written, electronic or substitute notice, each provision of the statute incorporates some form of notification. 17 Marshall Code §105(e). Furthermore, §105(f) of the Act provides leniency for data collectors that maintain their own notification procedures; however, it still requires the data collector to "notif[y] subject persons." *Id.* at §105(f). Therefore, the direct statutory interpretation of the language of the Act also supports the conclusion that notification is the main component in furtherance of the data protection purposes.

In light of the national policy, similar statutes, and language interpretation of the Marshall Data Protection Act, and the importance of notification, granting ConDevel discretion to notify is in stark contrast to the data protection movement and policy. In furtherance of ConDevel's already inept data protection standards for safeguarding equipment and personal information, ConDevel failed to take any notification action after it became aware of the breach

of the system. As the facts expressly state, ConDevel did “not inform any one about the incident,” even though its management concluded that “no one” knew the breach “ever happened.” Because ConDevel has placed its reputation over the important protection of consumers recognized by data protection legislation and current policies, it cannot be trusted to maintain its own notification procedures and should not have been granted discretion to do so.

**B. ConDevel is not exempt from the Marshall Code Data Protection Act on the basis of the § 105(d) “good faith acquisition” exception since ConDevel’s former employee surreptitiously installed the keylogger after his supervisor consistently told him to “mind his own business and leave technological issues to the technology support department” and since after the breach ConDevel did not inform any one and did not offer any investigation details to remedy effects of the breach.**

The acquisition of the personal information by ConDevel’s former employee does not meet the requirements for the good faith acquisition exemption provided for in § 105(d) of the Marshall Code Data Protection Act. Under the Act, good faith acquisition of personal information by an employee or agent of the agency excuses the agency from the affirmative duty to notify provided that (1) the personal information is used for the purpose designated by the agency, and/or (2) it is not subject to further unauthorized disclosure.

First, the secretive filtering of personal information by ConDevel’s employee to his home computer and his subsequent use of the stolen information for his own social entertainment is not a purpose designated by the agency. Second, ConDevel’s failure to fulfill its duty and investigate the breach or take further remedial actions, in light of the modern prevalence of identity theft, suggest a strong possibility that there was further unauthorized disclosure. Thus the breach of the security of the system was not a good faith acquisition and the Appellate Court erred in exempting ConDevel from its affirmative duty to notify under § 105 of the Marshall Code Data Protection Act.

**1. The secretive installation of a keylogger and subsequent theft of personal VIP information filtered to the personal computer of ConDevel's former employee despite continuous supervisory directions to leave the security issue alone does not constitute "good faith acquisition" under § 105(d) of the Marshall Code Data Protection Act.**

ConDevel's former employee, Nesbit, did not obtain Baylor's confidential personal information in good faith under § 105(d) of the Marshall Data Protection Act. In determining the meaning of good faith as it applies to the specific statutory provisions, courts have held that the plain meaning of a statute should be ascertained from the statute's language, object and policy and its specific language should be further examined. *Frees, Inc. v. McMillian*, 2007 U.S. Dist. LEXIS 57211 \*6 (W.D. La. August 6, 2007); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1123 (W.D. Wa. 2000). In examining "good faith," its plain meaning definition is a state of mind consisting in (1) honesty in belief or purpose, (2) faithfulness to one's duty or obligation, (3) observance of reasonable commercial standards of fair dealing in a given trade or business, or (4) absence of intent to defraud or to seek unconscionable advantage. *Black's Law Dictionary* 307 (Bryan A. Garner ed., 2d pocket ed., West 2001). In furtherance of this definitional concept, case law has held that to assert good faith a party has the burden of presenting evidence proving that they acted with good faith in the ordinary course of business and that their actions were not subject to unauthorized practices. *Trustmark Life Insur. Co. v. The U. of Chicago Hosp.*, 207 F.3d 876, 883 (7th Cir. 2000); *State of Ohio v. Grays*, 2001 Ohio App. LEXIS 5397 \*12 (8th Dist. Dec. 6, 2001).

In *Grays*, the court remanded the case to allow the fact-finder to resolve the issues of whether the parties met their respective burdens of proof. *Grays*, 2001 Ohio App. LEXIS 5397 \*13. The defendant in *Grays* owned a truck towing company which operated in conjunction with an automobile salvage yard. *Id.* at \*1. The indictment of the defendant resulted after an Auto

Theft Unit of the Police Department conducted a routine inspection and uncovered five automobiles missing their original vehicle identification numbers. *Id.* at \*3. The defendant argued that the statute at issue did not apply since his acquisition of the stolen vehicles was not done with his knowledge or purpose and such occurrence is common in the ordinary course of the car salvaging business. *Id.* Thus because the defendant acquired stolen vehicles without knowing or intending to, he was granted an exemption from the statute on the basis of its “good faith acquisition” provision. *Id.* at \* 5. The court concluded that the statute intends a reasonable result and that the reasonable result at hand required the court to remand the case for consideration by the fact-finder. *Id.* at \*9.

Unlike in *Grays*, the breach of security acquisition by ConDevel’s employee was not made with good faith and thus should not allow ConDevel the statutory exemption at issue. As in *Gray*, the breach of security was discovered as a result of a management check of the computer system. However, unlike in *Grays*, Nesbit knew of the stolen material prior to discovery. Further, it can be assumed that, although Nesbit’s job description in the ordinary course of business is not explicitly stated, Nesbit’s secret installation of a keylogger in a co-worker’s computer to filter confidential information to his home computer was not within the scope and manner of that job description. Though Nesbit’s initial intent, which he claimed to be to “help the company by exposing vulnerabilities,” may have seemed faithful, an element of “good faith” as described by *Blacks Dictionary*, it was not authorized by the company and any good faith that may have existed quickly faded when Nesbit became “immediately fascinated by the opportunities” and used the information for self-serving purposes. Based on Nesbit’s selfish purposes, unauthorized actions, and lack of honesty, this court should conclude that Nesbit did not acquire the personal information in good faith and thus ConDevel should not be entitled to

exemption from the statute.

2. **The breach of security of the system by ConDevel's former employee does not satisfy the second requirement necessary to constitute an exemption under 105(d) since Nesbit's filtering of human resource database files through installation of a hidden keylogger resulted in unauthorized acquisition of personal information that, by enabling the Nesbit to create a VIP alias and frequent upscale VIP venues, was used for purposes not designated by the agency.**

ConDevel's former employee, Nesbit, did not use the information obtained by his secret keylogger downloads for purposes designated by ConDevel. A designated purpose exists where the agency or employer directs, authorizes, or intends for an employee or agent to act or perform in a specific manner or capacity or when the activity is part of the employee's business activities. *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2005) (employee's authorization to access laptop terminated when he decided to quit in violation of his contract); *Butera & Andrews v. IBM, Corp.*, 2006 U.S. Dist. LEXIS 75318 \*3 (D.C. Oct. 18, 2006) (allowing an inference that attacks by a computer hacker traced to IBM were conducted by a rogue employee acting outside the scope of his or her employment and without authorization); *Calyon v. Mizuho Securities USA, Inc.*, 2007 U.S. Dist. LEXIS 66051 \*3 (S.D.N.Y. July 24, 2007); *Dudick v. Vaccarro*, 2007 U.S. Dist. LEXIS 45953 \*3 (M.D. Pa. June 25, 2007). In determining whether actions constitute "purposes designated" by an agency or employer, the court should consider whether the employee knew the action was in contravention of the wishes and interests of the employer and whether employee knew that he or she did not have authorization to access or perform the specified task. *Calyon*, 2007 U.S. Dist. LEXIS 66051 \* 3. Further, consideration as to what the initial employment agreement stated as the employee's job duties should be included in the analysis. *Dudick*, 2007 U.S. Dist. LEXIS 66051 \*5.

In *Dudick*, the court denied a dismissal order requested by the defendant in a federal claim

for violation of the Computer Fraud and Abuse Act (CFAA). *Id.* at \*19. Upon being hired for the plaintiff, the defendant was “entrusted with the duty” of maintaining contact with customers concerning bids, proposals, and orders which included access to confidential information. *Id.* Without the plaintiff’s knowledge, the defendant used the computers to divert the company’s confidential information, including personal client information, to his newly formed business venture to increase its financial success. *Id.* Upon realizing the loss in sales revenue and thereafter investigating the situation, the plaintiff filed an action claiming violation of the CFAA. *Id.* at \*5. In denying the defendant’s motion to dismiss, the court held that because the defendant accessed the information to divert it to his other venture, and because he did so in excess of the authorization given upon employment and without the plaintiff’s knowledge his access was unauthorized. *Id.* at 20.

In *Calyon*, the court also denied the defendants’ motion to dismiss on a CFAA action. *Calyon*, 2007 U.S. Dist. LEXIS 66051 \*5. Ten of the defendants in *Calyon* were employees of the plaintiff who resigned after signing employment agreements the night before. *Id.* at \* 2. Prior to resignation, the defendants copied information from the plaintiff’s computer and emailed it to their personal email accounts, both in violation of the plaintiff’s email provisions as defined in the employment agreements. *Id.* In analyzing the CFAA cause of action, the court held that the plain language of the statute should be the basis for the determination, and in looking at the plain meaning of CFAA, the court held that “without access” and “exceeds authorized access” would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer. *Id.* at 4. Based on this statutory interpretation it was concluded that the plaintiff’s employees did not have authorization to access the computer system and taking documents from it was not within the

purposes designated by the employment agreement. *Id.* In accordance, the court denied the defendants' motion to dismiss. *Id.* at \*5.

Here, the actions of ConDevel's employee are similar to those by the deceitful employees in the precedent cases. Like *Dudick*, Nesbit, a young sales associate, was an employee of the defendant subject to the express limitations voiced by his supervisors. As the defendant in *Dudick* did, Nesbit diverted the personal information of ConDevel's database to his personal computer at home. Nesbit did so by surreptitiously installing a keylogger onto the computer of the plaintiff, a fellow employee. Additionally, while the defendant in *Dudick* used the stolen information to fulfill his financial desires, Nesbit, while posing as a ConDevel executive at upscale restaurants, similarly used it for the purpose of fulfilling his dream of taking a "quick ladder to the top of the company" and enjoying the perks and benefits of the executives.

While the defendant in *Dudick* was "expressly entrusted" with an initial duty as an employee, the facts here do not indicate an express entrustment to Nesbit. However, the facts also do not indicate that Nesbit was unclear about this, nor should their absence bear negatively on the court's decision. The key factor considered by the court in *Dudick* focused on the fact that the defendant filtered information without plaintiff's knowledge, which is a factor clearly evident here. Thus, Nesbit's deceitful actions of installing the keylogger to filter confidential information to his personal computer is not within a purpose designated by ConDevel, and thus negates any claim of good faith.

Furthermore, Nesbit's filtering of human resource personal information is similar to the wrongful and unauthorized actions of the defendants in *Calyon*. In analyzing the statute at hand based on plain meaning, as the court in *Calyon* did, the term "purposes designated" can directly connote to actions that are not authorized or instructed by the agency or employer. Admittedly,

the facts here do not indicate an employment agreement that expressly states the designated purpose for Nesbit and the only employee direction indicated is a Computer Usage Policy; however, the repeated statements of Nesbit's supervisor that he needed to "mind his own business" and "leave the technological issues to the technology support department" clearly and expressly limited his access rights prior to his keylogger installation. The strict and repetitive instructions by Nesbit's supervisor also gave him reason to know that his intended actions were in contravention of his employer's wishes. Thus, Nesbit's installation of the keylogger, a technological issue, and theft of the personal information, clearly against the company's wishes, was not authorized by ConDevel and not within Condevel's designated purposes.

**3. The failure of ConDevel, a company paranoid of having its inadequate security system revealed, to institute credit report checks, investigation, or other reasonable remedial actions following the unauthorized breach of security and firing of the breaching employee support a strong likelihood that further unauthorized disclosure may have resulted.**

ConDevel failed to take measures to determine scope of breach, restore integrity to the system, and thus be entitled to the exception provision requiring that the information breached by Nesbit was not subject to further unauthorized disclosure. The Marshall Data Protection Act states that disclosure shall be made, consistent with legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. 17 Marshall Code § 105(a). This provision, similar to that in the California Database Security Breach Notification Act, places the responsibility on the data holder to disclose any actual or potential security breaches to allow consumers the ability to take curative measures. Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security*, 43 Hous.L.Rev. 1597, 1599 (2007).

Furthermore, the exception to the notification provision of the Marshall Data Protection

Act provides that “[g]ood faith acquisition of personal information by an employee or agent of the agency is not a breach of the security system, provided that the personal information is used for the purposes designated by the agency and/or *is not subject to further unauthorized disclosure.*” 17 Marshall Code § 105(d) (*emphasis* added) mirrors the “unlikelihood of harm” exceptions provided for in the statutes of States such as Florida and Connecticut. While these exceptions do not require notification, they do require and expect that companies, in meeting a burden of proof, will take “appropriate investigation and consultation with federal, state, and local agencies,” who then “determines that the breach will not likely result in harm.” Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C.L. Rev. 255, 286 (2005). The purpose of the notification requirement, or sufficient substitute thereof, is to protect the people to whom the confidential information is owned. *Id.* Misuse of improperly accessed personal data can result in a physical attack on a data subject or physical harm to property. *Id.* at 294; *Remsburg v Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003) (holding that an information broker owed a duty to exercise reasonable care in disclosing where woman was killed by party who purchased her personal data from an internet-based investigation service).

Courts have held that companies, agencies or employees have met their responsibility and duty to disclose and/or notify, in compliance with policy and current statutory schemes, where they not only instantly notified the subject of the personal information breached, but also provided credit reporting and tracking, and informational and identity protection services. *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018 (D. Minn. 2006); *Giordano v. Wachovia Securities, LLC*, 2006 U.S. Dist. LEXIS 52266 \* 3 (D.N. J. July 31, 2006).

In *Forbes*, the court granted the defendant’s motion for summary judgment in holding that plaintiffs failed to prove damages. *Forbes*, 420 F. Supp. 2d at 1021. The defendant was a

financial institution whose computers containing customer personal information, including the plaintiff's, were stolen. *Id.* at 1019. The defendant mailed letters to all affected and potentially affected customers notifying them of the computer theft and offering informational and identity protection services. *Id.* In recognizing these actions by the defendant and stating that there was no indication that the information on the stolen computers was accessed or misused, the court held that the plaintiffs did not have a cause of action. *Id.* at 1020.

Similarly, in *Giordano*, the court found that the plaintiff failed to prove that she suffered an injury-in-fact and it remanded the case to determine standing. *Giordano*, 2006 U.S. Dist. LEXIS 52266 \*15. As in *Forbes*, the defendant in *Giordano* was also a financial institution who accidentally disclosed the personal information of its customers. *Id.* at \*3. The defendant in *Giordano*, however, did so when it created reports, containing personal information of thousands of customers, and in the scope of its business mailed them to the customers. This case arose when the packages were never received. *Id.* To remedy the potential disclosure of the customers' information, the plaintiff conducted a "thorough executive investigation," carefully reviewed all of the mail carrier's procedures and internal reports, and offered to pay for a year of credit monitoring services for each customer. *Id.* at \* 4. While the court did not specifically conclude on the validity of these restorative procedures, it did conclude that there was no injury-in-fact, thus these remedial actions likely played a part in that decision. *Id.*

Unlike the defendants in *Forbes* and *Giordano*, ConDevel did not further the underlying policy of protecting consumers which supports an exemption from the duty to notify of a breach. After ConDevel discovered Nesbit's surreptitious installation of the keylogger and subsequent filtering of confidential information, ConDevel made a panicked conclusion that no one outside the company accessed the files, and no "true data breach had occurred. ConDevel did not seek

an objective determination by a professional, as proposed in the Florida statute, and did not execute investigations as the defendants in *Forbes* and *Giordano* did.

Furthermore, ConDevel also did not offer any credit monitoring services like those found sufficient in the precedent cases. Even though ConDevel allegedly “tightened security measures” after the breach, there is no evidence, and ConDevel has not provided any facts tending to prove that it did anything to allow Baylor curative opportunities. Based on ConDevel’s failure to provide any notification or any reparative options to Baylor, ConDevel did not fulfill its responsibility of notifying or proving sufficient substitution, as per the Data Protection Act. Because of the seriousness of potential harm to those who have been victim to personal information theft, like Baylor, ConDevel should not be excused from these notification obligations and in doing nothing in support of these policies does not deserve to be exempted from the uniform and directive provisions of the Marshall Data Protection Act.

### **CONCLUSION**

This Court should reverse by ruling that Nesbit intruded upon Baylor’s seclusion and by ruling that ConDevel was not exempt from the notification provision of the Marshall Data Protection Act.

Marshall should recognize this cause of action because it will protect the privacy interests of the citizens of Marshall. Nesbit’s actions constituted an unauthorized intrusion because he was a low-level employee who surreptitiously installed a keylogger program on Baylor’s computer and accessed his personal information. A reasonable person would be offended by the intrusion because Nesbit recorded Baylor’s keystrokes and accessed personal information. Baylor had a zone of solitude in his work computer because it was in his personal office and he had passwords on it. Baylor had a zone of solitude as to the disclosure of his personal

information to an unauthorized person because of the sensitive nature of the information and because Nesbit was not authorized to access the information. This Court should not require a showing of anguish and suffering because doing so will not protect the privacy interests of the citizens of Marshall. Even if this Court does require such a showing, the intrusion caused anguish and suffering because Baylor was embarrassed and humiliated when the managers at the golf club and restaurant told him he was banned.

ConDevel did not meet the burden of proof since Nesbit's secret installation of a keylogger program and filtering thereof to his personal computer did not constitute good faith acquisition, Nesbit's use of the information to imposter Baylor and obtain access to exclusive clubs was not a use for purposes designated by ConDevel, and ConDevel's failure to take any measures to determine the scope of the breach or to notify anyone do not satisfy a conclusion that the information was not subject to further unauthorized disclosure.

ConDevel is not entitled to discretion to notify since ConDevel failed to provide any proof of substitute procedures, and since ConDevel did not notify anyone, but instead sought ways to keep the breach undisclosed.

Therefore this court should reverse the ruling granting summary judgment.

DATED: September 24, 2007

Respectfully submitted,

---

Team: 25  
Attorneys for Appellant