

ISSUES PRESENTED

- I. Whether the Court of Appeals erred in failing to recognize Baylor's valid claim of intrusion upon seclusion when the protection of seclusion is fundamental to the right to privacy and Baylor's seclusion was violated by the surreptitious installation of a "keylogger" program on his computer.

- II. Whether the Court of Appeals erred in holding that the Marshall Data Protection Act did not apply to ConDevel when both the plain text and the purpose of the statute indicate that an exemption is only appropriate in instances of good faith.

TABLE OF CONTENTS

	<u>Page</u>
ISSUES PRESENTED.....	i
TABLE OF AUTHORITIES	v
OPINION BELOW.....	1
STATUTORY PROVISION	1
STATEMENT OF THE CASE.....	1
I. Statement of the Facts.....	1
II. Preliminary Statement.....	4
SUMMARY OF THE ARGUMENT	6
ARGUMENT	7
I. NESBIT INTRUDED UPON BAYLOR’S SECLUSION WHEN HE INSTALLED A KEYLOGGER PROGRAM ON BAYLOR’S WORKPLACE COMPUTER.....	8
A. <u>This Court Should Recognize Baylor’s Legitimate Claim for Intrusion Upon Seclusion</u>	9
B. <u>The Installation of a Keylogger Program on Baylor’s Computer Constituted an Intrusion into His Private Sphere</u>	11
C. <u>The Installation of a Keylogger on and Subsequent Monitoring of Baylor’s Computer by a Junior Employee Would Be Offensive to a Reasonable Person Subjected to Such an Intrusion</u>	13
D. <u>Baylor Had an Objectively Reasonable Expectation of Privacy in His Workplace Computer Against Intrusion by Junior Employees</u>	15
E. <u>The Intrusion Caused Baylor Suffering and Mental Anguish, Satisfying Even the Restrictive Requirement for the Tort Applied by the First and Second Marshall Circuit Courts</u>	16
F. <u>ConDevel Should Be Held Responsible for Nesbit’s Actions Because He Was Acting within the Scope of His Employment When He Installed the Keylogger on Baylor’s Computer</u>	18

1.	Nesbit’s Actions Were within the Scope of His Employment Because He Desired to Serve and Benefit ConDevel When He Installed the Keylogger.....	19
2.	Fairness Demands that ConDevel Be Held Responsible for Baylor’s Injuries Because Nesbit’s Actions Were Closely Related to His Employment and ConDevel Benefited from Those Actions.	20
II.	CONDEVEL VIOLATED THE MARSHALL DATA PROTECTION ACT WHEN IT FAILED TO NOTIFY BAYLOR OF THE DATA SECURITY BREACH.....	22
A.	<u>The Unambiguous Plain Meaning of the Marshall Data Protection Act’s Text Required ConDevel to Notify Baylor of the Data Security Breach.</u>	22
1.	A Breach of Security Occurred When Nesbit Downloaded the Personnel Files onto His Home Computer Because He Was Not Authorized to Acquire the Data and the Data Acquired Contained Personal Information.	23
2.	The Good Faith Exception to the Notification Requirement in the Statute Does Not Apply to ConDevel Because Nesbit Was Not Acting in Good Faith and the Acquired Information Was Not Used for Purposes Designated By ConDevel.	29
B.	<u>The Purpose of the Marshall Data Protection Act Is to Protect Individuals Like Baylor and Apply to Companies Like ConDevel.</u>	31
1.	The ConDevel Breach Is Just One of Many Recent Data Security Breaches that Have Demonstrated the Burgeoning Problem of Identity Theft.....	31
2.	The Legislative History of the California Model Statute Demonstrates Lawmakers Were Attempting to Prevent Identity Theft and Intended the Law to Apply to Companies Like ConDevel.	33
3.	The ChoicePoint Breach Showed the Efficacy of the California Statute and Spurred Other States to Pass Similar Laws to Promote Notification and Prevent Identity Theft in Their States.	37

4.	The Structure of the Marshall Data Protection Act Further Shows Its Purpose Is to Discourage Corporate Secrecy When Personal Information Has Been Acquired by Unauthorized Individuals.....	39
	CONCLUSION.....	40

TABLE OF AUTHORITIES

<u>CASES</u>	<u>Page</u>
 UNITED STATES SUPREME COURT	
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242 (1986).....	8
<i>Celotex v. Catrett</i> , 477 U.S. 317 (1986).....	8
<i>Cnty. for Creative Non-Violence v. Reid</i> , 490 U.S. 730 (1989).....	22, 23
<i>Crandon v. United States</i> , 494 U.S. 152 (1990).....	33
<i>Edwards v. Aguillard</i> , 482 U.S. 578 (1987).....	31
<i>Elder v. Holloway</i> , 510 U.S. 510 (1994).....	8
<i>Gulf States Steel Co. v. United States</i> , 287 U.S. 32 (1932).....	33, 34
<i>McCreary County Ky. v. Am. Civil Liberties Union of Ky.</i> , 545 U.S. 844 (2005).....	31
<i>Perrin v. United States</i> , 444 U.S. 37 (1979).....	23
<i>Poller v. Columbia Broad. Sys., Inc.</i> , 368 U.S. 464 (1962).....	29, 30
 UNITED STATES COURT OF APPEAL	
<i>Birnbaum v. United States</i> , 588 F.2d 319 (2d Cir. 1978).....	11
<i>Dietemann v. Time, Inc.</i> , 449 F.2d 245 (9th Cir. 1971)	11, 12

TABLE OF AUTHORITIES (Cont.)

<u>CASES</u>	<u>Page</u>
<i>Duffy v. United States</i> , 966 F.2d 307 (7th Cir. 1992)	19
<i>Int’l Airport Ctrs., L.L.C. v. Citrin</i> , 440 F.3d 418 (7th Cir. 2006)	26
<i>Pfizer, Inc. v. Int’l Rectifier Corp.</i> , 538 F.2d 180 (8th Cir. 1976)	29, 30
<i>Phillips v. Grendahl</i> , 312 F.3d 357 (8th Cir. 2002)	10
<i>Phillips v. Smalley Maint. Servs., Inc.</i> , 711 F.2d 1524 (11th Cir. 1983)	11
<i>Tompkins v. Cyr</i> , 202 F.3d 770 (5th Cir. 2000)	17
<i>United States v. Flemmi</i> , 225 F.3d 78 (1st Cir. 2000).....	25, 26
<i>United States v. Hill</i> , 579 F.2d 480 (8th Cir. 1978)	27, 28
<i>Vernars v. Young</i> , 539 F.2d 966 (3d Cir. 1976).....	15
<i>Walker v. Darby</i> , 911 F.2d 1573 (11th Cir. 1990)	15
UNITED STATES DISTRICT COURT	
<i>Amati v. City of Woodstock</i> , 829 F. Supp. 998 (N.D. Ill. 1993)	12
<i>Bauer v. Ford Motor Credit Co.</i> , 149 F. Supp. 2d 1106 (D. Minn. 2001).....	13
<i>Doe v. Kohn Nast & Graf, P.C.</i> , 862 F. Supp. 1310 (E.D. Pa. 1994)	15

TABLE OF AUTHORITIES (Cont.)

<u>CASES</u>	<u>Page</u>
<i>Fischer v. Mount Olive Lutheran Church, Inc.</i> , 207 F. Supp. 2d 914 (W.D. Wis. 2002)	15
<i>Peavy v. Wfaa-Tv, Inc.</i> , 37 F. Supp. 2d 495 (N.D. Tex. 1998)	12
<i>Pulla v. Amoco Oil Co.</i> , 882 F. Supp. 836 (S.D. Iowa 1994)	17
<i>Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.</i> , 119 F.Supp.2d 1121 (W.D. Wash. 2000).....	26
<i>Socialist Workers Party v. Attorney Gen. of U.S.</i> , 642 F. Supp. 1357 (S.D.N.Y. 1986).....	8
<i>United States v. Ropp</i> , 347 F. Supp. 2d 831 (C.D. Cal. 2004)	13
STATE SUPREME COURT	
<i>Bailer v. Erie Ins. Exch.</i> , 687 A.2d 1375 (Md. 1997)	10
<i>Baker v. Saint Francis Hosp.</i> , 126 P.3d 602 (Okla. 2005)	21
<i>District of Columbia v. Davis</i> , 386 A.2d 1195 (D.C. 1978)	21
<i>Fischer v. Hooper</i> , 732 A.2d 396 (N.H. 1999)	17
<i>Hamberger v. Eastman</i> , 206 A.2d 239 (N.H. 1964)	12
<i>Jensen v. Sawyers</i> , 130 P.3d 325 (Utah 2005).....	15
<i>Lake v. Wal-Mart Stores, Inc.</i> , 582 N.W.2d 231 (Minn. 1998).....	8, 9

TABLE OF AUTHORITIES (Cont.)

<u>CASES</u>	<u>Page</u>
<i>Monroe v. Darr</i> , 559 P.2d 322 (Kan. 1977)	17, 18
<i>Plains Res. v. Gable</i> , 682 P.2d 653 (Kan. 1984)	18
<i>Preferred Nat. Ins. Co. v. DocuSource, Inc.</i> , 829 A.2d 1068 (N.H. 2003)	10
<i>Remsburg v. Docusearch, Inc.</i> , 816 A.2d 1001 (N.H. 2003)	14
<i>Sage Club v. Hunt</i> , 638 P.2d 161 (Wyo. 1981)	20
<i>Sanders v. Am. Broad. Cos., Inc.</i> 978 P.2d 67 (Cal. 1999)	10, 12, 15
<i>State v. Mitchell</i> , 563 S.W.2d 18 (Mo. 1978)	34
<i>Times Mirror Co. v. Superior Court</i> , 813 P.2d 240 (Cal. 1991)	34
<i>Whipps Land & Cattle Co. v. Level 3 Commc'ns., LLC</i> , 658 N.W.2d 258 (Neb. 2003)	10
STATE COURT OF APPEALS	
<i>Doe v. High-Tech Inst., Inc.</i> , 972 P.2d 1060 (Colo. Ct. App. 1998)	9, 10, 16, 17
<i>Embrey v. Holly</i> , 442 A.2d 966 (Md. Ct. App. 1982)	18
<i>Gonpere Corp. v. Rebull</i> , 440 So. 2d 1307 (Fla. Dist. Ct. App. 1983)	18
<i>Household Credit Servs., Inc. v. Driscoll</i> , 989 S.W.2d 72 (Tex. App. 1998)	18

TABLE OF AUTHORITIES (Cont.)

<u>CASES</u>	<u>Page</u>
<i>K-Mart Corp. Store No. 7441 v. Trotti</i> , 667 S.W.2d 630 (Tex. App. 1984).....	15
<i>Lewis v. Dayton Hudson Corp.</i> , 339 N.W.2d 857 (Mich. Ct. App. 1983).....	10
<i>Lingar v. Live-In Companions, Inc.</i> , 692 A.2d 61 (N.J. Super. Ct. App. Div. 1997).....	10
<i>Los Ranchitos v. Tierra Grande, Inc.</i> , 861 P.2d 263 (N.M. Ct. App. 1993)	21
<i>Pemberton v. Bethlehem Steel Corp.</i> , 502 A.2d 1101 (Md. Ct. Spec. App. 1986).....	12
<i>Sabrina W. v. Willman</i> , 540 N.W.2d 364 (Neb. Ct. App. 1995).....	17
<i>Saint Julien v. S. Cent. Bell Tel. Co.</i> , 433 So. 2d 847 (La. Ct. App. 1983).....	18
<i>Sanchez-Scott v. Alza Pharms.</i> , 103 Cal. Rptr. 2d 410 (Cal. Ct. App. 2001).....	13
<i>Snakenberg v. Hartford Cas. Ins. Co.</i> , 383 S.E.2d 2 (S.C. Ct. App. 1989).....	16
<i>Swarthout v. Mut. Serv. Life Ins. Co.</i> , 632 N.W.2d 741 (Minn. Ct. App. 2001).....	14
<i>Turner v. State</i> , 494 So. 2d 1292 (La. Ct. App. 1986).....	20
<i>Young v. Stensrude</i> , 664 S.W.2d 263 (Mo. Ct. App. 1984).....	18, 19
 <u>STATUTES</u>	
STATE OF MARSHALL STATUTES	
17 Marshall Code §105 (2006).....	<i>passim</i>

TABLE OF AUTHORITIES (Cont.)

<u>STATUTES</u>	<u>Page</u>
Marshall R. Civ. P. 56(c)	8
 STATE STATUTES	
Cal. Civ. Code § 1798.29, §§ 1798.80-98 (2006).....	28, 34, 39
Ga. Code. Ann. § 10-1-910 (2007).....	38
815 Ill. Comp. Stat. 530/1-5 (2005).....	28
La. Rev. Stat. Ann. §§ 51-3072, 75 (2007)	38, 39
Me. Rev. Stat. Ann. tit. 10, § 1347 (2005)	27
Mont. Code. Ann. § 30-14-1701 (2005).....	38
Tenn. Code. Ann. § 47-18-2107.....	39
Wash. Rev. Code. § 19.255.010(10)(a) (2007)	39
 BILLS	
Assemb. B. 700, 2001-02 Reg. Sess. (Cal. 2002) (as amended in Senate, August 22, 2002).....	35
S.B. 1386 § 5, 2001-02 Reg. Sess. (Cal. 2002) (as amended in Assembly, June 30, 2002)	35
<i>Analysis of Assemb. B. No. 700 Before the Cal. S. Privacy Comm.</i> , 2001-02 Reg. Sess., at 7-8 (August 21, 2002).....	35, 36
 <u>MISCELLANEOUS</u>	
 RESTATEMENTS	
Restatement (Third) of Agency § 2.02 (2006)	25
Restatement (Second) of Torts, § 652B (1977).....	9, 10, 11
Restatement (Second) of Torts, § 652H (1977).....	10

TABLE OF AUTHORITIES (Cont.)

<u>MISCELLANEOUS</u>	<u>Page</u>
BOOKS	
Black’s Law Dictionary (8th ed. 2004).....	24, 29
ARTICLES	
Ian C. Ballon, <i>A Legal Analysis of State Security Breach Statutes</i> , 903 PLI/Pat 135 (2007).....	37
Don Corbett, <i>Virtual Espionage: Spyware and the Common Law Privacy Torts</i> , 36 U. Balt. L. Rev. 1 (2006)	7
Amanda Draper, Comment, <i>Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law</i> , 40 J. Marshall L. Rev. 681 (2007)	31, 32, 33
David Eggleston, <i>Privacy Issue as Serious as Y2K: Expert</i> , Strategy Magazine, September 13, 1999	33
Bruce E. H. Johnson & Kaustuv M. Das, Ph.D., <i>Data Breach Notice Legislation: New Technologies and New Privacy Duties?</i> , 865 PLI/Pat 203 (2006).....	31, 35
John B. Kennedy, <i>Slouching Towards Security Standards: The Legacy of California’s SB1386</i> , 865 PLI/Pat 91 (2006).....	32, 33
Satish M. Kini & James T. Shreve, <i>Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches</i> , 10 N.C. Banking Inst. 87 (2006).....	34, 37
Norbert F. Kugele & James Placer, <i>Navigating Some Uncertain Waters in Michigan’s New Security Breach Notification Law</i> , Privacy & Data Security L. 2007.07-5 (2007).....	37, 38

TABLE OF AUTHORITIES (Cont.)

<u>MISCELLANEOUS</u>	<u>Page</u>
Kristen J. Mathews, <i>Data Security Breach Notification: Complying with State Laws; Still Awaiting Pending Federal Legislation</i> , 1 No. 4 Privacy & Data Protection Leg. Rep. 3 (2006).....	34
Edmund Mierzwinski, <i>Testimony of Consumer and Privacy Groups on Data Security, Data Breach Notices, Privacy and Identity Theft</i> , 1533 PLI/Corp 333 (2006).....	37, 38
Kathryn E. Picanso, Note, <i>Protecting Information Security Under a Uniform Data Breach Notification Law</i> , 75 Fordham L. Rev. 355, 383 (2006).....	38
S. Kasim Razvi, <i>To What Extent Should State Legislatures Regulate Business Practices as a Means of Preventing Identity Theft?</i> , 15 Alb. L.J. Sci. & Tech. 639 (2005).....	32
Michael Sivy, Pat Regnier & Carolyn Bigda, <i>What No One Is Telling You About Identity Theft</i> , Money, July 2005.....	32, 33
Daniel J. Solove & Chris Jay Hoofnagel, <i>A Model Regime of Privacy Protection</i> , 2006 U. Ill. L. Rev. 357 (2006).....	37
Samuel D. Warren & Louis Brandeis, <i>The Right to Privacy</i> , 4 Harv. L. Rev. 193 (1890).....	7

TO THE SUPREME COURT OF THE STATE OF MARSHALL

Appellant, Ron Baylor, respectfully submits this brief in support of his request to reverse the judgment of the court below.

OPINION BELOW

The opinion and order of the Grant County District Court is unreported. The opinion of the Fourth Circuit Court of Appeals of the State of Marshall is unreported and is set forth in the record. (R. at 1.)

STATUTORY PROVISION

This case involves the following statutory provision: Marshall Data Protection Act, 17 Marshall Code § 105 (2006).

STATEMENT OF THE CASE

Statement of the Facts

Appellant Ron Baylor (“Baylor”) worked hard for over 25 years to reach his position as an executive vice president at Appellee ConDevel, Inc. (“ConDevel”) in the State of Marshall. (R. at 2.) He is in charge of the operations, sales, and human resources departments, and by virtue of his high rank is eligible to take part in the company’s “VIP Program.” (R. at 2.) While the program provides Baylor access to “exclusive clubs, VIP lounges, luxury suites, limousine services and the like,” he has not exercised all of these benefits. (R. at 2, 4.) Unbeknownst to Baylor, another employee acquired his personal information and assumed his identity at the venues he had yet to enjoy, including the Marshall League Club, the “most exclusive private social club in the state.” (R. at 4.)

Steve Nesbit (“Nesbit”) was a junior sales associate at ConDevel. (R. at 2.) Impatient to achieve the status and perks of upper management, he expressed interest in finding a “way to

enjoy the good life reserved to the executives.” (R. at 2.) Nesbit studied technology in his spare time and was interested in helping ConDevel improve its data security systems. (R. at 3.) ConDevel had recently downsized the technology support department and failed to invest in its information security infrastructure. (R. at 2.) Nesbit knew this and had expressed his opinion that “ConDevel was a data-breach waiting to happen.” (R. at 3.) However, he was told to “mind his own business and leave technological issues to the technology support department.” (R. at 3.)

Undeterred, Nesbit used his technology skills to write a program called a “keylogger.” (R. at 3.) Once installed on a computer, a keylogger records everything typed on the keyboard, from private emails to secret company passwords. (R. at 3.) Nesbit designed the program to save the recorded keystrokes to a text file and email the file to his private email account. (R. at 3.) He used an outside email address, rather than a ConDevel email address, because this would make him “more difficult to catch.” (R. at 3.) Nesbit then put his keylogger program onto a “flash drive,” a thumb-sized memory storage device, and waited for the opportunity to install the program on the first available computer. (R. at 3.)

One day, when Baylor left his office, Nesbit went inside, plugged the flash drive into Baylor’s computer, and installed the keylogger. (R. at 3.) The keylogger then allowed Nesbit to “see” everything Baylor typed on his computer. (R. at 3.) Because Baylor oversees the human resources department, the keylogger recorded Baylor’s username and password for ConDevel’s human resources database and transmitted that information to Nesbit. (R. at 4.) The human resources database holds the employees’ electronic personnel files, which contain sensitive material such as contact information, Social Security and driver’s license numbers, salary information, and other personal data. (R. at 2.)

Nesbit's original plan was to breach the system to demonstrate its vulnerabilities, then show ConDevel's management what he had done and how to fix it, hoping to gain recognition as a "team player and problem solver." (R. at 4.) However, after discovering he could access the VIP Program with Baylor's passwords, Nesbit abandoned his plan to improve the company's data security. (R. at 4.) Instead, he decided to treat himself to some of the benefits only available to ConDevel executives. (R. at 4.) To that end, he downloaded the entire human resources database onto his home computer, acquiring the sensitive personal information of all of ConDevel's employees. (R. at 4.)

Now able to examine the database at his leisure, Nesbit discovered that Baylor had not joined all of the clubs available to him. (R. at 4.) Nesbit took advantage of this by requesting several memberships in Baylor's name, which he had sent to his own address. (R. at 4.) Nesbit then began frequenting the establishments while posing as Baylor. (R. at 4.) The ruse continued until Nesbit-as-Baylor became seriously inebriated one night at the Marshall League Club and got into a fight with a prominent member. (R. at 4.) As a consequence, "Baylor" was banished from the club and subsequently blacklisted from the other exclusive establishments. (R. at 4.)

Baylor began to suspect something was wrong when, in successive incidents, he was turned away from the Shady Links golf club and Les Deux Pommes, an upscale restaurant. (R. at 4-5.) Both establishments informed him that he would not be allowed in as a result of his behavior at the Marshall League Club. (R. at 4-5.) Angry and humiliated, Baylor concluded his identity had been stolen. (R. at 5.) He began an investigation and was shocked to discover that someone had recently issued several memberships in his name. (R. at 5.) Baylor informed ConDevel's technology support department of the situation and his suspicions of possible unauthorized activity. (R. at 5.) A technology expert discovered the keylogger program on

Baylor's computer, and further investigation revealed the extent of Nesbit's activities. Soon after, Nesbit was fired. (R. at 5.)

ConDevel was concerned about the potential embarrassment and harm to company's reputation if word of a data security breach got to their clients, particularly in light of the recent budget cuts and technology support department lay-offs. (R. at 1, 2, 5.) The company's management decided that because Nesbit had been an employee, there had not been a "true" data breach, and therefore, there was no need to notify anyone. (R. at 5.) Significantly, ConDevel's chief operating officer left a voice mail for the director of the technology support department, warning: "As far as we know, no one knows that this ever happened. Let's keep it that way. The last thing we need right now is a lawsuit or a scandal. We cannot afford losing our good name and our clients." (R. at 5.) Consequently, neither Baylor nor any of the other employees were informed that someone had downloaded their personal information to a non-business computer, and therefore, none of the employees were given the opportunity to protect their identities. To date, no one at ConDevel has offered to help Baylor rebuild his good name. (R. at 5.)

II. Preliminary Statement

Baylor filed a lawsuit against Appellee in the Grant County District Court in July 2005, claiming (1) intrusion upon seclusion and (2) a violation of the Marshall Data Protection Act, 17 Marshall Code section 105 (2006). (R. at 5.) Appellee moved for summary judgment on both counts pursuant to Marshall Rule of Civil Procedure, Rule 56(c). (R. at 1, 5.) The district court granted Appellee's motion as to both counts. (R. at 5-6.) The court then found that Appellee had not violated the notification statute and held that because neither the Fourth Circuit Court of Appeals for the State of Marshall nor the Supreme Court of the State of Marshall had recognized the tort of intrusion upon seclusion, that it would not allow the action. (R. at 5-6.)

Baylor then petitioned the Fourth Circuit Court of Appeals for review of the district court opinion granting summary judgment. (R. at 6.) Presiding Judge Al Reyes reviewed the case *de novo*, using the same test for summary judgment as applied by the district court: “the evidence must demonstrate that there is no genuine issue as to any material fact and the moving party is entitled to a judgment as a matter of law.” (R. at 1.) On the claim of intrusion upon seclusion, the circuit court hesitated to endorse the tort without approval by the Marshall Supreme Court. (R. at 6-7.) Regardless, the court held that Baylor failed to satisfy one of the elements of the tort, finding that he had not pleaded any facts to prove mental anguish or suffering. (R. at 7.) The circuit court upheld the district court’s finding that Nesbit obtained the information while testing the computer security system and held that this constituted “good faith” acquisition under the exception in 17 Marshall Code section 105(d). (R. at 7.) The circuit court affirmed that Nesbit’s use of the data complied with Appellee’s “scopes and purposes” and that Appellee was free to choose whether or not to inform its employees of the breach. (R. at 7.)

On July 24, 2007, this Court granted Appellant leave to appeal the decision of the Fourth Circuit Court of Appeals upholding the Grant County District Court’s grant of summary judgment. (R. at 10.)

SUMMARY OF THE ARGUMENT

The district court improperly granted summary judgment on the claims of intrusion upon seclusion and ConDevel's violation of the Marshall Data Protection Act. There are genuine issues of material fact as to both causes of action and therefore summary judgment is inappropriate.

I.

Steve Nesbit intruded upon Ron Baylor's seclusion when he installed a keylogger program on Baylor's computer. Baylor had a legitimate expectation of privacy in his workplace computer, particularly against junior employees such as Nesbit. Nesbit's unauthorized surveillance of Baylor was a highly offensive intrusion as Nesbit recorded every keystroke Baylor entered into his computer, thus monitoring Baylor's confidential business and personal information and communications. While many courts consider an intrusion upon seclusion damaging in and of itself, Baylor has also pleaded facts sufficient to demonstrate mental anguish, satisfying even the more restrictive formulation of the tort.

Furthermore, ConDevel should be held responsible for Nesbit's intrusion because Nesbit was acting within the scope of his employment. Nesbit initially sought to assist ConDevel with its computer security and he reasonably believed that his installation of the keylogger was within his general employment duties. Additionally, as ConDevel benefited from Nesbit's actions through the revelation of its computer vulnerabilities, it is more fair to hold ConDevel responsible than leave Baylor uncompensated for the violation he has suffered.

II.

The Marshall Data Protection Act requires agencies that store unencrypted personal information to notify affected individuals when the information is acquired by an unauthorized

person. Baylor experienced identity theft after his data was acquired for entirely self-serving purposes by a former employee of ConDevel. This acquisition of Baylor's personal information was unauthorized under any reasonable interpretation of the terms of the statute, and ConDevel fails to demonstrate that it fell within the language of the good faith exception to the Act. Furthermore, the historical context and legislative history of other state data breach notification statutes demonstrate that the purpose of the statutes is to protect individuals like Baylor, apply to businesses like ConDevel, and to publicize incidents like the breach that occurred here. Similar occurrences across the country have shown that companies are unlikely to reveal damaging data breaches without legislative mandate. Requiring disclosure gives individuals the opportunity to protect themselves from identity theft.

ConDevel is not entitled to summary judgment given the plain meaning of the Act. Even if Nesbit's actions are susceptible to interpretation, whether the acquisition of personnel files fell within the good faith exemption is a factual inquiry that must be determined by a jury.

For these reasons, this Court should reverse the holding of the Fourth Circuit Court of Appeals and remand the case for trial.

ARGUMENT

As early as 1890, Samuel D. Warren and Louis Brandeis expressed their concern that “numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’” Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890). Their fears have been realized in the computer age with the invention of spyware programs, such as the keylogger utilized by Steve Nesbit to violate Ron Baylor's workplace privacy. See Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. Balt. L. Rev. 1, 4-10 (2006). Nesbit not

only used the keylogger to intrude upon Baylor's seclusion, he then used Baylor's passwords to breach ConDevel's human resources database and acquire the employee personnel files therein. Compounding Baylor's injuries, ConDevel failed to inform Baylor or any other employee of the breach and loss of information, thus violating the Marshall Data Protection Act.

Summary judgment is only proper if the evidence in the record demonstrates no genuine issue of any material fact and the moving party is entitled to judgment as a matter of law. Marshall R. Civ. P., Rule 56(c); *see Celotex v. Catrett*, 477 U.S. 317, 322 (1986). This Court reviews the circuit court's grant of summary judgment *de novo*. *See Elder v. Holloway*, 510 U.S. 510, 516 (1994). Summary judgment is improper where there is a genuine dispute about a material issue and a reasonable jury could return a verdict for the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In determining whether summary judgment is proper, a court must interpret all facts and draw all justifiable inferences in favor of the non-moving party. *See id.* at 255. As Baylor opposes the motion for summary judgment, the Court must construe all facts and inferences in the light most favorable to him. Summary judgment is improper in this case because the facts demonstrate genuine issues of material fact as to Baylor's claims for intrusion upon seclusion and violation of the Marshall Data Protection Act.

I. NESBIT INTRUDED UPON BAYLOR'S SECLUSION WHEN HE INSTALLED A KEYLOGGER PROGRAM ON BAYLOR'S WORKPLACE COMPUTER.

The vast majority of jurisdictions recognize the right to privacy in some form, either in common law or by statute, as "an integral part of our humanity." *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 235 (Minn. 1998); *see also Socialist Workers Party v. Attorney Gen. of U. S.*, 642 F. Supp. 1357, 1421-22 (S.D.N.Y. 1986). In recognizing the tort of intrusion upon seclusion, the Minnesota Supreme Court noted that "the heart of our liberty is in choosing which parts of our lives shall become public and which parts we shall hold close." *Lake*, 582 N.W.2d at

235. The First and Second Circuit Courts in the State of Marshall have embraced the tort of intrusion upon seclusion in a form similar to that found in the Restatement (Second) of Torts. (R. at 6.); *see* Restatement (Second) of Torts, § 652B (1977).

A. This Court Should Recognize Baylor's Legitimate Claim for Intrusion Upon Seclusion.

This Court has endorsed a general right to privacy actionable in related claims, but has never explicitly recognized the tort of intrusion upon seclusion. (R. at 6.) As one court has noted, “the vast majority of courts in other jurisdictions which have recognized other types of common law privacy claims, without significant debate, also have recognized the existence of a discrete claim for invasion of privacy based on intrusion upon seclusion.” *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1067 (Colo. Ct. App. 1998) (noting recognition by Alabama, Maine, Missouri, Texas, Washington, and Wisconsin). This Court should join the overwhelming national consensus and specifically recognize the tort of intrusion upon seclusion as integral to the protection of the privacy right and find the tort actionable in the State of Marshall.

Failing to recognize the tort, while recognizing privacy torts that depend on use or disclosure of private information (such as false light privacy or appropriation) makes an arbitrary distinction between the attempt to gain private information and the actual use of that information. This fails to take into account the damage done not only by the intrusion itself, but also by any acquisition of private information by the intruder. To protect the zone of solitude that the privacy right describes, this Court should recognize a cause of action based on the violation of that solitude, rather than requiring some further conduct for the violation to be made actionable. Doing otherwise would leave a gaping hole in the privacy interest and allow intruders to snoop and harass without fear of punishment, so long as they kept the private information to themselves.

While the First and Second Circuit Courts recognize the three traditional elements of intrusion upon seclusion, as found in the Restatement, requiring that a plaintiff must prove “(1) unauthorized intrusion or prying into the plaintiff’s seclusion; (2) the intrusion is offensive or objectionable to a reasonable person; [and] (3) the matter of the intrusion is private,” the Marshall courts have also required plaintiffs to demonstrate that “the intrusion causes anguish and suffering.” (R. at 6-7.); *see* Restatement (Second) of Torts, § 652B (1977). Many courts have maintained the traditional three-prong test endorsed by the Restatement. *See, e.g., Phillips v. Grendahl*, 312 F.3d 357, 372 (8th Cir. 2002) (applying Minnesota law); *Sanders v. Am. Broad. Cos., Inc.*, 978 P.2d 67, 71 (Cal. 1999); *Bailer v. Erie Ins. Exch.*, 687 A.2d 1375, 1380-81 (Md. 1997); *Lewis v. Dayton Hudson Corp.*, 339 N.W.2d 857, 859 (Mich. Ct. App. 1983); *Whipps Land & Cattle Co. v. Level 3 Commc’ns, LLC*, 658 N.W.2d 258, 269-70 (Neb. 2003); *Lingar v. Live-In Companions, Inc.*, 692 A.2d 61, 67 (N.J. Super. Ct. App. Div. 1997). The Restatement provides damages for the basic harm to the privacy interest itself and courts have generally found the intrusion into one’s private sphere is a harm in and of itself without the need to show further damages. *See* Restatement (Second) of Torts, § 652H (1977) (separately addressing the general harm to one’s privacy interest from the intrusion and additional damages from mental distress or other special damages); *Preferred Nat. Ins. Co. v. DocuSource, Inc.*, 829 A.2d 1068, 1075 (N.H. 2003) (“An action for intrusion upon seclusion does not require a claimant to prove any harm beyond the intrusion itself.”); *High-Tech Inst., Inc.*, 972 P.2d at 1066 (“damages for that invasion may include: (1) general damages for harm to a plaintiff’s interest in privacy resulting from the invasion; (2) damages for mental suffering; (3) special damages; and (4) nominal damages if no other damages are proven.”).

The Restatement’s traditional three-prong test, excluding the “mental anguish” element, best protects the privacy right and should be adopted by this Court. Every violation of privacy inherently involves some damage to one’s sense of solitude and seclusion. Establishing “mental anguish” as an element of intrusion upon seclusion confuses the elements of the tort with the damages caused by that tort. The “mental anguish” bar would prevent harmed plaintiffs from recovering at least nominal damages for intrusions upon their solitude and would allow violators of the privacy right to escape liability for their intrusions.

However, even if this Court adopts the restricted view of intrusion upon seclusion that has been applied by the lower court, the facts still demonstrate genuine issues of material fact as to the intrusion upon Baylor’s seclusion and his resulting mental anguish, making summary judgment improper in this case.

B. The Installation of a Keylogger Program on Baylor’s Computer Constituted an Intrusion into His Private Sphere.

Nesbit intruded in an actionable manner when he installed a keylogger program on Baylor’s computer. The Restatement makes clear that a physical intrusion is not necessary for the tort to be actionable and lists several examples of intrusive behaviors, including voyeurism and eavesdropping (with or without mechanical aids), opening personal mail, searching safes or wallets, and prying into personal bank accounts. Restatement (Second) of Torts, § 652B, comm. b. (1977). Courts have found intrusions by means of opening mail, photography, peeping through windows, and even overzealous prying into private affairs through questioning and coercive demands. *See, e.g., Phillips v. Smalley Maint. Servs., Inc.*, 711 F.2d 1524, 1526, 1532 (11th Cir. 1983) (finding actionable improper questions and demands regarding the plaintiff’s sexual preferences); *Birnbaum v. United States*, 588 F.2d 319, 326 (2d Cir. 1978) (finding an intrusion by a defendant who opened private mail belonging to the plaintiff); *Dietemann v. Time*,

Inc., 449 F.2d 245, 247-48 (9th Cir. 1971) (affirming a judgment of intrusion for secretly photographing and recording a plaintiff). It is clear that the tort includes a wide swath of intrusive activities and the installation of a keylogger fits within this ambit as it gave Nesbit access to Baylor's private sphere that he otherwise would not have had.

Courts have routinely found similar intrusions by means of eavesdropping and recording devices within the purpose of the tort. *See, e.g., Sanders*, 978 P.2d at 69 (intrusion by a reporter's use of a video camera in an office setting); *Pemberton v. Bethlehem Steel Corp.*, 502 A.2d 1101, 1117 (Md. Ct. Spec. App. 1986) (intrusion by a "detection device" at the plaintiff's motel room); *Hamberger v. Eastman*, 206 A.2d 239, 239-40, 242 (N.H. 1964) (intrusion by a listening device installed in the plaintiff couple's bedroom by their landlord). One court noted that "eavesdropping is the quintessential example of a highly offensive intrusion upon seclusion." *Peavy v. Wfaa-Tv, Inc.*, 37 F. Supp. 2d 495, 521 (N.D. Tex. 1998). In *Peavy*, the defendants used a police scanner to listen to plaintiff's telephone conversations over a period of months. *Id.* The court not only found the action intrusive, but held that it constituted intrusion as a matter of law. *Id.*

A similar result was reached in *Amati v. City of Woodstock*, a case involving the tapping of a telephone line. 829 F. Supp. 998, 1000-01 (N.D. Ill. 1993). In *Amati*, the city police department maintained a private, untapped telephone line for personal phone calls to and from the department. *Id.* At some point in time, the chief of police surreptitiously installed a wiretap and recording device on the private line and began continuously monitoring the calls placed on that line. *Id.* at 1001. The court found that the use of the mechanical monitoring device violated the plaintiff's privacy right and therefore constituted an intrusion upon the caller's seclusion. *Id.* at 1010-11.

The keylogger program at issue in the case at bar is directly analogous to these mechanical devices for eavesdropping and recording conversations. The program recorded every keystroke Baylor typed and transmitted that information to Nesbit, just as a listening device records and transmits every word spoken by the person being monitored. The only appreciable difference between recording a conversation and recording what is entered into a computer is that the former records audible speech. Otherwise, the keylogger is directly comparable to a surreptitious electronic monitoring device. In fact, one court recently noted that such a program “‘eavesdrops’ on the person typing messages into the computer” and called the installation of a keylogger “a gross invasion of privacy.” *United States v. Ropp*, 347 F. Supp. 2d 831, 838 (C.D. Cal. 2004). Given the similarities to eavesdropping and recording devices and the *Ropp* court’s observations, Nesbit clearly intruded upon Baylor’s seclusion when he installed the keylogger on Baylor’s computer.

C. The Installation of a Keylogger on and Subsequent Monitoring of Baylor’s Computer by a Junior Employee Would Be Offensive to a Reasonable Person Subjected to Such an Intrusion.

The common test for judging the offensiveness of an intrusion considers “the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder’s motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.” *Bauer v. Ford Motor Credit Co.*, 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001); *see also Sanchez-Scott v. Alza Pharms.*, 103 Cal. Rptr. 2d 410, 419 (Cal. Ct. App. 2001). Nesbit’s intrusion would be offensive to a reasonable person in light of this evaluation. While Baylor was an executive vice president at ConDevel, Nesbit was a junior employee with little access. (R. at 2.) Yet, Nesbit intruded on Baylor’s private workplace computer, a setting in which Baylor would expect to have almost complete privacy, particularly

from a junior salesperson. Nesbit's keylogger monitored every single keystroke Baylor entered into his computer, amounting to a constant surveillance by Nesbit of Baylor's computer usage. (R. at 3, 4.) While such an action might be reasonable if taken by one's superiors, an executive would find this level of surveillance offensive, objectionable and insulting if committed by such a low-level employee. Nesbit's unauthorized installation of the keylogger was a complete violation of workplace trust and expected privacy and would be offensive to a reasonable person in such a situation.

The offensiveness of Nesbit's intrusion extends beyond the monitoring to the information Nesbit gained by recording Baylor's keystrokes. This information extended to Baylor's private passwords, communications, thoughts, business documents and every other keystroke entered by Baylor. While the intrusion itself is offensive given the circumstances and relationship between Baylor and Nesbit, it is even more offensive when considering the deep and pervasive character of the monitoring and the degree of access Nesbit gained to Baylor's every keystroke.

Moreover, courts have stated that determination of the offensiveness of an intrusion is "ordinarily a question for the fact-finder and only becomes a question of law if reasonable persons can draw only one conclusion from the evidence." *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1008-1009 (N.H. 2003) (finding that the question of the offensiveness of disclosure of Social Security numbers should be left to a jury); *see also Swarthout v. Mut. Serv. Life Ins. Co.* 632 N.W.2d 741, 745 (Minn. Ct. App. 2001). It is certainly reasonable that a jury could find the installation of the keylogger to be offensive to a reasonable person in Baylor's circumstances. Given the relationship between Nesbit and Baylor, there is a genuine issue of material fact as to the offensiveness of the intrusion and summary judgment is therefore improper.

D. Baylor Had an Objectively Reasonable Expectation of Privacy in His Workplace Computer Against Intrusion by Junior Employees.

Courts have recognized that reasonable expectations of privacy vary with the context and circumstances, particularly in the workplace. As one court noted, “whether a person is entitled to solitude of seclusion is a relative and highly fact-dependent matter.” *Jensen v. Sawyers*, 130 P.3d 325, 341 (Utah 2005). The *Jensen* court recognized that “reasonable people may find a legally protectable private environment in a multiple and varied array of physical settings.” *Id.* Privacy may not be absolute in the workplace, but courts have established relational privacy rights in certain situations. *See, e.g., Walker v. Darby*, 911 F.2d 1573, 1579 (11th Cir. 1990) (finding a possible privacy right against electronic recording of conversations by coworkers at a shared workstation); *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976) (finding a right of privacy against coworkers opening personal mail belonging to plaintiff); *Fischer v. Mount Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 928 (W.D. Wis. 2002) (finding a possible privacy right in personal email access); *Doe v. Kohn Nast & Graf, P.C.*, 862 F. Supp. 1310, 1326 (E.D. Pa. 1994) (finding possible intrusion in workplace searches that could reveal personal matters unrelated to employment); *Sanders*, 978 P.2d at 71-79 (finding the possibility of relative workplace aural and visual privacy against certain covert recording by the media); *K-Mart Corp. Store No. 7441 v. Trotti*, 667 S.W.2d 630, 638 (Tex. App. 1984) (finding a privacy right in an employee’s locked locker and personal belongings kept within). These cases closely parallel the type of privacy Baylor expected, demonstrating relative privacy over the types of information and conversations that Nesbit monitored through the use of the keylogger program.

As the cases demonstrate, workplace privacy is a relative concept and depends on a factual analysis of the specific circumstances. In the instant case, while Baylor may not have had an absolute expectation of privacy in his workplace computer and keystrokes as against certain

other employees, he maintained a legitimate expectation of privacy in regards to most employees, particularly junior employees such as Nesbit. Baylor expected that his computer and the keystrokes he entered into it would not be accessed or monitored by anyone without authorization, which Nesbit lacked. Baylor's keystrokes included his private passwords, plainly not intended for disclosure to an employee such as Nesbit, but also likely included personal email, confidential business information, private records, personal thoughts, and other information that Baylor would expect to be kept relatively secret. This Court should follow the common doctrine of relative workplace privacy and recognize the privacy interest Baylor maintained in his computer and keystrokes, particularly against employees such as Nesbit. At the very least, Baylor has established a genuine issue of material fact as to the privacy of his workplace computer in relation to Nesbit's monitoring and this Court should reject summary judgment on that basis.

E. The Intrusion Caused Baylor Suffering and Mental Anguish, Satisfying Even the Restrictive Requirement for the Tort Applied by the First and Second Marshall Circuit Courts.

As noted above, the Restatement and a number of courts do not require plaintiffs to prove any elements beyond an intrusion into private matters that would be offensive to a reasonable person. Courts have often held that a simple violation of the privacy right is presumptively harmful and demands compensation as a matter of law, with additional damages possible for further harm beyond the harm to the privacy interest. *See, e.g., High-Tech Inst., Inc.*, 972 P.2d at 1066; *Snakenberg v. Hartford Cas. Ins. Co.*, 383 S.E.2d 2, 6 (S.C. Ct. App. 1989). Given the importance of the privacy right and the need for protection through state tort law, requiring mental anguish as an element sets too high a bar for recovery by injured plaintiffs. While evidence of mental anguish and suffering may be necessary to establish more substantial damage

awards, the intrusion is damaging in and of itself and should be compensated as such. *See High-Tech Inst., Inc.*, 972 P.2d at 1066; *Sabrina W. v. Willman*, 540 N.W.2d 364, 369-70 (Neb. Ct. App. 1995). This Court should accept the traditional three-prong Restatement test for intrusion upon seclusion and reject the “mental anguish” requirement used by the Marshall circuit courts because the traditional test is more protective of the right of privacy and therefore more fair to those injured.

However, even if this Court chooses to accept the more restrictive “mental anguish” requirement applied by the circuit courts, it is clear that Baylor has stated facts sufficient to create a genuine issue of material fact as to his mental anguish and suffering from the intrusion. Demonstrating mental anguish does not require a showing of physical injury or manifestation. *Fischer v. Hooper*, 732 A.2d 396, 402 (N.H. 1999). Further, expert testimony is not required, as the “mental anguish” element turns purely on the testimony of the plaintiff. *Id.* “The decision of whether to believe the plaintiff’s testimony regarding [his] injuries is fundamentally a question of fact for the jury.” *Id.* As Baylor has pleaded facts regarding his feelings of mental anguish in relation to the intrusion, he has demonstrated genuine issues of material fact that should be put to a jury.

Courts have accepted a wide range of feelings to demonstrate mental anguish, providing numerous examples for this Court to follow. *See, e.g., Tompkins v. Cyr*, 202 F.3d 770, 782 (5th Cir. 2000) (finding plaintiffs’ testimony that they experienced “fear, stress, anxiety, depression, and sadness” sufficient to satisfy the requirement of mental anguish); *Pulla v. Amoco Oil Co.*, 882 F. Supp. 836, 869 (S.D. Iowa 1994) (finding a reasonable jury could find that plaintiff reacted to an intrusion with indignation, humiliation and embarrassment); *Monroe v. Darr*, 559 P.2d 322, 327 (Kan. 1977) (requiring “some evidence to show that [plaintiff] suffered anxiety,

embarrassment, or some form of mental anguish,” even if “skimpy”); *Saint Julien v. S. Cent. Bell Tel. Co.*, 433 So. 2d 847, 853 (La. Ct. App. 1983) (finding plaintiffs’ testimony of fright and mental distress upon discovery that someone had entered their home unauthorized sufficient to satisfy requirement of mental anguish); *Household Credit Servs., Inc. v. Driscoll*, 989 S.W.2d 72, 91 (Tex. App. 1998) (mental anguish includes “grief, severe disappointment, indignation, wounded pride, shame, despair, and/or public humiliation”).

The record demonstrates that Baylor satisfies the requirement of mental anguish as described by various courts. When Baylor learned of the intrusion, he felt “shocked” and suffered anger and embarrassment in the aftermath. (R. at 4-5.) As in *Monroe*, even if the facts pleaded by Baylor are “somewhat skimpy” as to his mental anguish, he has demonstrated suffering in response to the intrusion, at least to the degree necessary to pose a genuine issue of material fact. 559 P.2d at 327. While Baylor certainly suffered from Nesbit’s actions beyond the installation of the keylogger and subsequent monitoring, it is clear that he meets the “mental anguish” requirement necessary to put the facts to a jury.

F. ConDevel Should Be Held Responsible for Nesbit’s Actions Because He Was Acting within the Scope of His Employment When He Installed the Keylogger on Baylor’s Computer.

While ConDevel did not directly intrude upon Baylor’s seclusion, the company should be held liable for Nesbit’s actions as he was seeking to serve ConDevel in his attempt to expose the company’s faulty computer security by installing the keylogger on Baylor’s computer. Courts have held employers liable for the intentional torts of their employees in a number of contexts. *See, e.g., Gonpere Corp. v. Rebull*, 440 So. 2d 1307, 1308 (Fla. Dist. Ct. App. 1983) (holding employer liable for assault and battery); *Plains Res. v. Gable*, 682 P.2d 653, 660-62 (Kan. 1984) (trespass); *Embrey v. Holly*, 442 A.2d 966, 970-72 (Md. Ct. App. 1982) (defamation); *Young v.*

Stensrude, 664 S.W.2d 263, 265-66 (Mo. Ct. App. 1984) (intentional infliction of emotional distress). Similarly, this Court should hold ConDevel responsible for Nesbit’s intrusion upon Baylor’s seclusion.

While it is not clear how the Marshall courts have addressed the issue of employer liability for intentional torts committed by employees acting within the scope of employment, Nesbit’s actions satisfy the two most common approaches utilized in other jurisdictions.

1. Nesbit’s Actions Were within the Scope of His Employment Because He Desired to Serve and Benefit ConDevel When He Installed the Keylogger.

The traditional restrictive test for scope of employment implicates ConDevel in Nesbit’s actions. As an example of this approach, under Illinois law, one court held that an employee’s action is within the scope of employment if: “(1) it is of the kind he is employed to perform; (2) it occurs substantially within the authorized time and space limits; and (3) it is actuated, at least in part by a purpose to serve the master.” *Duffy v. United States*, 966 F.2d 307, 314 (7th Cir. 1992).

Nesbit’s intrusion came at the workplace during work hours. (R. at 3.) Further, Nesbit could have reasonably interpreted ConDevel’s Computer Usage Policy as including some responsibility for general computer security within his broader employment duties. ConDevel employees were given at least some personal responsibility for the security of the computer network. The policy states “employees are responsible for safeguarding all equipment and software provided by the company.” (R. at 2.) While Nesbit’s concerns about the lack of computer security were brushed off by his supervisors and he was told to mind his own business, it is reasonable to believe that he felt that computer security issues were within his general duties to the company. The policy does not explicitly limit employee responsibility to an employee’s personal computer. It would be reasonable for Nesbit to believe that this implied some sort of

general involvement in computer security. While ConDevel never authorized any of Nesbit's actions, his intrusion is sufficiently connected to his general employment for ConDevel to be held responsible for the injuries to Baylor. Finally, Nesbit installed the keylogger and intruded upon Baylor's solitude in an attempt to assist ConDevel with its computer security. (R. at 3.) Nesbit was motivated, at least in part, by his desire to serve ConDevel, thus making ConDevel responsible for his actions. While Nesbit may have had personal motivations as well and later deviated from his initial purpose, the installation of the keylogger falls squarely within the scope of his employment and ConDevel should therefore be held liable for his intrusion upon Baylor's seclusion.

2. Fairness Demands that ConDevel Be Held Responsible for Baylor's Injuries Because Nesbit's Actions Were Closely Related to His Employment and ConDevel Benefited from Those Actions.

The modern scope of employment test asks whether "the tortious conduct of the employee is so closely connected in time, place, and causation to his employment duties as to be regarded as a risk of harm fairly attributable to the employer's business." *Turner v. State*, 494 So. 2d 1292, 1295 (La. Ct. App. 1986). "The rule is a matter of economic and social policy, based both on the fact that the employer has the right to control the employee's actions and that the employer can best bear the loss as a cost of doing business." *Sage Club v. Hunt*, 638 P.2d 161, 162 (Wyo. 1981). Under this rubric, Nesbit's actions fit within the scope of his employment because his intrusion took place at the ConDevel office during work hours and could be considered reasonably related to his employment duties. As noted above, Nesbit could have reasonably interpreted ConDevel's Computer Usage Policy as including some responsibility for computer security within the scope of his general duties. Further, it is more fair that ConDevel bear the cost of the damages inflicted upon Baylor by Nesbit than leave

Baylor without a remedy for Nesbit's intrusion. While ConDevel did not authorize Nesbit's activities and eventually fired him, the company did benefit from Nesbit's keylogger. Nesbit's actions revealed the extent of ConDevel's computer security vulnerabilities and prompted the company to upgrade to prevent further incursions. It would be unfair for ConDevel to receive this benefit while forcing Baylor to suffer uncompensated for the violation of his privacy.

At least one court has noted a recent liberalization in the application of the theory of *respondeat superior* towards greater employer liability. *District of Columbia v. Davis*, 386 A.2d 1195, 1204 (D.C. 1978). In this context, ConDevel should be held responsible for Nesbit's intrusion upon seclusion because Nesbit could reasonably be seen as acting as within the scope of his employment under either test. In any case, whether an employee was acting within the scope of his employment is a question of fact properly left to a jury. *Los Ranchitos v. Tierra Grande, Inc.*, 861 P.2d 263, 267 (N.M. Ct. App. 1993) ("Whether an employee's actions come within the scope of employment is generally a question of fact to be determined on a case-by-case basis."); *Baker v. Saint Francis Hosp.*, 126 P.3d 602, 606 (Okla. 2005) ("The question of whether or not a servant should be considered to have been acting within the line of duty . . . is normally a question of fact to be determined by the jury from all the surrounding circumstances.") Given Nesbit's initial desire to improve ConDevel's computer security and his reasonable interpretation of ConDevel's Computer Usage Policy, there are genuine issues of material fact as to whether Nesbit was acting within the scope of his employment and summary judgment is therefore inappropriate in this case.

II. CONDEVEL VIOLATED THE MARSHALL DATA PROTECTION ACT WHEN IT FAILED TO NOTIFY BAYLOR OF THE DATA SECURITY BREACH.

A. The Unambiguous Plain Meaning of the Marshall Data Protection Act’s Text Required ConDevel to Notify Baylor of the Data Security Breach.

The United States Supreme Court has stated “[t]he starting point for our interpretation of a statute is always its language.” *Cnty. for Creative Non-Violence v. Reid*, 490 U.S. 730, 739 (1989). It is therefore appropriate to look first at the text of the Marshall Data Protection Act (“the Act”) to determine whether ConDevel is liable for failing to notify Baylor of the breach of data security. Subsections (a) and (b) of the Act require notification, at a minimum “without unreasonable delay,” subject to the needs of law enforcement agencies as laid out in subsection (c) and a good faith exemption laid out in subsection (d). 17 Marshall Code § 105 (2006). Subsection (g) provides private citizens the right to “a civil action against any data collector that obfuscates evidence of a breach or makes an informed choice not to inform data subjects of a breach.” 17 Marshall Code § 105 (g) (2006). This section gives Baylor a claim under the Act because ConDevel made an “informed choice not to inform” Baylor of the data security breach after the technology support department learned of Nesbit’s actions. (R. at 5.)

The Act requires notification in case of a breach of security such as the one perpetrated by Nesbit. Subsection (a) of the Act requires agencies having control over computerized data containing personal information to provide “notification of the breach in the security of the data to any resident of Marshall whose unencrypted personal information was . . . acquired by an unauthorized person.” 17 Marshall Code § 105 (a) (2006). Here, it is undisputed that Baylor’s unencrypted personnel file was acquired by Nesbit. (R. at 4.) Nonetheless, ConDevel argues that it was exempt from the Act because, Nesbit being an employee, there had not been a true data breach and therefore it was within its discretion to notify its employees. (R. at 5, 7.)

However, “breach of the security of the system” is defined in the Act as “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.” 17 Marshall Code § 105 (d) (2006). Because the text of the statute precisely defines “breach of the security of the system,” it was not within ConDevel’s power to make its own decision about the existence of a breach without regard for the plain meaning of the Act. *Id.* Notification is a statutory requirement triggered by a breach as defined by the Act, and the text of the statute does not leave this determination up to the discretion of the company.

1. A Breach of Security Occurred When Nesbit Downloaded the Personnel Files onto His Home Computer Because He Was Not Authorized to Acquire the Data and the Data Acquired Contained Personal Information.

While “breach of the security of the system” is defined in the Act, ConDevel may argue that two terms within that definition do not apply to the situation at hand. In order for the Act to apply to ConDevel, first the term “unauthorized” must apply to Nesbit and his actions, and second, the data acquired by Nesbit must qualify as “personal information.”

When interpreting the meaning of terms, “[a] fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.” *Perrin v. United States*, 444 U.S. 37, 42 (1979). Furthermore, when a term is undefined in a statute, but has a well-established meaning under the common law, the court must assume that the common law meaning is meant to be used. *Cnty. for Creative Non-Violence v. Reid*, 490 U.S. 730, 739 (1989). It is therefore appropriate to look to contemporary usage and the common law meaning of these terms when determining their definitions.

The term “unauthorized” as used in the Act applies to Nesbit’s acquisition of the personnel files. “Unauthorized” is generally defined as “done without authority.” Black’s Law Dictionary (8th ed. 2004). “Authority” is further defined as “the right or permission to act legally on another’s behalf . . . in accordance with the other’s manifestations of assent.” *Id.* Actual authority exists when the authority is intentionally given or the agent reasonably believes, based on dealings with the principal, that the authority exists. *Id.* Authority may be “express” (given by explicit agreement) or “implied” (intentionally given as the result of the principle’s conduct). *Id.*

Because ConDevel asserts that the data were “obtained by an employee for the purposes of testing the system security,” it is essentially arguing that Nesbit’s actions in downloading the human resources database files were not “unauthorized” within the meaning of the statute. (R. at 7.) However, Nesbit was a sales associate and had not been assigned to investigate the security of the company’s computers. In fact, he had been specifically told not to work on technological issues. (R. at 3.) Nesbit’s acquisition of the human resources database files cannot qualify as authorized because he was not employed in either the human resources or technology support departments. Further, ConDevel does not claim that Nesbit had been assigned to download the files onto his home computer. Therefore, because ConDevel did not explicitly agree to Nesbit’s downloading of the personnel files, Nesbit could not have had express authority. Based on dealings with his supervisor in which he was repeatedly told to “leave technological issues to the technology support department,” Nesbit could not reasonably have believed that he had authority to download the personnel files. (R. at 3.) Thus, ConDevel also cannot convincingly argue that it had given Nesbit implied authority to acquire the data when it had specifically instructed Nesbit not to work on technology issues.

ConDevel may argue that its Computer Usage Policy (“the Policy”) stating “employees are responsible for safeguarding all equipment and software provided by the company” constituted authorization for Nesbit to conduct his test of the security of the system. (R. at 2.) While Nesbit may reasonably have believed that the Policy gave him some responsibility for computer security, it did not extend authorization to Nesbit’s acquisition of the human resources database files. According to the Restatement (Third) of Agency, authority to take action depends on “the agent reasonably understand[ing] the principal’s manifestations and objectives.” Restatement (Third) of Agency § 2.02 (2006). It goes on to state that the understanding is considered “reasonable if it accords with the principal’s manifestations and the inferences that a reasonable person would draw from the circumstances creating the agency.” *Id.* Nesbit was initially very enthusiastic about helping ConDevel by testing the security of the computer system, and because of his technological background he may reasonably have thought the Policy gave him an excuse to conduct the test. Nevertheless, to extend this understanding to include acquisition of all human resources database files is unreasonable. Nesbit had enough proof of the weaknesses in ConDevel’s computer security system with the information he acquired through the keylogger program, and he did not need to actually download the files in order to make a convincing report to the company. Any reasonable employee interpreting the Policy would understand the contradiction between pursuing the objective of “safeguarding all equipment and software” and compromising the personal information of his colleagues.

Further, because Nesbit was hired to work in the sales department, it is not reasonable to infer that he was authorized to acquire the human resources database files, especially in light of his entry-level status. “The test [of authority] is . . . whether such a power usually accompanies, is integral to, or is reasonably necessary for the due performance of the task.” *United States v.*

Flemmi, 225 F.3d 78, 86 (1st Cir. 2000). In *Flemmi*, the court found that FBI agents lacked the authority to grant immunity to an informant because the connection between granting immunity and their authority to investigate crimes was “far too attenuated.” *Id.* Here, because Nesbit was hired as a sales agent and was not employed in the human resources or technology support departments, the connections between his duties in sales and his actions in downloading the files to his home computer are likewise “far too attenuated” to be accepted as authorized.

In *Int’l. Airport Ctrs., L.L.C. v. Citrin*, an employee’s authorization to access his laptop was found to have terminated when he engaged in misconduct. 440 F.3d 418, 420-21 (7th Cir. 2006). Judge Posner noted:

[The] breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of the authority had been that relationship. Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship. Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.

Id. at 420-21 (internal citations omitted). Here, Nesbit’s interests became adverse to ConDevel once he decided to download the personnel files for his own personal use. ConDevel was unaware of these adverse interests at the time Nesbit acquired the files, and therefore even if this Court finds that Nesbit had some authority to generally test the system, that authority ceased to exist before the data breach occurred. *See also Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (employees were without authorization to access computers after they developed interests adverse to the employer).

In addition to these strong indications that Nesbit was not actually authorized to acquire the human resources database files, the fact that ConDevel fired Nesbit when it discovered what he had done makes it very hard to claim that Nesbit’s actions were authorized. If it was true that

Nesbit had been authorized to acquire the personal information of all employees, the only reason to have fired him for doing so would be if ConDevel thought he had used this information for an improper purpose. In that case, even a good faith acquisition is a breach under the statute because the exemption only applies “provided that the personal information is used for purposes designated by the agency.” 17 Marshall Code § 105 (d) (2006).

Looking to a contemporary statutory definition of the term, Maine, in its equivalent statute, defines “unauthorized person” as “a person who does not have authority or permission of a person maintaining personal information to access personal information maintained by the person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.” Me. Rev. Stat. Ann. tit. 10, § 1347 (2005). Here, Nesbit did not have authority within the scope of his sales position to access the human resources database files, regardless of whether he may reasonably have believed he was within the scope of his employment in testing the computer security system with the keylogger. There is also no evidence that Nesbit had permission from Baylor or anyone else to access the personnel files maintained by the human resources department. Additionally, the manner in which Nesbit conducted the installation of the keylogger, including the use of an outside email address to make him harder to catch, demonstrates his use of subterfuge that led to his acquisition of the personal information. Thus, as Nesbit qualifies as an “unauthorized person” under this contemporary definition in a similar statute, he also should be held unauthorized here.

At the very least, the extent of Nesbit’s authorization presents an issue of fact that should be decided by a jury. In addressing whether a defendant’s authority to pick up and hold his mother’s mail extended to the opening and using of that mail, the court in *United States v. Hill*, noted that deciding on “a specific degree of authority for an agent . . . would lead to intricate

factual inquiries as to the degree of authority granted and the amount of control exercised by the agent.” 579 F.2d 480, 482 (8th Cir. 1978). Thus, if there is an interpretation of Nesbit’s actions that could qualify them as “unauthorized,” a genuine issue of material fact exists and summary judgment in this case is inappropriate.

In addition to Nesbit being unauthorized, the files he acquired contained personal information. “Personal information” is not defined in the Act, but under any contemporary definition, the data contained in the personnel files, including Social Security and driver’s license numbers, would qualify. Both Illinois and California have similar statutes, and both define “personal information” as including, *inter alia*, “an individual’s first name or first initial and last name in combination with any one or more of the following data elements . . . (1) Social Security Number. (2) Driver’s license number.” Cal. Civ. Code § 1798.80 (2006); 815 Ill. Comp. Stat. 530/5 (2005). In addition, Nesbit obtained nonpublic information such as performance evaluations, salary data, benefits information and employee awards and honors of every ConDevel employee when he downloaded all the personnel files to his home computer. (R. at 2, 4.) This sensitive information reasonably could be considered “personal information” in and of itself, but in any case, because Nesbit also obtained the names, Social Security numbers, and driver’s license numbers of each employee when he downloaded the personnel files, this information is unquestionably included in the definitions provided by equivalent statutes. (R. at 2, 4.)

In similar statutes that do define “personal information,” “publicly available information” is excepted from the definition, presumably because if the information is available in some other easily accessible form no harm has been done by its disclosure. *See* Cal. Civ. Code § 1798.81.5 (2006); 815 Ill. Comp. Stat. 530/5 (2005). It is not clear from the record whether Nesbit needed

to use Baylor's Social Security number or driver's license number in order to have the club memberships issued. However, the breach occurred when Nesbit downloaded the personnel files to his computer, before he used any of the information. Since the downloaded information did contain Social Security and driver's license numbers along with other sensitive information, Nesbit acquired personal information under the meaning of the Act.

2. The Good Faith Exception to the Notification Requirement in the Statute Does Not Apply to ConDevel Because Nesbit Was Not Acting in Good Faith and the Acquired Information Was Not Used for Purposes Designated By ConDevel.

ConDevel is not exempt from the Act because Nesbit was not acting in good faith. "Good faith" is defined as "a state of mind consisting in (1) honesty in belief or purpose . . . or (4) absence of intent to defraud." Black's Law Dictionary (8th ed. 2004). As one federal court noted, "[s]ummary judgment is notoriously inappropriate for determination of claims in which issues of intent, good faith and other subjective feelings play dominant roles." *Pfizer, Inc. v. Int'l Rectifier Corp.*, 538 F.2d 180, 185 (8th Cir. 1976). Furthermore, in deciding on a summary judgment motion, the record must be viewed in the light most favorable to the party opposing the motion. *See Poller v. Columbia Broad. Sys., Inc.*, 368 U.S. 464, 472 (1962).

Here, the facts going to the timing of Nesbit's actions are not in dispute. Nesbit did start the project in good faith, because his initial intent was to help ConDevel. However, he had a change of heart before he downloaded the human resource database files to his home computer when he realized he could use the VIP Program for his own benefit. (R. at 4.) At that point he was no longer in a state of mind that was honest in purpose, and he had fully developed his intent to defraud the benefits system. (R. at 4.) This downloading of the database was the "acquisition of personal information" that constituted the breach. Because the facts regarding the timing of Nesbit's actions are undisputed, it must be assumed for the purposes of summary judgment that

Nesbit lacked good faith at the time he acquired the personnel files. If Nesbit lacked good faith, ConDevel cannot benefit from the good faith exemption to the disclosure requirement set forth in the Act. However, even if the timing or purpose of his actions are susceptible to interpretation, this presents a genuine issue of material fact. Because the presence or absence of good faith is a question of fact that should be put to a jury, summary judgment is inappropriate. *See Pfizer*, 538 F.2d at 185.

Even if the acquisition is somehow found to be in good faith, the exception does not apply because the information was not used for purposes designated by the agency. The Court of Appeals agreed with ConDevel's statement that Nesbit's use of the data was "within, or in compliance with, the Company's scopes and purposes." (R. at 7.) While it may be possible to argue that on a very general level, the personal information is used by ConDevel to set up employee benefits, and that Nesbit's use of that information for that purpose was thus somehow "in compliance with the Company's scopes and purposes," this language is much broader than that of the statute and is not supported by the plain text. On the contrary, the statute says that in order to qualify for the good faith exemption the information may only be used for "purposes designated by the agency." 17 Marshall Code § 105 (d) (2006). ConDevel's benefits policy is intended to "attract and foster loyalty among top executives" by rewarding employees based on their rank, seniority, and salary. (R. at 2.) Nesbit's use of Baylor's information to circumvent this policy and gain access to benefits not available to employees of his rank cannot reasonably be considered to be a purpose designated by ConDevel. Here, the record must be viewed most favorably to Baylor in deciding to grant summary judgment, thus if the interpretation of whether the data were used for purposes designated by the agency is at all ambiguous it presents a genuine issue of material fact and should be left to the jury. *See Poller*, 368 U.S. at 473 (1962).

B. The Purpose of the Marshall Data Protection Act Is to Protect Individuals Like Baylor and Apply to Companies Like ConDevel.

An examination of the history and purpose of the Act and similar state laws supports the contention that the statute should apply to ConDevel and reinforces the plain meaning of the statute. “Examination of purpose is a staple of statutory interpretation that makes up the daily fare of every appellate court in the country.” *McCreary County, Ky. v. Am. Civil Liberties Union of Ky.*, 545 U.S. 844, 861 (2005). “[S]crutinizing purpose does make practical sense . . . where an understanding of official objective emerges from readily discoverable fact.” *Id.* at 862. In *Edwards v. Aguillard*, which examined a state law requiring the teaching of both creationism and evolution, the Court stated that it is appropriate to consider the “historical context” and “the specific sequence of events leading to [its] passage” in determining a statute’s purpose. 482 U.S. 578, 595 (1987). Here, the historical context and legislative history of similar state data breach notification statutes indicate the Marshall legislature intended for the Act to apply to ConDevel in this situation.

1. The ConDevel Breach is Just One of Many Recent Data Security Breaches that Have Demonstrated the Burgeoning Problem of Identity Theft.

Identity theft is one of the fastest growing crimes in the United States. Amanda Draper, Comment, *Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law*, 40 J. Marshall L. Rev. 681, 682 (2007). The Act and other data breach notification laws are part of a “broader effort” to address this problem. Bruce E. H. Johnson & Kaustuv M. Das, *Data Breach Notice Legislation: New Technologies and New Privacy Duties?*, 865 PLI/Pat 203 (2006). Identity theft occurs when someone “uses another person’s personal information to commit fraud.” Draper, *supra*, at 682-83. The term “personal information” typically includes data such as an individual’s name, Social Security number, birth date, or

driver's license number. Draper, *supra*, at 682-83. Identity theft can have “devastating consequences” for its victims and has been compared to contracting a chronic disease. *Id.* at 684; Michael Sivy et al., *What No One Is Telling You About Identity Theft*, Money, July 2005, at 95-99. In 2003, the Federal Trade Commission estimated that victims of identify theft spent an average of \$500 and 30-60 hours to clean up the direct damage caused, not including emotional distress or effort expended to resolve related problems. S. Kasim Razvi, *To What Extent Should State Legislatures Regulate Business Practices as a Means of Preventing Identity Theft?*, 15 Alb. L.J. Sci. & Tech. 639, 640-41 (2005).

Here, Baylor has suffered all of the trappings of identity theft. Nesbit impersonated him and took advantage of the club memberships and other amenities that Baylor is entitled to as an executive vice president of ConDevel. Moreover, because Nesbit's bad behavior got Baylor blacklisted at the Marshall League Club and several other establishments, Baylor has been deprived of a significant social, financial, and employment benefit. Further, Baylor endured the kind of emotional distress described above, in that he was “deeply embarrassed and angry” over his revoked membership at the Shady Links golf club and had a “heated argument” with the manager of Les Deux Pommes restaurant. (R. at 4, 5.) He has had to expend significant time deducing what happened to his identity, especially since ConDevel did not share the results of its investigation. (R. at 5.) Even more devastating, it will likely take a long time to regain good standing at these exclusive establishments and ConDevel has not offered to help. (R. at 5.)

The ConDevel incident is just one of many instances across the country of a bad actor gaining access to sensitive information contained in institutional databases. From February 2004 to March 2005, someone stole the credit card information of 1.4 million customers from the database of shoe-seller DSW, Inc. John B. Kennedy, *Slouching Towards Security Standards:*

The Legacy of California's SBI386, 865 PLI/Pat 91, 97 (2006). In February 2005, Bank of America lost computer tapes containing the records of 1.2 million customers, and a laptop with information on 100,000 students, alumni, and applicants was stolen from the University of California, Berkeley. *Id.* In March, someone used stolen passwords to gain access to personal information of 32,000 Lexis-Nexis customers. *Id.* In June, CardSystems Solutions suffered a breach, giving unauthorized access to the credit card records of 40 million customers. *Id.*

The incident at ConDevel is no different, and no less serious, than these high profile security breaches. ConDevel collects and maintains a database of electronic employee personnel files. (R. at 2.) These files contain sensitive data such as contact information, Social Security numbers, and driver's license numbers. (R. at 2.) This is the type of information that has been stolen and used to commit identity theft and that commentators and privacy experts have been concerned about securing. *See Draper, supra*, at 681, 684-86; *see also* David Eggleston, *Privacy Issue as Serious as Y2K: Expert*, Strategy Magazine, September 13, 1999, at D 11 (discussing the need to pay attention to privacy issues to gain consumer confidence and comply with government regulation). Moreover, it is precisely the kind of information that laws like the Act are designed to protect. One consumer advocate theorized "forcing firms to admit to serious data security breaches might embarrass them into beefing up their protections." Sivy, *supra*, at 98.

2. The Legislative History of the California Model Statute Demonstrates Lawmakers Were Attempting to Prevent Identity Theft and Intended the Law to Apply to Companies Like ConDevel.

Legislative history should be relied upon in construing the Act because "[i]n determining the meaning of the statute, we look not only to the particular statutory language, but to the design of the statute as a whole and to its object and policy." *Crandon v. United States*, 494 U.S. 152, 158 (1990). Moreover, "When possible, every statute should be rationally interpreted with the

view of carrying out the legislative intent.” *Gulf States Steel Co. v. United States*, 287 U.S. 32, 45 (1932).

The history and commentary from the strikingly similar statutes of other states indicate their collective intention was to protect individuals from identity theft by enacting a robust notification requirement. Courts have endorsed the practice of examining similar laws from other jurisdictions and their accompanying legislative histories when construing a statute’s meaning. *See State v. Mitchell*, 563 S.W.2d 18, 24 (Mo. 1978) (finding it appropriate to consider the legislative history of the federal Comprehensive Drug Abuse Prevention and Control Act of 1970 because the Missouri legislature did not provide legislative history for the state Narcotic Drug Act patterned after the federal law); *see also Times Mirror Co. v. Superior Court*, 813 P.2d 240, 247 (Cal. 1991) (stating that the legislative history of the Freedom of Information Act could “serve to illuminate” their interpretation of the California Public Records Act). Here, because there is no reported legislative history available for the Act, it is appropriate to examine the history of the California statute, which is recognized as the model for data breach notification laws across the country. Satish M. Kini & James T. Shreve, *Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches*, 10 N.C. Banking Inst. 87, 88 (2006).

In 2003, California passed the country’s first data breach notification statute. Kristen Mathews, *Data Security Breach Notification: Complying with State Laws; Still Awaiting Pending Federal Legislation*, 1 No. 4 Privacy & Data Protection Leg. Rep. 3 (2006). This statute, the Security Breach Notification Act, California Civil Code § 1798.80 *et seq.*, is nearly identical to the Marshall Data Protection Act. *Comp. Cal. Civ. Code § 1798.82, with 17*

Marshall Code §105 (2006). It is also particularly relevant because, like the Marshall Act, the California law grants individuals a civil cause of action. *Id.*; Johnson & Das, *supra*, at 219, 221.

The bills that led to the California statute, Assembly Bill 700 and Senate Bill 1386, went through some notable changes during the amendment process. For example, the notification provision was originally triggered when an unauthorized person “accessed” personal information, but it was then changed to read “acquired.” Assemb. B. 700, 2001-02 Reg. Sess. (Cal. 2002) (as amended in Senate, August 22, 2002). This recognized the reality that an employee who inadvertently or briefly glimpsed personal information did not pose a risk to that data, and thus did not necessitate notification. *Analysis of Assemb. B. No. 700 Before the Cal. S. Privacy Comm.*, 2001-02 Reg. Sess, at 7-8 (August 21, 2002) [hereinafter *Bill Analysis*].¹

More important, however, was the catalyzing event that illustrated the need for data protection laws. The *Bill Analysis* described a 2002 data breach at the Stephen P. Teale Data Center, where hackers illegally acquired the sensitive personal information of approximately 265,000 state workers. *Id.* at 2. The breach was not discovered for a month and employees were not notified for a full six weeks; in the meantime unauthorized persons made at least two attempts at identity theft. *Id.* Indeed, for a few rounds of amendments the senate bill contained language declaring it an “urgency statute” that needed to take effect immediately, specifically because of the incident at the data center. S.B. 1386 §5, 2001-02 Reg. Sess. (Cal. 2002) (as amended in Assembly June 30, 2002).

The ConDevel incident is analogous to the breach that occurred at the Teale facility. Both databases held personal employee information and were breached by unauthorized persons. Employees did not discover the breaches immediately; at Teale, it took nearly a month, at

¹ Available at http://www.leginfo.ca.gov/pub/0102/bill/asm/ab_06510700/ab_700_cfa_20020821_093035_sen_comm.html.

ConDevel, about six weeks. *Bill Analysis* at 2; (R. at 3, 5.). However, while it appears that the security lapse was discovered at Teale before any real damage was done, ConDevel did not discover its breach until after Nesbit stole Baylor's identity and damaged his reputation. The ConDevel incident is even more serious than the Teale breach because here, the unauthorized acquisition of personal information caused actual damages to an employee. The damage to Baylor was compounded by ConDevel's failure to disclose the incident.

The California *Bill Analysis* also described another contemporary breach and noted that the latter company's subsequent, voluntary notification of affected consumers was "a practice this bill seeks to encourage." *Bill Analysis* at 3. However, the *Bill Analysis* lamented, "not all companies are as forthcoming." *Id.* at 7. It thus outlined a final reason for the bill: "Forewarned is forearmed against identity theft" and stated "[a]ll too often events of this sort go completely unreported" because the potential embarrassment or fear of lost business takes corporate precedence over the needs of the affected individuals. *Id.*

Here, ConDevel is exactly the kind of company the California Legislature referred to in the *Bill Analysis*, and the incident is precisely of the type the Legislature sought to address. Rather than being forthcoming about Nesbit's actions, ConDevel management's primary concern was that "news of this incident could harm ConDevel's reputation." (R. at 5.) Indeed, the chief operating officer actively attempted to prevent the breach from becoming public, something section 105(g) of the Act specifically prohibits. *See* 17 Marshall Code § 105(g) (2006). His voice mail message to the director of the technology support department shows he knew about the breach and intended to cover it up, for he stated that, "no one knows that this ever happened. Let's keep it that way. The last thing we need right now is a lawsuit or a scandal. We can't afford losing our good name and our clients." (R. at 5.) As this message makes clear, ConDevel

feared for its reputation and made a conscious decision to keep the breach quiet. This is the very kind of corporate secrecy that statutes like the Marshall Data Protection Act seek to stop.

3. The ChoicePoint Breach Showed the Efficacy of the California Statute and Spurred Other States to Pass Similar Laws to Promote Notification and Prevent Identity Theft in Their States.

A watershed moment in data breach notification laws occurred in February of 2005 when data aggregating company ChoicePoint notified 35,000 Californians that it had inadvertently sold their personal information to data thieves. Norbert F. Kugele & James Placer, *Navigating Some Uncertain Waters in Michigan's New Security Breach Notification Law*, Privacy & Data Security L. 2007.07-5 (2007). Many commentators credit the California law with this revelation and one has posited “[w]e wouldn’t even know about these data security breaches if it weren’t for the pioneering efforts of California.” Edmund Mierzwinski, *Testimony of Consumer and Privacy Groups on Data Security, Data Breach Notices, Privacy and Identity Theft*, 1533 PLI/Corp 333, 338 (2006) (excerpting testimony from the Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft before Committee on Banking, Housing, and Urban Affairs); *see also* Ian C. Ballon, *A Legal Analysis of State Security Breach Statutes*, 903 PLI/Pat 135, 137 (2007); Daniel J. Solove & Chris Jay Hoofnagel, *A Model Regime of Privacy Protection*, 2006 U. Ill. L. Rev. 357, 373 (2006). In addition to notifying California residents, ChoicePoint acceded to the pressure of the Attorneys General in 19 states, eventually notifying all affected persons nationwide and admitting that 163,000 records were involved. Kugele & Placer, *supra*, at 1; Kini & Shreve, *supra*, at 87.

As a result of the ChoicePoint revelations, as well as many other reported data security breaches in 2005, twenty-three states passed laws modeled on the California statute that year. Kini & Shreve, *supra*, at 92-94. As of July 2007, thirty-five states have passed data breach

notification laws. Kugele & Placer, *supra*, at 1. Some state laws include legislative findings recognizing timely notification as an important component to preventing identity theft and demonstrating their intent to protect the personal information of their citizens. For example, the Georgia legislature stated “[v]ictims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative.” Ga. Code Ann. § 10-1-910 (2007). *See also* La. Rev. Stat. Ann. § 51:3072 (2007); Mont. Code Ann. § 30-14-1701 (2005) (stating its purpose is “to enhance the protection of individual privacy and to impede identity theft”).

Here, the Act requires notification independent of any judgment by the data holder as to whether the breach poses a risk of harm (a “harm trigger”). *See* 17 Marshall Code §105(a) (2006); *see also* Kathryn E. Picanso, Note, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 Fordham L. Rev. 355, 383 (2006). Consumer advocates have pointed out that this requirement is the best way to eliminate the inherent conflict of interest companies have if given the discretion to decide whether notice is required, while at the same time standing to benefit by keeping the breach secret. Mierzewski, *supra*, at 351. As one commentator noted “[w]hen businesses know that they must tell consumers about every security breach . . . they may choose to invest more in data security, preventing more breaches.” *Id.*

ConDevel demonstrated exactly this conflict of interest, in that the company chose to protect its reputation rather than inform its employees about unauthorized acquisition of their personal information. This is the kind of behavior the data breach notification laws were designed to prohibit, and allowing it would defeat the plain meaning of the statute and the policy adopted by the State of Marshall when it passed the Act without a harm trigger. This Court should hold that the Act applies to ConDevel because enforcement will make companies like

ConDevel less likely to keep breaches secret. It will also give companies an incentive to continue tightening security and prevent embarrassing data breaches in the first place.

4. The Structure of the Marshall Data Protection Act Further Shows Its Purpose Is to Discourage Corporate Secrecy When Personal Information Has Been Acquired by Unauthorized Individuals.

The Act takes intentional failure to report data breaches very seriously. In section (g)(1), the cap on monetary damages is an astonishingly high \$100,000 per plaintiff. 17 Marshall Code §105(g) (2006). The Act also allows punitive damages of up to \$30 million for a “deliberate and malicious” violation. 17 Marshall Code §105(g)(3) (2006). Compared to other data breach notification statutes that allow civil causes of action, the State of Marshall seeks to restore affected individuals completely and punish violators harshly. *Comp.* 17 Marshall Code §§ 105(g)(1), 105(g)(3) (2006), *with* Cal. Civ. Code § 1798.84(b) (2006) (permitting up to \$3000 for “willful, intentional, or reckless” violation); La. Rev. Stat. Ann. § 51:3075 (2007) (providing for actual but not punitive damages); Tenn. Code Ann. § 47-18-2107(g) (2007) (requiring injury and not providing for punitive damages); Wash. Rev. Code § 19.255.010(10)(a) (2007) (no punitive damages and notification not required where criminal activity is unlikely). As these amounts demonstrate, the Marshall Legislature intended to encourage compliance with the statute and did not intend to let violators off lightly. Moreover, the Act does not require a demonstration of injury to state a cause of action; injury is presumed from a violation of section (g). *See* 17 Marshall Code § 105(g) (2006).

As previously discussed, Nesbit’s actions constituted a “breach of the security system” under the meaning of the Act. At the very least, whether Nesbit acted in good faith is a question for a jury, and therefore summary judgment for Appellee was inappropriate. Because this is precisely this kind of breach the Act intended to be made public and because ConDevel made an

informed choice not to notify Baylor and other ConDevel employees of the breach, Appellant respectfully requests this Court reverse the decision of the Fourth Circuit Court of Appeals for the State of Marshall and remand this case for trial.

CONCLUSION

Nesbit intruded upon Baylor's seclusion when he installed a keylogger on Baylor's computer, violating Baylor's relative workplace privacy in an offensive manner and causing Baylor mental anguish. ConDevel should be held responsible because Nesbit was acting within the scope of his employment. Additionally, ConDevel's failure to inform Baylor of the breach of security was a violation of the Marshall Data Protection Act according to the statute's plain text and purpose. At the very least, Baylor has presented genuine issues of material fact as to the intrusion and violation of the statute, both of which should properly be put before a jury. For the foregoing reasons, Baylor respectfully requests this Court reverse the Court of Appeals' decision and remand this case to the district court for trial.

Dated : September 24, 2007

Respectfully Submitted,

Team 7, Attorneys for Appellant