The John Marshall Journal of Information Technology & Privacy Law

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

Article 7

Spring 2008

The Twenty-Sixth Annual John Marshall International Moot Court Competition in Information Technology and Privacy Law: Brief for the Respondent, 25 J. Marshall J. Computer & Info. L. 371 (2008)

Stacy Appleton

Adam Butkus

Nick Mutton

Recommended Citation

Stacy Appleton, Adam Butkus & Nick Mutton, The Twenty-Sixth Annual John Marshall International Moot Court Competition in Information Technology and Privacy Law: Brief for the Respondent, 25 J. Marshall J. Computer & Info. L. 371 (2008)

BRIEF FOR THE RESPONDENT

No. 2007-CV-315

IN THE
SUPREME COURT OF THE STATE OF MARSHALL
FALL TERM 2007

RON BAYLOR,
Petitioner,
v.
CONDEVEL, INC.,
Respondent.

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

BRIEF FOR RESPONDENT

Stacy Appleton
Adam Butkus
Nick Mutton

QUESTIONS PRESENTED

I. Whether Baylor stated a claim for intrusion upon seclusion against ConDevel when its employee, Nesbit, without authorization surreptitiously installed a keylogger program on Baylor's computer, accessed corporate personnel files, and used the information for his personal benefit.

II. Whether ConDevel was exempt from the disclosure requirements of Marshall's Data Protection Act when Baylor knew about an unauthorized acquisition of computerized data, Nesbit acquired the data to protect ConDevel's computer system, and no one outside the company accessed the information.

TABLE OF CONTENTS

OPINIONS BELOW

In case number CV-06-0326, the Grant County District Court granted summary judgment in favor of the Respondent, ConDevel, Inc. In case number 2006-CV-0326, the Fourth Circuit Court of Appeals of the State of Marshall affirmed the district court's order granting summary judgment.

STANDARD OF REVIEW

The standard of review of a lower court's grant of summary judgment is de novo. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). The evidence must show no genuine issue of material fact and that the movant is entitled to judgment as a matter of law. Marshall R. Civ. P. 56(c).

STATEMENT OF THE CASE

I. Statement of the Facts

Respondent, ConDevel, Inc. ("ConDevel"), is a leading real estate construction and development business in Marshall. (R. at 1) ConDevel provides its executives certain privileges or "perks" through its longstanding "VIP Program." (R. at 2) Implemented "to attract and foster loyalty among top executives," the program is designed to allow executives to obtain memberships to a number of exclusive clubs. (R. at 2) ConDevel awards these privileges based on an employee's rank, seniority, and salary. (R. at 2)

Petitioner, Ron Baylor ("Baylor"), is an executive vice president for ConDevel. (R. at 2) Baylor oversees the sales, operations, and human resources departments. (R. at 2) Consequently, Baylor can access all ConDevel employees' electronic personnel files. (R. at 2) These files include "employee contact information, social security numbers, drivers license numbers, employee performance evaluations, employee salary data, employee benefits information, employee awards and honors, and other personal data." (R. at 2)

Steve Nesbit ("Nesbit") was one of Baylor's subordinates who worked at ConDevel as a sales associate. (R. at 2) In his free time, Nesbit enjoyed many forms of high-tech entertainment and gained extensive knowledge of computer vulnerabilities. (R. at 2) As such, Nesbit became frustrated by what he saw as ConDevel's refusal to upgrade its technological equipment and security. (R. at 3) On several occasions, Nesbit told his supervisor that he believed ConDevel's computer infrastructure was vulnerable. (R. at 3) However, his supervisor told to mind his own business and leave technological issues to the technology support department. (R. at 3)

Nevertheless, motivated by his desire to act as a team player and problem solver, Nesbit devised a plan to raise the company's awareness of its computer vulnerabilities. (R. at 3) Nesbit created a keylogger program, which would allow him to "discover user names, passwords, and any other information entered via the target computer's keyboard." (R. at 3) Nesbit planned to fully report to corporate management any documented computer vulnerabilities. (R. at 3)

On April 25, 2005, Nesbit seized an opportunity to implement his plan. (R. at 3) Despite ConDevel's Computer Usage Policy holding employees "responsible for safeguarding all equipment and software," (R. at 2), Baylor left his office in a hurry, leaving his computer on and unattended. (R. at 3) While Nesbit had not targeted Baylor specifically, he installed his program on Baylor's computer. (R. at 3) Subsequently, Nesbit received information sent to his private e-mail address via the keylogger program, which enabled him to acquire Baylor's login and passwords. (R. at 4) For the specific purpose of identifying ConDevel's computer weaknesses for company management, Nesbit used this information to access the human resources database that contained employee personnel files. (R. at 4)

After Nesbit acquired "the personally identifiable information of every employee, including Baylor," he "had a change of heart." (R. at 4) Being an ambitious young man, Nesbit once remarked that he "wonder[ed] if there is another way to enjoy the good life reserved to the executives." (R. at 2) Thus, when Nesbit discovered he acquired access to business files related to the "VIP Program," he became fascinated with the benefits and decided to use the information he obtained for his own benefit. (R. at 4) He then downloaded the human resources files on his home computer. (R. at 4)

Noticing Baylor had not used many of the benefits awarded to him, Nesbit had several credentials for exclusive clubs issued to Baylor, but sent to his own address. (R. at 4) These credentials included a membership card to the Marshall League Club ("the Club"), where Nesbit began frequenting under Baylor's name. (R. at 4) On May 25, 2005, Nesbit became extremely intoxicated and fought with a prominent Club member. (R. at 4) The Club's security physically removed Nesbit from the premises and suspended Baylor's membership. (R. at 4) Subsequently, many exclusive establishments effectively blacklisted Baylor upon learning of his suspended membership with the Club. (R. at 4)

On June 1, 2005, Baylor began to suspect that someone misused his personal information. (R. at 4) When he took some friends to play golf, Baylor learned that the golf club revoked his membership due to his behavior at the Club. (R. at 4) However, Baylor never joined the Club and had not gone there in years. (R. at 4) The following week, an upscale restaurant denied Baylor a table because of his inappropriate behavior at the Club. (R. at 5) Following these instances, Baylor felt angry and embarrassed. (R. at 4-5)

Baylor knew that obtaining membership cards required access to the human resources database. (R. at 5) Thus, Baylor believed that someone posed as him and used his benefits. (R. at 5) Baylor's own investigation confirmed his belief. (R. at 5) Additionally, he discovered that someone used his name to authorize the issuance of the cards. (R. at 5)

Baylor informed management and had the director of technology analyze his computer. (R. at 5)

Through a scan of Baylor's hard drive and further analysis, ConDevel discovered Nesbit's unauthorized actions. (R. at 5) ConDevel did not offer Baylor investigative details or to help him restore his reputation. (R. at 5) However, ConDevel immediately fired Nesbit and determined that no one outside the company accessed any personnel files. (R. at 5) The technology support department tightened security. (R. at 5)

II. Summary of the Proceedings

On July 30, 2005, Baylor filed a complaint against ConDevel, asserting claims for intrusion upon seclusion and violation of the Marshall Data Protection Act. (R. at 5) ConDevel moved for summary judgment on both counts. (R. at 5) The trial court granted ConDevel's motions for summary judgment as (1) the "State of Marshall does not recognize the tort of intrusion upon seclusion" and (2) there was "no violation of the notification statute." (R. at 5-6) On appeal, the Fourth Circuit affirmed summary judgment by determining ConDevel was entitled to judgment as a matter of law. (R. at 1)

SUMMARY OF THE ARGUMENT

Viewed in the light most favorable to Baylor, the undisputed facts do not raise a genuine issue of material fact that Baylor stated a claim for intrusion upon seclusion. Nor do they show that the Marshall Data Protection Act required ConDevel to notify Baylor of Nesbit's unauthorized acts. Therefore, ConDevel respectfully requests this Court affirm summary judgment.

This Court has not recognized the tort of intrusion upon seclusion. However, were it an actionable tort, Baylor must prove each of the following elements: (1) ConDevel intentionally intruded or pryed into Baylor's seclusion without authorization, (2) the intrusion was highly offensive to a reasonable person, (3) the matter intruded upon was private, and (4) the intrusion caused anguish and suffering. However, Baylor failed to prove all of the elements.

The facts indicate that ConDevel did not intentionally commit an unauthorized intrusion as ConDevel is authorized to access its corporate records and Baylor voluntarily supplied the information in his personnel files. Further, Nesbit did not act as ConDevel's agent because his acts in obtaining and subsequently using Baylor's membership cards were unauthorized and served only his personal interest. Additionally, ConDevel did not ratify Nesbit's conduct because ConDevel immediately fired him upon learning of his actions. Thus, Nesbit acted outside the scope of his employment, and ConDevel is not liable.

Baylor also failed to show that the alleged intrusion was highly offensive because he had no reasonable expectation of privacy. One cannot have a reasonable expectation of privacy concerning information obtainable via public record or related solely to a corporate interest. Baylor's personnel file contains public record information or otherwise relates only to his corporate interest. Thus, accessing Baylor's personnel file is not a highly offensive intrusion.

Finally, Baylor cannot show that the alleged intrusion caused him the requisite anguish and suffering. The facts indicate that Nesbit's drunken altercation at the Club caused Baylor's anger and embarrassment. Thus, the alleged intrusion and Baylor's anger and embarrassment are only remotely linked.

Additionally, Baylor failed to raise a genuine issue that the Marshall Data Protection Act required ConDevel to notify Baylor of Nesbit's actions. The undisputed facts indicate that Baylor learned of an unauthorized acquisition of computerized data before ConDevel. Therefore, notifying Baylor of what he already knew was unnecessary.

Further, ConDevel was exempt from the notification statute, as an employer is not required to disclose an employee's good faith acquisition of personal information when the information was used for purposes designated by the employer "and/or" is not subject to further unauthorized disclosure. Nesbit acquired Baylor's personal information in good faith, as he merely wanted to show management the company's computer vulnerabilities. Nesbit used Baylor's information to obtain membership cards. This was the designated purpose of using such information in the "VIP Program" files. Additionally, this information is not subject to further unauthorized disclosure because ConDevel immediately took remedial actions by firing Nesbit, tightening security, and ensuring no one outside the company accessed the information. Therefore, ConDevel respectfully requests this Court affirm summary judgment.

ARGUMENT

The Fourth Circuit Court of Appeals correctly affirmed summary judgment for ConDevel because no genuine issue of material fact exists regarding Baylor's questionably actionable tort claim and the applicability of Marshall's Data Protection Act. Summary judgment is proper when no genuine issue of material fact exists and the moving party is entitled to judgment as a matter of law. Marshall R. Civ. P. R. 56(c); *Celotex*, 477 U.S. at 322-323. Rule 56 mandates summary judgment against a party who fails to sufficiently establish a required element in his claim. *Celotex*, 477 U.S. at 322 (interpreting the federal Rule 56, which is identical to Marshall's Rule 56). And a party is entitled to summary judgment if the applicable substantive law leads to only one reasonable verdict. *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 250 (1986). The undisputed facts indicate that Baylor failed to state a claim for intrusion upon seclusion and that the narrowly tailored Marshall Data Protection Act did not require ConDevel to notify Baylor of Nesbit's unauthorized acts. Therefore, ConDevel respectfully requests this Court affirm summary judgment.

I. The Appellate Court Properly Affirmed Summary Judgment Because Baylor Failed to State a Claim for Intrusion upon Seclusion

While privacy is a recognized human value entitled to certain legal protections, *Leopold v. Levin,* 259 N.E.2d 250, 254 (Ill. 1989), no absolute right to privacy exists. *Bank of Am. v. Tremunde,* 365 N.E.2d 295, 298 (Ill. App. Ct. 1977). The area of tort law known as invasion of privacy is modeled after the late Dean Prosser's writings on four limited privacy branches, *Melvin v. Burling,* 490 N.E.2d 1011, 1012 (Ill. App. Ct. 1986), which the Restatement (Second) of Torts formally adopted, including intrusion upon the seclusion of another. *Lovgren v. Citizens First Nat. Bank of Princeton,* 534 N.E.2d 987, 988 (Ill. 1989). Neither this Court nor Marshall's legislature recognizes the tort of intrusion upon seclusion.

Courts should proceed with caution in defining the right to privacy. *Bradley v. Cowles Magazines, Inc.,* 168 N.E.2d 64, 65 (Ill. App. Ct. 1960). The Constitution creates "zones of privacy" through its specific provisions. *Paul v. Davis,* 424 U.S. 693, 712 (1976). These "zones of privacy" protect only those personal rights that are "'fundamental' or 'implicit in the concept of ordered liberty.'" *Id.* at 713. Such personal rights involve "matters relating to marriage, procreation, contraception, family, relationships, and child rearing and education." *Id.* However, a civil action for invasion of privacy "is not rooted in the Constitution." *Lake v. Wal-Mart Stores, Inc.,* 582 N.W.2d 231, 236 (Minn. 1998) (Tomljanovich, J., dissenting).

Many of the states that adopted a cause of action for intrusion upon seclusion did so legislatively. Michael S. Raum, *Torts—Invasion of Privacy: North Dakota Declines to Recognize a Cause of Action for Invasion of Privacy,* 75 N.D. L. Rev. 155, 163 (1999) (observing that New York, Virginia, Nebraska, Rhode Island, Wisconsin, Florida, Oklahoma, and Utah all adopted intrusion upon seclusion by statute, thus making it an actionable tort in those jurisdictions). However, Marshall's legislature does not recognize the tort.

Therefore, neither the Constitution nor Marshall's legislation provides a basis for recognizing the tort of intrusion upon seclusion. As it is not a recognized action in Marshall, summary judgment in favor of ConDevel is appropriate.

Summary judgment is appropriate also because Baylor does not state a claim for intrusion upon seclusion. An intentional intrusion, physical or otherwise, into another's solitude or private affairs constitutes invasion of privacy only if a reasonable person would find the intrusion highly offensive. The Restatement (Second) of Torts §652(B) 377, 378 (1977). The nature of this tort therefore depends largely upon some type of highly offensive prying. *Lovgren*, 534 N.E.2d at 989 (citing W. Prosser & W. Keeton *Torts* §117, at 854-56 (5th ed. 1984)).

Thus, to state a claim for intrusion upon seclusion, Baylor must prove each of the following elements: (1) ConDevel intentionally intruded or pried into Baylor's seclusion without authorization, (2) the intrusion was highly offensive to a reasonable person, (3) the matter intruded upon was private, and (4) the intrusion caused anguish and suffering. *E.g., Melvin*, 490 N.E.2d at 1013-14; *Tremunde*, 365 N.E. 2d at 297-98.[1] Failure to prove any element of this questionably actionable tort terminates the claim. *Id.* Baylor failed to plead facts sufficient to establish every element of this alleged tort. Therefore, his claim must fail as a matter of law.

A. Baylor Failed to State a Claim Because ConDevel Did Not Intentionally and Without Authorization Intrude or Pry into Baylor's Seclusion

Claims for intrusion upon seclusion must fail absent proof that one intentionally invaded another's privacy without authorization. *O'Donnell v. United States*, 891 F.2d 1079, 1082-83 (3d Cir. 1989). An employer does not commit an "unauthorized intrusion" into his employee's seclusion by disclosing information that the employee voluntarily provided to his employer. *Miller v. Motorola, Inc.*, 560 N.E.2d 900, 904 (Ill. App. Ct. 1990).[2] Furthermore, an employer does not commit an "intentional" intrusion upon the seclusion of another where he acts neither individually nor through his authorized agents. *New Summit Assoc. Ltd. v. Nistle*, 533 A.2d 1350, 1354 (Md. Ct. Spec. App. 1987).[3]

[1] The Restatement's second and third elements are inter-related as one cannot claim that an intrusion is offensive unless he has some reasonable expectation of privacy in the area intruded upon. *White v. White*, 781 A.2d 85, 92 (N.J. Super. Ct. 2001). Therefore, this brief addresses these elements concurrently.

[2] While the Restatement does not define "intrusion," Webster's Dictionary defines "intrude" as thrusting oneself in without invitation, permission, or welcome. *Webster's Third New Int'l Dictionary* 1187 (1996). Moreover, the comments and illustrations to Restatement §652(B) indicate that intrusion-upon-seclusion claims usually involve a defendant who believes that he lacks the necessary personal permission or legal authority to do the intrusive act. Comment (b), illustrations 1-5 (1977).

[3] The Restatement (Second) of Torts §8 defines "intent" to mean that one either actually desires to cause the consequences of his act or believes that the consequences are substantially certain to result from his act.

Courts consistently refuse to extend liability to employers for their employees' intentional acts because a master is liable for acts of a servant only when they further the employer's business interest or fall within the scope of the employee's real or apparent authority. *E.g. Bussen v. S. Cent. Bell Tel. Co.,* 682 F.Supp. 319, 325 (S.D. Miss. 1987).

1. No Unauthorized Intrusion Occurred Because ConDevel is Authorized to Access its Business Records, Including Information That Baylor Voluntarily Provided

An employer has the right to access and investigate its business files. *Mucklow v. John Marshall Law Sch.,* 531 N.E.2d 941, 946 (Ill. App. Ct. 1988). *See* Michael J. Leech, Hinshaw & Culberson, *Federal, State, and Common Law Privacy Issues for the Computer Age,* PLI Order No. HO-OOLU 231, 265 (2003) (noting that an employer maintains a compelling argument that any office search is authorized since the employer owns the property in question). No unauthorized intrusion results where an employer discloses or otherwise publishes information voluntarily provided to it by an employee. *Miller,* 560 N.E.2d at 904. *See Fletcher v. Price Chopper Foods of Trumann, Inc.,* 220 F.3d 871, 876-78 (8th Cir. 2000) (observing that no unauthorized intrusion occurs where an individual consents to an intrusive act); Samuel D. Warren and Louis Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193, 199-200 (1890) (acknowledging that one's right to privacy in certain information is lost when he discloses it to others).

An employee in *Miller* claimed that her employer intruded upon her seclusion when it disclosed her mastectomy surgery to co-workers after the employer's resident nurse assured the employee that her medical information, which the employer maintained in its office, would remain confidential. 560 N.E.2d. at 902. Because the employee voluntarily disclosed her medical procedure to her employer, the court held that the employee failed to state a claim for unreasonable intrusion upon seclusion even though she never consented to further disclosure of her personal information. *Id.* at 904.

No unauthorized intrusion occurred here because ConDevel has a right to access its personnel files, which contain personal information that Baylor voluntarily provided. Similar to the employee in *Miller,* 560 N.E.2d at 902, Baylor willingly disclosed personal information to his employer, ConDevel, including his social security number, driver's license number, etc. (R. at 2) And like the employer in *Miller,* 560 N.E.2d at 902, ConDevel stored and maintained Baylor's personnel records at its place of business—more specifically, on its human resources database. (R. at 2) Moreover, Baylor was not naive to the contents or accessibility of personnel files, including his own at ConDevel. In fact, as executive vice president, Baylor supervised the human resources department, which controlled electronic personnel files, and had direct access to all ConDevel employees' personal information. (R. at 2) It follows logically that Baylor, more than anyone, understood ConDevel's need to access and update its employees' personnel files. Thus, ConDevel did not engage in an unauthorized intrusion into Baylor's seclusion because Baylor voluntary disclosed his personal information.

2. *ConDevel Did Not Intentionally Intrude Into Baylor's Seclusion Because Nesbit Acted Without Authorization*

A claim is not actionable for intrusion upon the seclusion of another unless the plaintiff shows an intentional intrusion. *O'Donnell*, 891 F.2d at 1083; *Nistle*, 533 A.2d at 1354 (affirming no basis for employer liability exists in an intrusion-upon-seclusion claim absent proof that the employer intentionally participated in the alleged intrusion through his agents or employees). Under the common-law agency doctrine of respondeat superior, an employer is liable for an employee's intentional actions only if (a) the employee acted while furthering his employer's business interest, (b) the employee acted within the scope of his employment, and (c) the employer participated in, authorized, or ratified the conduct. *Ex Parte Atmore Cmty. Hosp.*, 719 So.2d 1190, 1194 (Ala. 1998); *Jones v. Baisch*, 40 F.3d 252, 254 (8th Cir. 1994) (confirming the doctrine of respondeat superior precludes employer liability unless an employee's actions can be imputed to his employer).

Although determining whether an employee acted within the scope of his employment is generally a question of fact, summary judgment is appropriate if the undisputed facts lead to only one reasonable conclusion. *Mason v. Kenyon Zero Storage,* 856 P.2d 410, 414 (Wash. App. 1993). Here, the stipulated facts indicate that Nesbit acted only for his personal interest without ConDevel's participation, authorization, or ratification. Accordingly, ConDevel did not intentionally intrude upon Baylor's seclusion.

i. Nesbit's Actions Served Only His Personal Interest

An employer is liable only for acts committed by an employee in furtherance of the employer's business interest. *Tichenor v. Roman Catholic Church*, 32 F.3d 953, 959 (5th Cir. 1994). Behavior aimed primarily at satisfying an employee's personal desires serves no business interest. *Atmore*, 719 So.2d at 1194. A master is not liable when his servant steps aside from the master's business to effectuate the servant's own purpose, such as acts undertaken solely based on jealousy, hatred, or other ill feelings. *Mason*, 856 P.2d at 415.

In *Atmore*, a hospital employee sued her co-worker and employer for invasion of privacy. 719 So.2d. at 1192-93. The employee argued that her employer was liable for a co-worker's repeated sexual harassment. *Id.* Because the sole purpose of the co-worker's numerous sexual inquiries were to fulfill his own lustful desires, the court found that the employee failed to establish a basis for her employer's liability. *Id.* at 1194.

Conversely, in *Mason*, genuine issues of material fact existed as to whether a supervisor acted in furtherance of his employer's interest when he drove a forklift into a co-worker's back. 856 P.2d at 415. The court held that the evidence did not support the employer's assertion that the supervisor acted out of ill-will because one could reasonably infer that the supervisor acted consistently with prior disciplinary measures effectuated on the employer's behalf. *Id.* Accordingly, under *Atmore* and *Mason*, an employee acting primarily for his personal benefit, not for his employer's purpose, serves no business interest.

The stipulated facts demonstrate that Nesbit stepped aside from ConDevel's business interest and acted out of envy for the "good life reserved to ConDevel executives." (R. at 2) Unlike *Mason*, where evidence indicated that the supervisor's duties included maintaining order and discipline within the crew, 856 P.2d at 414, here, no evidence indicates that Nesbit's duties included maintaining or otherwise monitoring ConDevel's personnel files or executive benefits system. And in stark contrast to *Mason*, where evidence showed that the supervisor previously used forklift ramming as a disciplinary tool amongst crew members, 856 P.2d at 414, here, no evidence shows that Nesbit previously used ConDevel's human resources database as a tool to perform his sales duties. Rather, Nesbit hoped to expedite his climb up the corporate ladder by impressing his ConDevel superiors with his initiative. (R. at 2) Hence, Nesbit devised his calculated plan to reveal computer vulnerabilities within ConDevel's corporate system. (R. at 4)

However, similar to the employee in *Atmore*, 719 So.2d at 1194, Nesbit ultimately desired to satisfy only his personal curiosities when he downloaded ConDevel's personnel files to his home computer. (R. at 4) Although Nesbit initially developed and installed the keylogger program to test ConDevel's technology infrastructure and intended to report his findings to management, (R. at 3), Nesbit admittedly "had a change of heart." (R. at 4) As soon as Nesbit realized the extent of information he accessed, especially ConDevel's benefits system and "VIP Program," Nesbit abandoned his original plan and usurped the information for his own selfish designs. (R. at 4) Specifically, Nesbit obtained memberships to various private social clubs. (R. at 4) At no point thereafter did Nesbit raise the security inadequacies he discovered to anyone at ConDevel. (R. at 4) Nesbit ultimately acted to enhance his own personal social circumstances rather than protect ConDevel's corporate information. Thus, no rational relationship exists between Nesbit's ultimate conduct and a desire to serve ConDevel's business interests.

ii. Nesbit Acted Outside the Scope of his Employment

No liability imputes to an employer unless the employee acted within the scope of his individual employment. *O'Bryan v. KTIV Television*, 868 F.Supp. 1146, 1158 (N.D. Iowa 1994) *rev'd on other grounds,* 64 F.3d 1188 (8th Cir. 1995). An employee acts within the scope of his individual employment if his actions are so closely related to the tasks he is hired to perform that they are methods of carrying out the employment objectives. *Atmore*, 719 So.2d at 1194. *See also Jones*, 40 F.3d at 254 (holding that an employee acts within the scope of employment only if his conduct occurs within the authorized time and space limits).

The court noted in *Atmore* that because an employee's repeated sexual inquiries and advances qualified as entirely personal in nature, they could not fall within the scope of his assigned duties. 719 So.2d at 1194. Likewise, in *Jones*, the court ruled that a physician's office could not be held liable for acts of a nurse and her assistant when they disclosed a patient's diagnosis to their friends. 40 F.3d at 254. The *Jones* court reasoned that the disclosure of the patient's medical records occurred substantially outside the work environment and without authorization from the physician. *Id.* Therefore, under *Atmore* and *Jones*, an employee's conduct related to personal matters outside the office does not fall within the scope of employment.

Nesbit's surreptitious acquisition exceeded the scope of his employment. Analogous to *Jones*, where employees used a patient's medical information for personal entertainment outside the office, 40 F.3d at 253, Nesbit used Baylor's personnel information and executive benefits for his personal entertainment outside the office. (R. at 4) Nesbit accessed ConDevel's corporate files through his private e-mail address and had the credentials to various social clubs sent directly to his home mailing address. (R. at 3-4) And as in *Jones*, where the employer never instructed his employees to disclose the patient's information, 40 F.3d at 253-54, ConDevel's managers never instructed Nesbit to use executive benefits. ConDevel employed Nesbit as an entry-level sales associate. (R. at 3) Despite his personal fascination with information technology, Nesbit had no authority to use the computer systems he hacked. (R. at 3-4) In fact, Nesbit's supervisor explicitly told Nesbit to "mind his own business" when Nesbit attempted to involve himself with ConDevel's technology infrastucture. (R. at 3)

Nesbit's sales position in no way required access to ConDevel's personnel files. Yet Nesbit collected other employees' personal information from ConDevel's electronic database using his private e-mail address.

(R. at 3) Nesbit then stored the information on his home computer and had credentials sent to his home address. (R. at 4) Accordingly, Nesbitt acted entirely outside the scope of his employment.

iii. ConDevel Did Not Participate in, Authorize, or Ratify Nesbit's Actions

No employer liability exists for tortious conduct when the employer neither authorizes nor tolerates a course of activity outside the employee's prescribed duties. *Bussen*, 682 F.Supp. at 325. An employer ratifies tortious conduct by knowing of the conduct and failing to take adequate steps to remedy the situation. *Atmore*, 719 So.2d at 1195. Authorization is legitimate only if it comes from a high-level managerial agent. *Morris v. Ameritech Illinois*, 785 N.E.2d 62, 71 (Ill. App. 2003).

In *Bussen*, a telephone company service representative accessed a customer's billing account, which contained the customer's unlisted telephone number, in contravention of company policy. 682 F.Supp. at 322-23. The customer alleged that the employee made harassing phone calls to her home and disclosed her private number to her ex-husband, who did the same. *Id.* at 323. The employer countered that its investigation revealed no such phone calls or disclosure, but nevertheless suspended the employee for improperly accessing the customer's file. *Id.* at 323-24. The court held that even if the employee's actions constituted an invasion upon the customer's privacy, the employer is not liable because it neither authorized nor approved the employee's conduct. *Id.* at 325.

Similarly, in *Morris*, a telephone company employee alleged that her employer invaded her privacy when it authorized other employees to access her phone records and eavesdrop on her conversations. 785 N.E.2d at 64. The employer argued that its managers never authorized these actions as it maintained a strict policy of firing any employee found to have eavesdropped. *Id.* at 67. The court upheld summary judgment in favor of the employer since the employee failed to produce any evidence that the employer's managers authorized or requested the eavesdropping. *Id.* at 71. Accordingly, under *Bussen* and *Morris*, an employer assumes no liability unless management participates in, authorizes, or ratifies an employee's conduct.

Although ConDevel's Computer Usage Policy instructed employees to safeguard their individual computers, the Policy did not instruct employees to hack into their co-worker's computers. (R. at 2) Like *Morris*, where the employer never requested its employee to eavesdrop on a coworker's telephone conversations, 785 N.E.2d at 67, ConDevel never requested Nesbit to test its corporate information security or download his co-worker's personnel files. (R. at 3) Nesbit independently took it upon himself to test ConDevel's computer system despite direct orders from his supervisor to leave technological issues to the technology support department. (R. at 3) In fact, like the employer in *Morris*, 785 N.E.2d at 67-68, ConDevel had no knowledge that Nesbit designed the keylogger program and secretly installed it on Baylor's computer until after Baylor alerted ConDevel's director of technology support, who then traced the software to Nesbit and presented his findings to management. (R. at 5)

Similar to the employer in *Bussen*, 682 F.Supp. at 325, ConDevel responded immediately to Baylor's complaint with an internal investigation. (R. at 5) Finally, as in *Bussen*, where the employer confronted its offending employee with proof of her wrongdoing and punished her, *Id.* at 323-24, ConDevel confronted Nesbit with proof of his wrongdoing and fired him. (R. at 5) No manager at ConDevel authorized Nesbit's keylogger program. (R. at 3) As soon as ConDevel knew of the program and Nesbit's subsequent use of corporate records, ConDevel fired Nesbit and tightened security. (R. at 5) Thus, ConDevel in no way participated in, authorized, or ratified Nesbit's self-motivated actions.

Applying the stipulated facts to the relevant law leads to only one reasonable conclusion: ConDevel did not intentionally intrude upon Baylor's seclusion because Nesbit exceeded the scope of his sales duties when he defiantly accessed ConDevel's corporate records and used the information for personal gain. Under the well-established agency doctrine of respondeat superior, Nesbit's actions do not impute to ConDevel. Therefore, ConDevel respectfully requests this Court affirm summary judgment.

B. Baylor Failed to State a Claim Because He Had No Reasonable Expectation of Privacy, the Alleged Intrusion Was Not Highly Offensive, and Baylor's Personnel Information Was Not Private

The reasonable expectation of privacy represents the cornerstone of intrusion upon seclusion, *Fletcher*, 220 F.3d at 877, which requires that the intrusion be "highly offensive" to a reasonable person. *White v. White*, 781 A.2d 85, 91-92 (N.J. Super. Ct. 2001). Judicial determination of offensiveness depends on one's expectation of privacy, *Id.* at 91-92, which must be both subjectively held and objectively reasonable. *Med. Lab. Mgmt. Consultants v. Am. Broad. Co.*, 306 F.3d 806, 812-13 (9th Cir. 2002). When undisputed material facts demonstrate either no reasonable expectation of privacy or an insubstantial impact on an individual's privacy interest, the question of invasion is a matter of law. *Deteresa v. Am. Broad. Co., Inc.*, 121 F.3d 460, 465 (9th Cir. 1997).

1. Baylor Had no Reasonable Expectation of Privacy

To establish an intrusion-upon-seclusion claim, a plaintiff must show unauthorized penetration of a surrounding physical or sensory privacy zone. *Shulman v. Group W. Prods.*, 955 P.2d 469, 490 (Cal. 1998). To that end, the Supreme Court recognized, and lower courts affirmed, that an individual's expectation of privacy is less in commercial property than in an individual's home. *Minnesota v. Carter*, 525 U.S. 83, 90 (1998); *Smith v. Colorado Interstate Gas Co.*, 777 F. Supp. 854, 857 (D. Col. 1991) (holding that no unreasonable intrusion upon seclusion is implicated where the allegations involve business affairs rather than personal solitude); *Morningstar v. State*, 428 So.2d 220, 221 (Fla. 1983) (finding that while a party might have an actual subjective expectation of privacy for conversations occurring in his home, that does not mean that society recognizes an absolute right to privacy in one's office).

One demonstrates a subjective expectation of privacy through behavior consistent with actually having a privacy expectation in a specific area. *Med. Lab.*, 306 F.3d at 812-13. In *Medical Laboratory*, the plaintiff's conduct failed to demonstrate an objective privacy expectation in certain office spaces when he provided several undercover reporters with a tour of the company's medical lab and a conference room. *Id.* at 818-19. However, stopping the reporters from entering his personal office indicated the plaintiff's privacy expectation in that specific space. *Id.* at 813-14. Here, Baylor potentially had a subjective expectation of privacy as he similarly did not explicitly grant Nesbit access to his business office.

However, Baylor's subjective belief that his personnel information was private is not enough. Baylor must also have an objectively reasonable privacy expectation in the data. *Shulman*, 955 P.2d at 490. No objectively reasonable expectation of privacy exists with respect to specific information that one willingly shares with others. *White*, 781 A.2d at 92.

The nature of a work environment dictates whether an employee has a reasonable expectation of privacy in his workspace. *O'Connor v. Ortega*, 480 U.S. 709, 718-19 (1987). To that end, an employee cannot objectively expect his employer not to access his office space or furniture when the employee works in an open environment and workspace is designated for official business only. *O'Bryan*, 868 F.Supp. at 1159. Moreover, the absence of an official policy regulating the contents of an employee's office and equipment does not create an expectation of privacy. *Ortega*, 480 U.S. at 719. *See also Garrity v. John Hancock Mutual Life Ins. Co.*, WL 974676 (D. Mass. 2002) (holding that even in the absence of a corporate policy, employees had no reasonable privacy expectation in business e-mails sent and received over the shared computer system owned by the employer).

The five-judge majority in *Ortega* affirmed that a government employer intruded upon an employee's privacy by searching the employee's office during his absence. 480 U.S. at 719. The Court held that the employee had a reasonable expectation of privacy in his office because of the significant personal nature of the items found in the employee's desk and file cabinets, which included personal medical files, financial records, correspondence, and gifts. *Id.* at 718.

In stark contrast, the *O'Bryan* court dismissed an employee's intrusion-upon-seclusion claim against an employer who admittedly searched its employee's workspace for corporate records. 868 F.Supp. at 1158-59. Following the principles outlined in *Ortega*, the court held that the employee had no reasonable expectation of privacy because the employer merely looked for employer-owned documents, not unrelated personal items that belonged to the employee. *Id.*

The present dispute closely resembles *O'Bryan* and is readily distinguishable from *Ortega*. Unlike *Ortega*, where the employer's authorized agents entered the plaintiff's locked office and searched his locked desk and file cabinet, 480 U.S. at 718-19, ConDevel's unauthorized employee entered Baylor's unlocked office and searched his unlocked computer. (R. at 3) The record is devoid of any evidence suggesting that Baylor (or any other ConDevel employee for that matter) routinely locked their offices or turned off their computers. In contrast to *Ortega,* where the plaintiff stored significant quantities of personal health, financial, and sentimental items in his office, *Id.*, Baylor plead no facts to suggest that he stored any personal health, financial, or sentimental items in his office. However, like *O'Bryan*, 868 F.Supp. at 1159, Nesbit searched ConDevel's computer system for corporate records, including those regarding Baylor. (R. at 3-4)

ConDevel's Computer Usage Policy charged each employee with protecting the equipment and software provided by the company. (R. at 2) Yet Baylor failed to plead facts showing that he had exclusive use or control of his office and its contents or that he used his office computer for personal matters. Applying the rules of law under the objective standard to the stipulated facts, Baylor had no reasonable expectation of privacy.

2. *Nesbit Did Not Commit a Highly Offensive Intrusion*

In determining the offensiveness of one's conduct, courts consider factors such as degree of intrusion; context, conduct, and circumstances surrounding the intrusion; intruder's motives and objectives; setting intruded upon; and expectations of those whose privacy is invaded. *Deteresa*, 121 F.3d at 465. While determining what is highly offensive to a reasonable person appears to suggest a jury question, a court must first discern a cause of action for intrusion by making a preliminary legal determination of "offensiveness." *Id.* at 465.

The Restatement § 652(B), Comment B, provides that a highly offensive intrusion requires an exceptional kind of prying, such as (1) taking a photograph of a woman hospitalized due to a rare disease over her objection, (2) using a telescope to look into someone's bedroom window, or (3) taking intimate pictures with a telescopic lens.

Building on these examples, courts have held that a film crew's taping a man's emergency medical treatment in his home and without his consent is highly offensive. *E.g. Schulman*, 955 P.2d at 493. Likewise, repeated inquiries into one's sexual proclivities, combined with numerous sexual propositions and unwanted touching, are also highly offensive. *Cunningham v. Dabbs*, 703. So.2d 979, 982 (Ala. Civ. App. 1997). However, covertly videotaping a business conversation conducted in a corporate office does not rise to the level of exceptional prying into another's private affairs, even where confidential business information is discussed. *Med. Lab.*, 306 F.3d at 819.

In *Medical Laboratory*, a group of undercover reporters, posing as potential business partners, surreptitiously videotaped a private conversation with an employer's lab technician and broadcast portions of the conversation to the general public. 306 F.3d at 814-15. The technician argued that the broadcast was highly offensive since the conversation included discussion of proprietary business information. *Id.* The court disagreed, holding that given the conversation's inherent business nature, only de minimis intrusion resulted, which cannot qualify as highly offensive to a reasonable person. *Id.* at 819-20.

Similar to the undercover reporters in *Medical Laboratory*, 306 F.3d at 815, Nesbit covertly installed the keylogger program on Baylor's computer and downloaded ConDevel's business files. (R. at 3-4) However, unlike *Schulman*, 955 P.2d at 490-91, and *Dabbs*, 703 So.2d at 982, where the defendants' employees intruded into inherently personal affairs involving the plaintiffs' medical injuries and sexual interests, Nesbit accessed only corporate records, including Baylor's personnel file and fringe benefits package. (R. at 4) Even though Nesbit accessed this business information without authorization, no facts indicate that Nesbit accessed or sought information related to Baylor's medical, sexual, or family affairs. (R. at 4) Consequently, only a de minimis degree of intrusion, if any, resulted, which is not highly offensive to a reasonable person. *See Med. Lab.,* 306 F.3d at 819 (observing that conduct resulting in only de minimis intrusion into business matters is not highly offensive to a reasonable person). Thus, no offensive intrusion occurred given the inherent business nature of the information Nesbit accessed.

3. *Baylor's Personnel File Was Not Private*

The information that courts acknowledge as private, and therefore presenting triable issues of fact, differs substantially from the information involved in the present dispute. *See Johnson v. K-Mart Corp.*, 723 N.E.2d 1192, 1196-97 (Ill. App. 2000) (noting that courts traditionally recognize private information as pertaining to an employee's family problems, romantic interests, sex life, and health problems); *Shulman*, 955 P.2d at 491 (holding that information conveyed by a medical patient to a paramedic during the course of emergency treatment is private); *Doe v. High-Tech Inst.*, 972 P.2d 1060, 1069 (Colo. App. 1998) (holding that information derived from a patient's blood sample is private). The Supreme Court recognized "marriage" and "sexual" concerns as fundamental rights entitled to privacy protection. *Griswold v. Connecticut*, 381 U.S. 479, 485-86 (1965).

Here, however, Baylor plead no facts indicating that Nesbit (or any other ConDevel employee) accessed information regarding his family life, romantic interests, sex life, or health problems. Rather, Baylor's claim concerns general identity information and information specific to his employment with ConDevel. (R. at 2, 4) Accordingly, Baylor failed to plead sufficient facts indicating an intrusion upon private information.

i. *Baylor's General Identity Information is Readily Accessible on the Public Record*

Examination of information available at public record does not trigger an intrusion upon another's seclusion. *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1018 (Ill. App. 2004). Discovery of another's social security number fails to qualify as an intrusion upon seclusion. *Phillips v. Grendahl*, 312 F.3d 357, 373 (8th Cir. 2002); *see also Bodah v. Lakeville Motor Express, Inc.*, 649 N.W.2d 859, 862 (Minn. App. 2002) (observing that although social security numbers are recognized as confidential and private, unlike medical information, they "are not on their face revealing, compromising, or embarrassing").

In *Busse*, a cell-phone customer sued her phone manufacturer for intrusion upon seclusion when the manufacturer distributed her identity information to third parties. 813 N.E.2d at 1015. The information consisted merely of the customer's legal name, mailing address, date of birth, and proof of marriage. *Id.* at 1018. The court affirmed summary judgment for the defendant and held that such information is not private since it is readily available on the public record. *Id.* In *Grendahl*, the court held that although social security numbers are technically private, because they are widely and continuously provided to others in modern society, discovery of another's social security number does not fit the profile of intrusion upon another's seclusion. 312 F.3d at 373. Therefore, information that is widely disseminated or available through public record is not private.

Similar to *Busse*, where the personal information included names, addresses, and social security numbers, 813 N.E.2d at 1015, here, the personal information includes Baylor's name, address, and social security number. (R. at 2, 4) And like *Grendahl*, where the plaintiff voluntarily disclosed his social security number on a credit report, 312 F.3d at 372, Baylor voluntarily disclosed his social security number on his personnel record. (R. at 2) Therefore, the information regarding Baylor's name, address, and social security number is not private information under the intrusion-upon-seclusion tort.

ii. Baylor's Executive Profile at ConDevel Relates Only to his Corporate Interest

Confidential information related to one's business interests and operations, as opposed to one's personal life, is not private information entitled to protection under the intrusion-upon-seclusion tort. *Smith*, 777 F.Supp. 854, 857 (D. Colo. 1991); *Med. Lab.*, 306 F.3d 806, 814 (9th Cir. 2002) (finding that privacy is personal to individuals and does not encompass one's corporate interest).

In *Medical Laboratory*, the plaintiff claimed he had a privacy right when discussing confidential business information, including operations and testing procedures. 306 F.3d at 814. The Ninth Circuit Court of Appeals disagreed, holding that the plaintiff had no privacy right to proprietary corporate information because it was not personal to the plaintiff. *Id.*

In *Smith*, an employee sued for intrusion upon seclusion when her employer contacted the employee's former supervisor to investigate the nature and circumstances of her departure from a previous job. 777 F.Supp. at 856. The employee claimed her current employer intruded upon her seclusion by contacting her former supervisor, who disclosed allegedly embarrassing situations as to why the company fired her. *Id.* at 856-57. Because all of the alleged intrusions involved the employee's business affairs, the court held that the employer did not intrude into the employee's seclusion. *Id.* at 857. Accordingly, the right to privacy is substantially limited when information relates solely to one's corporate interest.

Similar to the plaintiffs in *Medical Laboratory*, 306 F.3d at 814, and *Smith*, 777 F.Supp. at 857, Baylor's personnel information consists of official employee records and business operations. (R. at 4) Specifically, Nesbit accessed ConDevel's human resources database, which included the benefits system and "VIP Program" files. (R. at 4) The latter listed exclusive social club memberships available to ConDevel executives. (R.

at 4) Along the same lines as *Smith*, where the employer's manager investigated an employee's prior work history, 777 F.Supp. at 856-57, Nesbit investigated—albeit without authorization—Baylor's work profile. (R. at 4) Nesbit at no point accessed information related to Baylor's personal affairs. Accordingly, information regarding Baylor's executive status is not private.

The undisputed material facts demonstrate that Baylor had no reasonable expectation of privacy in his personnel information, some of which he voluntarily provided to ConDevel. Baylor also evidenced no zone of solitude in his workspace or computer, both of which he left open to the rest of the office. Moreover, Nesbit's conduct resulted in de minimus intrusion, if any, since Nesbit did not access information related to Baylor's medical, sexual, or family affairs. Nesbit merely accessed information either available at public record or related to Baylor's corporate interest. Therefore, Baylor failed to establish an intrusion upon his seclusion, and ConDevel respectfully requests this Court affirm summary judgment.

C. Baylor Failed to Plead the Requisite Anguish and Suffering Because His Anger and Embarrassment Are Only Remotely Linked to Nesbit's Alleged Intrusion

Generally, establishing causation requires sufficient facts that a defendant's conduct substantially caused the injury claimed by the plaintiff. *Tompkins v. Cyr,* 202 F.3d 770, 782 (5th Cir. 2000). Anyone claiming an unreasonable intrusion upon seclusion must prove that the alleged intrusion caused anguish and suffering. *Schmidt v. Ameritech Illinois*, 786 N.E.2d 303, 315 (Ill. App. Ct. 2002); *Robyn v. Phillips Petroleum*, 774 F.Supp. 587, 592 (D. Colo. 1991) (confirming that the perpetrator's alleged intrusion must result in extreme mental anguish, embarrassment, humiliation, or injury to a person of ordinary sensibilities). *See Preferred Nat. Ins. Co. v. Docusource, Inc.*, 829 A.2d 1068, 1075 (N.H. 2003) (holding that the intrusion itself must cause the requisite harm).

Harm is not anguish and suffering when the harm is only remotely linked to an alleged intrusion. *Hoth v. Am. States Ins. Co.,* 735 F.Supp. 290, 293 (N.D. Ill. 1990). In order to demonstrate the requisite suffering and anguish for intrusion upon seclusion, a plaintiff must prove actual injury, such as a medical illness, inability to sleep or work, or a loss of reputation and integrity in the community. *Schmidt*, 786 N.E.2d at 316. *But see Deteresa*, 121 F.3d at 466 (holding that when an alleged privacy invasion does not encroach upon the plaintiff's physical property, the resulting harm is de minimis and, therefore, insufficient to sustain a cause of action for intrusion upon seclusion).

In *Hoth*, an employee alleged that his employer improperly authorized a search of his office, file cabinet, and desk and collected personal documents used as the basis of a memo accusing the employee of theft, which eventually led to the employee's termination. 735 F.Supp. at 291. Consequently, the employee implied that he suffered damage to his reputation based on the employer's allegations. *See id.* at 291 (noting employee claimed his employer made false statements in reckless disregard of the truth). Because the underlying theft prompted the employee's termination, the court found the employer's document search only remotely linked to the termination. *Hoth*, 735 F.Supp. at 293. Therefore, the court dismissed the claim for failure to establish a sufficient causal link between the document search and the alleged anguish and suffering. *Id.*

Likewise, in *Schmidt*, a plaintiff sued his former employer, for intruding upon his seclusion when it reviewed his personal telephone records and then later fired the employee. 768 N.E.2d at 306. As a result, the employee claimed he suffered depression. *Id.* at 316. However, the court found that the employer fired the employee for repeatedly lying about a disability in order to get paid time off work, not because of information found in the employee's telephone records. *Id.* at 316-17. Therefore, an employee does not sufficiently plead anguish and suffering when the causal connection between the alleged intrusion and resulting harm is either attenuated or nonexistent. *Id.* at 317.

In stark contrast to both *Schmidt*, 786 N.E.2d at 316, and *Hoth*, 735 F.Supp. at 293, where the employers fired the employees after the disputed events, no facts suggest ConDevel fired Baylor or that Baylor otherwise left ConDevel's employment. Rather, analogous to the employee in *Hoth*, Baylor implies damage to his reputation based on Nesbit's behavior while using Baylor's social club memberships. Specifically, Baylor contends that he felt anger and embarrassment on two isolated occasions: first, when a private golf course revoked his membership and, second, when an upscale restaurant denied him a table for dinner. (R. at 4-5)

However, under the causation rationale discussed in *Schmidt* and *Hoth*, Baylor's supposed anger and embarrassment resulted not from Nesbit's alleged intrusion, but from Nesbit's subsequent behavior at the social clubs. Nesbit became intoxicated one evening and got into a fight with another club member. (R. at 4) This altercation led to Nesbit's physical removal from the club and subsequent cancellation of Baylor's memberships. (R. at 4) Following this uncontested chain of events, Nesbit's installation of the keylogger program and acquisition of Baylor's corporate records is only remotely linked to Nesbit's drunken antics, which actually caused Baylor's anger and embarrassment. Accordingly, Baylor failed to plead that the alleged intrusion caused the requisite anguish and suffering.

The Fourth Circuit Court of Appeals properly affirmed summary judgment because Baylor failed to state a claim for intrusion upon seclusion. First, ConDevel did not intentionally authorize an intrusion into Nesbit's seclusion because ConDevel had a right to access its business records and Nesbit acted without authorization or ratification when he secretly installed spyware on Baylor's computer and accessed ConDevel's human resources database. Second, a de minimis intrusion, if any, resulted from Nesbit's actions because Baylor does not have an objectively reasonable expectation of privacy in corporate records that contain information Baylor voluntarily shared with ConDevel. And third, Baylor failed to plead the requisite anguish and suffering because Nesbit's drunken brawl, not the alleged intrusion, caused Baylor's anger and embarrassment. Therefore, ConDevel respectfully requests this Court affirm summary judgment.

II. THE APPELLATE COURT PROPERLY AFFIRMED THAT CONDEVEL WAS EXEMPT FROM THE DISCLOSURE REQUIREMENT OF MARSHALL'S DATA PROTECTION ACT

The plain language of Marshall's Data Protection Act ("the Act") as well as the surrounding circumstances demonstrate that ConDevel did not violate the Act. The Act requires an agency that owns computerized data including personal information to disclose any "breach of the security of the system," which means that the agency must disclose an "unauthorized acquisition of computerized data." 17 Marshall Code § 105(a), (d) (2006). Here, Baylor knew of the unauthorized acquisition of computerized data before ConDevel, (R. at 5), so he already had the information that the Act would require ConDevel to disclose. Thus, disclosure was unnecessary.

ConDevel was also exempt under the Act's good-faith-acquisition exemption: An employee's "[g]ood faith acquisition of personal information" is not a breach of the security of the system, "provided that the personal information is used for the purposes designated by the agency and/or is not subject to further unauthorized disclosure." *Id.* at § 105(d). Therefore, in certain situations, the Act does not require a company to disclose an unauthorized acquisition of computerized data. This case, stemming from Nesbit's actions, presents one of those situations. Therefore, the appellate court properly affirmed summary judgment.[4]

[4] The appellate court's analysis references Baylor's argument that ConDevel violated the Act by failing to notify other employees of Nesbit's actions. (R. at 7) However, ConDevel's decision not to notify other employees of Nesbit's actions does not make ConDevel liable to Baylor under the Act. *See* Sec'y of State of Maryland v. Joseph H. Munson Co., Inc., 467 U.S. 947, 955 (1984) (reasserting that a plaintiff does not have standing to sue by resting his claim only on the rights or interests of others).

A. Disclosure Was Unnecessary Because Baylor Already Knew the Information that the Act Would Require ConDevel to Disclose

ConDevel was not subject to the Act's disclosure requirement because the Act requires disclosure only "following discovery or notification" of a security breach. 17 Marshall Code § 105(a). After Baylor notified ConDevel of the unauthorized acquisition of computerized data, disclosure was unnecessary because Baylor already knew the information that the Act would require ConDevel to disclose. *See id.* at § 105(a), (d) (showing that an agency need not disclose anything more than an unauthorized acquisition of computerized data). Therefore, the appellate court properly affirmed summary judgment.

1. *Before Learning of Nesbit's Actions, ConDevel Did Not Owe Baylor a Duty Under the Act*

The Act's plain language imposes a duty to disclose only "following discovery or notification of the breach in the security of the data . . . ." 17 Marshall Code § 105(a). The Act does not impose a duty prior to discovery or notification. Other parts of the Act also show that an agency has a duty only after learning of a breach. For example, the Act allows an agency discovering or receiving notification of a breach to investigate the matter before disclosing details: "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with . . . any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." 17 Marshall Code § 105(a) (emphasis added). This provision contemplates that a company may investigate an alleged breach to determine whether it affected anyone before having to disclose it. Similarly, a data subject does not have a cause of action under the Act unless the data collector "obfuscates evidence of a breach or makes an informed choice to not inform data subjects of a breach." 17 Marshall Code § 105(g). This provision shows that the agency must have at least some evidence of a breach before a cause of action arises. Read together, these provisions show that ConDevel did not have a duty under the Act before ConDevel learned of Nesbit's actions. *See People v. McCarty*, 858 N.E.2d 15, 31 (Ill. 2006) (restating a standard rule of statutory interpretation that "provisions of a statute must be read as a whole").

2. *After ConDevel Learned of Nesbit's Actions, Disclosure was Unnecessary Because Baylor already knew of the Unauthorized Acquisition of Computerized Data*

The Act requires an agency that owns or licenses computerized data that includes personal information to disclose any "breach of the security of the system" to "any resident of Marshall whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." 17 Marshall Code § 105(a). A "breach of the security of the system" is "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." *Id.* at § 105(d). Therefore, any resident of Marshall who knows of an unauthorized acquisition of computerized data already has the information that the Act would require the agency to disclose.

The stipulated facts show that Baylor knew of the unauthorized acquisition of computerized data. First, Baylor knew that someone used his name to authorize, issue, and obtain membership cards for various social clubs. (R. at 5) Also, Baylor knew obtaining membership cards required access to the human resources database. (R. at 5) Accessing the human resources database under Baylor's name required Baylor's login and passwords. (R. at 4) Thus, Baylor knew that whoever used his name to authorize, issue, and obtain membership cards acquired his login and passwords to the human resources database. The record does not indicate that Baylor authorized anyone to use his login and passwords. Consequently, Baylor knew that an unauthorized acquisition of computerized data occurred. Therefore, he already had all the information that the Act would require ConDevel to disclose.

The Act's plain language grants ConDevel discretion in whether to disclose additional investigative details or to assist Baylor in rebuilding his reputation. As long as the disclosure is consistent with the Act's timing requirements, an agency complying with its own notification procedures, if any, is in compliance with the Act. 17 Marshall Code § 105(f). Here, the record does not suggest that ConDevel ever implemented notification procedures requiring ConDevel to disclose information not otherwise subject to the Act's disclosure requirement. (R. at 2) Therefore, ConDevel's decision not to offer investigative details or help Baylor rebuild his reputation did not violate an internal notification procedure and, thus, did not make ConDevel liable to Baylor under the Act. (R. at 5)

Recent case law defining the scope of disclosure under a nearly identical Indiana statute confirms the validity of ConDevel's response to Nesbit's conduct. The Indiana statute requires that "after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident . . . ." Ind. Code § 24-4.9-3-1 (2006). This provision requires only disclosure of a security breach and does not require "any other affirmative act in the wake of a breach." *Pisciotta v. Old Nat'l Bancorp*, 2007 WL 2389770, at *5 (7th Cir. Aug. 23, 2007).

Disclosure requirements under a federal law as well as a nearly identical California law show that the information Baylor already had nullified any need for further disclosure. The duty to disclose under the Act is similar to a duty to disclose security breaches under the federal Gramm-Leach-Bliley Act ("GLBA"). 15 U.S.C. § 6801 (2006); 70 Fed. Reg. 15736, 15736 (March 19, 2005) (clarifying the responsibilities of financial institutions under the GLBA). The GLBA requires financial institutions to disclose security breaches to customers. 70 Fed. Reg. at 15752. The purpose of disclosure is simply to enable a customer to take steps to prevent identity theft. *Id.* at 15738.

California's data protection act serves a similar purpose. As in Marshall, California requires disclosure of a "breach in the security of the system," defined in exactly the same way as Marshall defines it: "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." Cal. Civ. Code § 1798.29(a), (d) (2007); 17 Marshall Code § 105(d). Thus, the California and Marshall data protection acts require agencies to disclose the same information. California's legislative analysis indicates that disclosure under the statute gives Californians "the information necessary to protect their financial wellbeing." Cal. Bill Analysis, Assembly Bill 700, S. 2001 - 2002, Reg. Sess. (Aug. 21, 2002). Therefore, the purpose of disclosure is simply to enable data subjects to protect their identity and financial wellbeing.

Here, Baylor knew that someone without authorization accessed his personal information, which includes his contact information and social security and drivers license numbers stored on ConDevel's human resources database. (R. at 2, 5) This knowledge provided Baylor the opportunity to mitigate any potential damage by requesting a fraud alert on his credit file, obtaining copies of his credit report, scrutinizing his account statements, and taking other protective measures. *See* Deborah Platt Majoras, Prepared Statement of the Federal Trade Commission, *Data Breaches and Identity Theft*, 2005 WL 1432201 (June 16, 2005) (describing basic approaches in disclosing a data breach). Under the GLBA and California's data protection statute, which impose disclosure requirements similar to the Act, Baylor already had information sufficient to serve the purpose of any disclosure that ConDevel could have made. Therefore, ConDevel's decision not to disclose additional information did not harm Baylor with respect to the Act.

Baylor informed ConDevel about the unauthorized acquisition of his computerized data. (R. at 5) This was the first time ConDevel had reason to suspect a security breach. Logically, ConDevel did not need to "disclose" to Baylor what he already knew. Neither the Act nor ConDevel's internal procedures required disclosure of additional information. Because Baylor had enough information to serve the purpose of the disclosure requirement, disclosure was unnecessary. Therefore, ConDevel respectfully requests this Court affirm summary judgment.

B. ConDevel Was Exempt Because Nesbit in Good Faith Acquired Baylor's Personal Information, Which Was Used for the Purposes Designated by ConDevel "and/or" Was Not Subject to Further Unauthorized Disclosure

A good faith acquisition is the "gaining of possession or control over something" absent a state of mind intending fraud or seeking an unconscionable advantage. *Black's Law Dictionary* 25 (Bryan A. Garner ed., 8th ed., West 2004). The undisputed facts show that Nesbit acquired Baylor's personal information in good faith when he obtained Baylor's login and passwords. Nesbit used the information for the purpose designated by ConDevel, and the personal information is not subject to further unauthorized disclosure. Therefore, ConDevel was exempt from the statute's disclosure requirement, and the appellate court properly affirmed summary judgment. *See Guillory v. Domtar Indus. Inc.*, 95 F. 3d 1320, 1326 (5th Cir. 1996) (noting that summary judgment is appropriate where material facts concerning state of mind are undisputed).

1. *Nesbit Acquired the Personal Information When he Obtained Baylor's Login and Passwords*

The Act does not define "acquisition." Where a statute does not define a term, courts interpret the term according to its ordinary meaning. *Texas Employment Com'n v. Ben Hogan Co.*, 854 S.W.2d 292, 295–96 (Tex. App. 1993); *McConnell v. Sutherland*, 898 P.2d 254, 257 (Or. App. 1995). Dictionaries provide the ordinary meaning of terms. *E.g. Texas Employment Com'n*, 854 S.W.2d at 296 (using *Black's Law Dictionary* to define "acquire"); *In re Marriage of Massee*, 970 P.2d 1203, 1212 (Or. 1999) (using *Webster's Third New Int'l. Dictionary* to define "acquisition").

"Acquisition" is the "gaining of possession or control over something." *Black's Law Dictionary* 25 (Bryan A. Garner ed., 8th ed., West 2004). This definition contemplates only the actual moment when someone gains control and does not encompass the person's subsequent actions, such as how the person uses the item gained. Thus, the moment of acquisition occurs when someone gains possession or control over something. Under the Act, the relevant point of inquiry is the moment of acquisition because the Act exempts a company from having to disclose an employee's "[g]ood faith acquisition of personal information . . . ." 17 Marshall Code § 105(d). Therefore, the relevant point of inquiry is when Nesbit gained possession or control of Baylor's personal information.

Nesbit gained possession and control of this information when he acquired Baylor's login and passwords to access the human resources database. (R. at 4) Acquiring a password constitutes obtaining possession and control over information protected by the password. *United*

States v. Ivanov, 175 F.Supp.2d 367, 371-72 (D. Conn. 2001). In *Ivanov*, the federal government charged Ivanov with illegally accessing a corporation's protected computers in furtherance of fraud and gaining something of value. *Id.* at 370. From his home computer in Russia, Ivanov hacked into the corporation's computer system in the United States and obtained key passwords. *Id.* at 369, 370, 372. The passwords allowed Ivanov to copy, sell, transfer, alter, or destroy the data. *Id.* at 371. As Ivanov was able to do more than access and view the data, he had control over it. *Id.* He then transferred the data to a computer in Russia. *Id.* at 372. The court determined that Ivanov gained possession and control over computer data the moment he obtained passwords, not when he transferred the data. *Id.* at 371-72.

Therefore, *Ivanov* established three applicable rules. First, acquiring a password constitutes gaining possession or control over information protected by the password. *Id.* Second, having the ability to do more than access and view the data equates to having control over the data. *Id.* at 371. Third, gaining possession or control over protected computer data is separate from transferring and using the data. *Id.* at 371-72.

Combining these rules with the plain meaning of "acquisition" shows that Nesbit acquired Baylor's personal information when he acquired Baylor's login and passwords. Baylor was an executive vice president responsible for ConDevel's human resources department. (R. at 2) Accordingly, he had access to the human resources database, which includes all employees' personal information. (R. at 2) By acquiring Baylor's login and passwords, Nesbit could do more than simply access and view the data. For example, he was able to authorize membership cards in Baylor's name and receive the credentials at his home. (R. at 4) Therefore, like the defendant in *Ivanov*, Nesbit gained possession and control over information protected by Baylor's login and passwords prior to transferring the data. This constituted the "acquisition of personal information."

As in *Ivanov*, Nesbit's subsequent acts—transferring the files to his home computer and using the data to obtain memberships to exclusive clubs—were separate from his data acquisition. (R. at 4) Whether Nebit acted in good faith during these subsequent acts is irrelevant with respect to the Act, which exempts an agency from having to disclose an employee's "good faith acquisition of personal information." 17 Marshall Code § 105(d). Accordingly, the question is whether Nesbit acquired Baylor's login and passwords in "good faith."

2. *Nesbit Acquired the Login and Passwords in Good Faith*

The Act does not define "good faith." As courts have used dictionaries to define "acquisition," courts have used dictionaries to define "good faith" when a statute does not otherwise define it. *E.g., Bendiburg v. Dempsey*, 707 F.Supp. 1318, 1342 (N.D.Ga.,1989) *rev'd on other grounds*, 909 F.2d 463 (11th Cir. 1990); *Nicoletta v. Rochester Eye and Human Parts Bank, Inc.*, 519 N.Y.S.2d 928, 930 (N.Y. Sup. Ct. 1987). Where "acquisition" is defined by a particular moment, "good faith" is defined by a particular state of mind: "Absence of intent to defraud or to seek unconscionable advantage" constitutes good faith. *Black's Law Dictionary*, at 713.

The undisputed facts show that Nesbit acted in good faith when he acquired Baylor's login and passwords because he did not intend to defraud or seek unconscionable advantage. Before he acquired Baylor's login and passwords, Nesbit told his supervisor that he felt ConDevel's technology infrastructure was vulnerable. (R. at 3) Nesbit wanted to raise management's awareness of the vulnerabilities and to act as a team player and problem solver. (R. at 4) ConDevel's Computer Usage Policy mandated, "employees are responsible for safeguarding all equipment and software provided by the company." (R. at 3-4) However, the Policy did not define or restrict what constituted appropriate safeguarding measures. (R. at 2) Thus, Nesbit planned to use his keylogger program to access files in the human resources database so that he could submit a full report to management. (R. at 3) This uncontested chain of events indicates that Nesbit did not intend to defraud or seek unconscionable advantage. Therefore, he acted in good faith at the moment of acquisition.

Nesbit complied with the Computer Usage Policy by attempting to safeguard ConDevel's computer system. (R. at 2) Nevertheless, Baylor may argue that Nesbit did not act in good faith because as a salesman, he was unauthorized to deal with technological issues. However, this argument misconstrues the scope of the Act. The Act requires disclosure of a security breach only under certain circumstances when an *unauthorized* person acquires computerized data. 17 Marshall Code § 105(a). The Act does not require disclosure of an *authorized* acquisition of computerized data. The Act simply is not that broad. Under the whole-act doctrine, courts should construe statutory provisions so as to render them consistent with the statute's scope. McKNIGHT v. MOUND BAYOU PUB. SCH. DIST., 879 So.2d 493, 497–98 (Miss. Ct. App. 2004). Consequently, the good-faith provision exempting a company from having to disclose an employee's acquisition must concern an acquisition only by an *unauthorized* employee. Therefore, any suggestion that Nesbit did not act in good faith simply because he was unauthorized to acquire the information misconstrues the scope of the Act. The Act itself contemplates that sometimes, employees, without authorization, acquire computerized data in good faith, 17 Marshall Code § 105(d), as Nesbit did here.

Nesbit acquired the login and passwords for the purpose of aiding ConDevel. (R. at 4) He did not intend to defraud or seek unconscionable advantage. Only after having acquired Baylor's personal information did Nesbit's good faith state of mind change. (R. at 4) Nesbit's subsequent state of mind is irrelevant with respect to the plain language of the Act. The exemption from the duty to disclose provides that "good faith acquisition of personal information by an employee or agent of the agency is not a breach of the security of the system . . . ." 17 Marshall Code § 105(d). A basic rule of statutory interpretation is to interpret terms according to their plain meanings. *Gonzalez v. McNary*, 980 F.2d 1418, 1420 (11th Cir. 1993). The plain meanings are dispositive unless the legislature has clearly expressed a contrary intent. *Id.* The legislature defined the phrase "breach of the security of the system." 17 Marshall Code § 105(d). This shows that when the legislature intends to define a term or phrase in a particular way, the legislature clearly expresses that intent. The legislature chose not to define "[g]ood faith acquisition." Thus, the legislature has not clearly expressed an intent that those terms mean anything but their ordinary meaning. When Nesbit acquired the personal information, he had only a good faith state of mind. (R. at 4) Therefore, Nesbit acquired Baylor's personal information in good faith.

3. The Personal Information Was Used for the Purposes Designated by ConDevel "and/or" is Not Subject to Further Unauthorized Disclosure

If an employee acquires personal information in good faith, the employer is exempt from disclosing the acquisition, "provided that the personal information is used for the purposes designated by the agency *and/or* is not subject to further unauthorized disclosure." 17 Marshall Code § 105(d) (emphasis added). Therefore, an employee's good faith acquisition coupled with either the designated use of the personal information or the lack of further unauthorized disclosure, or both, exempts a company from having to disclose the acquisition of personal information. The "and/or" language indicates that either one, or both, is sufficient.

Nesbit used Baylor's personal information for the purpose designated by ConDevel. ConDevel designated the use of the information in the "VIP Program" files for obtaining memberships to exclusive clubs. (R. at 4) Nesbit accessed the "VIP Program" files and used Baylor's information to obtain memberships to exclusive clubs. (R. at 4) Nesbit did not otherwise use Baylor's personal information. Therefore, Nesbit used Baylor's personal information for the purpose designated by ConDevel. That Nesbit lacked authority to use this information means only that he was the wrong person to use it, not that he used the information for a purpose not designated by ConDevel.

Baylor may emphasize that the original purpose of the "VIP Program" was "to attract and foster loyalty among top executives." (R. at 2) Thus, Baylor may conclude that since Nesbit used the information for his personal benefit, he did not use the information "for the purposes designated by the agency." However, "designated purposes" do not include mere incidental benefits that may flow from the use. *Drager by Gutzman v. Aluminum Indus. Corp.*, 495 N.W.2d 879, 883 (Minn. Ct. App. 1993). For example, the ordinary designated purpose of a window screen is to allow for ventilation and to prevent the ingress of insects. *Id.* Although the window screen may also prevent people from falling out of the window, this benefit is incidental to the window screen's primary purpose. *Id.* Likewise, here, the purpose for using the information in ConDevel's "VIP Program" files is to obtain memberships to clubs. Although the ability to obtain these memberships may attract and foster loyalty among top executives, this benefit is incidental to the primary purpose of using the information in the "VIP Program" files.

Thus, any suggestion that Nesbit failed to further the original purpose of the "VIP Program" misdirects the inquiry to an incidental benefit of using the information and away from the Act's plain language, which simply considers whether "the personal information is used for the purposes designated by the agency." 17 Marshall Code § 105(d). The legislature did not express a clear intent that this phrase means anything but its plain meaning. *See Gonzalez*, 980 F.2d at 1420 (asserting that plain meanings of statutory terms are dispositive absent clear legislative intent to the contrary). Here, ConDevel designated the use of the information in the "VIP Program" for obtaining memberships to clubs. (R. at 4) Nesbit used Baylor's information for that purpose. (R. at 4) Therefore, Nesbit used Baylor's personal information for the purpose designated by ConDevel.

Moreover, Baylor's personal information is not subject to further unauthorized disclosure. As soon as ConDevel learned of Nesbit's actions, ConDevel fired Nesbit, and the technology support department tightened security. (R. at 5) ConDevel investigated the matter and found that no one outside the company accessed the files. (R. at 5) These actions ensured that Baylor's personal information is not subject to further unauthorized disclosure.

Baylor may argue that the information is subject to further unauthorized disclosure because Nesbit downloaded the human resources files to his home computer. (R. at 4) However, this argument portrays an unworkable standard for the good-faith exemption. Courts violate established principles of statutory interpretation by creating unworkable standards. *Town of Dover v. Massachusetts Water Res. Auth.*, 607 N.E.2d 1001, 1004 (Mass. 1993). Once a person has acquired information, that information is almost always subject to further disclosure. The person might have copied the information or simply memorized it. Ensuring that acquired information is not subject to further unauthorized disclosure by the one who acquired the information creates an unworkable standard because the company would have to disclose even inadvertent or harmless breaches.

This standard would render the Act inconsistent with parallel federal law. The duty to disclose under the Act is similar to a duty to disclose security breaches under the GLBA. 15 U.S.C. § 6801; 70 Fed. Reg. at 15736. Under the GLBA, financial institutions should notify affected customers of a security breach only after becoming aware of an incident, conducting a reasonable investigation, and then determining the likelihood that misuse of information has occurred or is reasonably possible. 70 Fed. Reg. at 15752. Accordingly, the GLBA discourages financial institutions from notifying customers of a security breach prematurely or unnecessarily. *Id.* at 15743. The concern is that notifying customers of every possible fraud or identity theft would "needlessly alarm customers where little likelihood of harm exists." *Id.* Customers should not receive notices "that would not be useful to them" because they would eventually regard frequent false alarms as commonplace. *Id.* These false alarms would dilute the effectiveness of legitimate notices. *Id.*

Rather, since acquired information is always subject to further disclosure, a workable standard should require that the company take steps to ensure that the information it possesses is not subject to further unauthorized disclosure. Here, ConDevel took those steps. As soon as ConDevel learned of Nesbit's actions, ConDevel fired Nesbit and tightened security. (R. at 5) ConDevel investigated the matter and concluded that no one outside the company accessed the files. (R. at 5) Thus, ConDevel ensured that Baylor's personal information is not subject to further unauthorized disclosure.

Nesbit acquired Baylor's personal information in good faith because he obtained Baylor's login and passwords in an attempt to help ConDevel. Nesbit used the information for the purpose designated by ConDevel, and ConDevel ensured that the information is not subject to further unauthorized disclosure. Thus, Nesbit's actions did not constitute a "breach of the security of the system," so ConDevel did not have a duty to disclose Nesbit's actions. Consequently, ConDevel respectfully requests this Court affirm summary judgment.

CONCLUSION

Baylor failed to state a claim, if recognized, against ConDevel for intrusion upon seclusion. ConDevel has the right to access its business records. The undisputed facts show that Nesbit did not act on ConDevel's behalf and ConDevel did not ratify Nesbit's actions. Further, the alleged intrusion was not highly offensive to a reasonable person and did not cause Baylor the requisite anguish and suffering.

Baylor also failed to raise a genuine issue of material fact on whether ConDevel was exempt from Marshall's Data Protection Act. As the undisputed facts show, Baylor already knew the information that the Act would have required ConDevel to disclose, so disclosure was unnecessary. Further, ConDevel was exempt because Nesbit acquired Baylor's personal information in good faith and used it for the purpose designated by ConDevel, and the personal information is not subject to further unauthorized disclosure.

Because Nesbit failed to state a claim and presented no genuine issues of material fact, ConDevel respectfully requests this Court affirm summary judgment on both claims.

CERTIFICATE OF SERVICE

We hereby certify that a true and correct copy of the above and foregoing Brief for the Respondent was mailed by first-class certified mail, return receipt requested, to all counsel of record on this 24th day of September 2007.

Respectfully Submitted,

____

Attorneys for Respondent

APPENDIX A:

Restatement (Second) of Torts, § 652(B) (1977)

§ 652(B). Intrusion Upon Seclusion

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

APPENDIX B:

17 Marshall Code § 105 (2006)

Data Protection Act, § 105 Disclosure of Breach

(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Marshall whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore reasonable integrity of the data system.

(d) For purposes of this section, "breach of the security system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency is not a breach of the security of the system, provided that the personal information is used for the purposes designated by the agency and/or is not subject to further unauthorized disclosure.

(f) Notwithstanding subsection (c), a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(g) Any and all data subjects within the State of Marshall shall have a civil action against any data collector that obfuscates evidence of a breach or makes an informed choice to not inform data subjects of a breach.

APPENDIX C:

California Civil Code § 1798.29 (West 2007)

§ 1798.29. Agencies owning, licensing, or maintaining, computerized data including personal information; disclosure of security breach; notice requirementsA-3

(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods.

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision

(g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

APPENDIX D:

Indiana Code § 24-4.9-3-1 (West 2006)

24-4.9-3-1 Duties of data base owner

Sec. 1. (a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose:

(1) unencrypted personal information was or may have been acquired by an unauthorized person;

or

(2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

(b) A data base owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

A-5