

SUMMARY OF ARGUMENTS

I

The Grant County District Court erred in granting summary judgment in favor of the Defendant / Appellee ConDevel and the Fourth Circuit Court of Appeals of the State of Marshall erred in affirming the same. ConDevel moved for summary judgment on the violation of the notification statute and on the intrusion upon seclusion count. Summary judgment is a request that the Court enter judgment without trial because there is no genuine issue of “material fact” to be decided by the fact-finder, that is, because the evidence is legally insufficient to support a verdict in the non - movant's favor. Issuance of summary judgment can be based only upon the Court's findings that:

1. There are no issues of "material fact" requiring a trial for their resolution, and
2. In applying the law to the undisputed facts, one party is clearly entitled to judgment.

Summary judgment was granted in favor of ConDevel inspite of the presence of "material facts" that indicate that the tort of invasion of privacy in the form of intrusion upon seclusion was committed and that there was a clear breach of personal security which is actionable under the Marshall Data Protection Act, 17 Marshall Code § 105 (2006).

The fact that Nesbit “eavesdropped” on Baylor's telephonic conversation and on overhearing that he was leaving for a meeting “right now” waited till he left and then gained access to Baylor's office and installed a keylogger program on his computer, indicate the presence of “material facts” to prove that the tort of intrusion upon seclusion was committed.

The “material facts” that indicate that there was a violation of the notification statute include that the e-mail address that sent the data from Baylor's computer to Nesbit via the keylogger program was traced to Nesbit. Also Nesbit had access to all employees' personal data files that contained classified information. Nesbit used this information to avail of membership to prestigious clubs through ConDevel's “VIP Program.” He also downloaded the human resources database on his home computer.

In view of the presence of the above material facts the Grant County District Court erred in granting summary judgment in favor of ConDevel and the Fourth Circuit Court of Appeals erred in affirming the same.

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.

The Court of Appeals erred in affirming the Order of the Grant County District Court and subsequently failed to recognize the tort of intrusion upon seclusion. The tort of intrusion upon seclusion under the Restatement (Second) of Torts § 652B is recognized by majority of the States in the United States of America. In tort law, the right of privacy has been defined as “the right to be let alone.” In making the determination of intrusion upon seclusion, the Court should consider all the circumstances including the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruders motives and objectives, the setting into which he intrudes and the expectations of those whose privacy is invaded.

The Fourth Circuit Court of Appeals of the State of Marshall stated that the tort of intrusion consists of the following elements: (1) unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion is offensive or objectionable to a reasonable

person, (3) the matter of the intrusion is private; and (4) the intrusion causes anguish and suffering.

Baylor was an executive vice president at ConDevel. He was responsible for operations, sales and the human resources department. He had worked hard and climbed up the ranks at ConDevel from a sales associate position which he started twenty-five years ago, to his current position as vice president. He was a valued employee and over the years, had helped grow the company's revenue several fold. By virtue of his position, Baylor had access to all employees' electronic personnel files including his own. Such files contained employee contact information, social security numbers, driver's license numbers, employee performance evaluation, employee personal data, employee benefits information, employee awards and honors and other personal data.

Therefore, Baylor held a key position in ConDevel, and had access to information which only he was entitled to by virtue of his seniority and position of responsibility as that of an executive vice president of ConDevel.

Nesbit was a young sales associate at ConDevel. He graduated from college a couple of years ago. He was considered smart, very ambitious and was also quite tech savvy. He enjoyed many forms of hi-tech information including computer gaming, blogging and social networking websites. He felt that information should be free and was a big fan of the so-called "security sites". Through these illicit sites that make public information about computer vulnerabilities and provide instructions for hackers, Nesbit had gained a basic understanding of various security exploits and had also dabbled with some very basic hacks. (R. 2)

Nesbit also wanted to take a quick ladder to the top of his company and enjoy all the benefits and perks of the top-ranked executives. He had frequently expressed to his colleagues his disappointment that he would have to wait for years before enjoying any

of the benefits restricted to the high level employees. He had been heard to say jokingly, "I wonder if there is any other way to enjoy the good life reserved to the executives."

(R. 2)

In light of the above facts, it is stated that Nesbit's intention was to attain success in a short time. Privacy torts are intentional torts; therefore, it is axiomatic that the actor must have intent. The three most basic elements of intent are: (1) It is a state of mind; (2) About the consequences of an act (or omission) and not about the act itself; (3) It extends to not only having in mind a purpose or desire to bring about a given consequence but also to having in mind a belief (or knowledge) that the given consequences are substantially certain to result from the act. It is also essential that the state of mind exists when the act occurs. An action for the intrusion upon seclusion theory of invasion of privacy focuses on the manner in which the information was obtained, not on the information's publication; in this respect, the claim is analogous to a trespass except that a physical intrusion of property is unnecessary.

Nesbit obtained information from Baylor's computer surreptitiously, that is, he was marked by quiet and caution and secrecy and he did that in an unauthorized manner, thereby satisfying the first ingredient of intrusion upon seclusion which is unauthorized intrusion upon another's seclusion.

Nesbit downloaded all of the human resource database files on his home computer. Examining Baylor's file, Nesbit noticed that Baylor had not joined many of the executive clubs available to him via ConDevel's executive package. Nesbit accessed the benefit system and had several credentials issued to Baylor, but sent to Nesbit's home address. The credentials included a membership card to the Marshall League Club, the most exclusive private social club in the State. Nesbit started frequenting the

Marshall League Club and several other establishments, gaining entry by using credentials issued in Baylor's name.

To state a cause of action for invasion of privacy, a plaintiff must aver that there was an intentional intrusion on the seclusion of his or her private concerns which was substantial and highly offensive to a reasonable person, and aver sufficient facts which could establish that the information disclosed would have caused mental suffering, shame, or humiliation to a person of ordinary sensibilities.

Baylor at the first instance was embarrassed at the Shady links with his friends and subsequently at Les Deux Pommes when he went with his family. He was humiliated on two occasions.

For an employer to be found liable for intrusion upon seclusion, some Courts require a physical intrusion by the employer. The matter intruded upon by Nesbit was in Baylor's "zone of solitude" and of a highly confidential nature and included files containing employees' electronic personnel data, including Baylor's own details, contact information, social security numbers, driver's license numbers, employees performance evaluations, employees salary data, employees benefits information, employee awards and honors and other personal data by virtue of which the information so intruded upon is private.

Therefore in the instant case, the four elements required to prove the tort of intrusion upon seclusion fall squarely in the ambit of the instant case.

II

Some States within the United States of America accept the general principles of data protection from the various federal laws available on the subject. However, each State has their own interpretation and judgments of the theories and concepts of data protection law.

§ 105 (d) of the Marshall Data Protection Act highlights a “breach of the security of the system”. As per the Act, a breach is considered to occur when there is any unauthorized acquisition of computerized data. The actions of Nesbit were clearly unauthorized and he did not have the right to access the computerized data from Baylor’s computer.

The undisputed facts of the case clearly state that Nesbit was fascinated by the opportunity that the executives at ConDevel were given and had a “change of heart.” This clearly shows that there was no “good faith” and the Grant County District Court and Court of Appeals of the State of Marshall have erred in holding that ConDevel’s employee Nesbit acquired information in good faith. Further, Nesbit was always aware and in want of the privileges and benefits that were derived from ConDevel’s “VIP Program.” Due to the information gained by his unauthorized access he was tempted to use the facilities available in the “VIP Program” to his benefit. In accordance with this intention, Nesbit started using the benefit system and issued several membership cards and other services in Baylor’s name, but for his own personal use.

The above facts and Nesbit’s actions and intentions are *res ipsa loquitor* that the breach of the security of the system was a result of an unauthorized acquisition of computerized data. Nesbit was clearly unauthorized to access this data and therefore the provisions of § 105 (d) of the Marshall Data Protection Act apply in this instant case.

Further, § 105 (d) of the Marshall Data Protection Act, talks of “good faith acquisition of personal information.” This section emphasises that if the personal information is acquired by an employee or agent of the agency in good faith then such an acquisition is not considered to be a breach of the security system. Therefore, this section lays down the exception of the “good faith” criteria in determining the intention behind the acquisition of the data. Such acquisition is further allowed only if it is used for the purposes designated by the agency and / or is not subject to further unauthorized disclosure. 17 Marshall Code § 105 (2006) of the Data Protection Act § 105 (d).

“Good faith” is a state of mind consisting in: (i) honesty in belief or purpose; (ii) faithfulness to one's duty or obligation;(iii) observance of reasonable commercial standards of fair dealing in a given trade or business, or (iv) absence of intent to defraud or to seek unconscionable advantage. Nesbit clearly had none of the above ingredients of a “good faith” state of mind.

On learning about the security breach, ConDevel’s management fired Nesbit. This act of theirs is proof of the fact that Nesbit indeed was guilty of the crime. However, the management decided that it was in the interest of the reputation of the company not to let anyone know that a security breach had happened. They feared a lawsuit or a scandal and so the company’s chief operation officer and the director of the technology support department decided that this information was best kept concealed.

This act of hiding the fact that a data security breach had occurred makes ConDevel directly liable under § 105 (g) of the Data Protection Act. Following their discovery, ConDevel’s management tightened the security system. Further, they did not offer any investigation details to Baylor and neither did they offer to assist Baylor in rebuilding his good name. The facts are clear that ConDevel made an informed choice not to inform the data subjects of a breach. Therefore they are guilty of violation of the

provisions of the said Act and are therefore liable to pay Baylor monetary and punitive damages as the section provides.

ARGUMENTS

I. The Fourth Circuit Court of Appeals erred in affirming the summary judgment of the Grant County District Court and subsequently holding that the surreptitious installation of a so-called “keylogger” on the Appellant’s computer did not state a claim for a recognized tort of invasion of privacy under the theory of intrusion upon seclusion.

A. The Fourth Circuit Court of Appeals erred in affirming the summary judgment that was granted by the Grant County District Court.

The Plaintiff / Appellant Ron Baylor hereby submits that the Grant County District Court as well as the Fourth Circuit Court of Appeals of the State of Marshall erred in granting a summary judgment in favor of the Defendant / Appellee ConDevel .

The Federal R. Civ. P., Rule 56 (c) states:

Motion and Proceedings Thereon.

The motion shall be served at least 10 days before the time fixed for the hearing. The adverse party prior to the day of hearing may serve opposing affidavits. The judgment sought shall be rendered forthwith if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law. A summary judgment, interlocutory in character, may be

rendered on the issue of liability alone although there is a genuine issue as to the amount of damages.

In the instant case ConDevel moved for summary judgment on the violation of the notification statute and on the intrusion upon seclusion count.

Under Rule 56 of the Federal Rules of Civil Procedure, 28 U.S.C.A., which provides for summary judgment, it was not intended to deprive litigants of a right to full hearing on the merits if any issue of fact exists. The procedure was not intended to be used as a substitute for regular trial where the outcome of the litigation depends upon disputed questions of fact. *Avrick et al. v. Rockmont Envelope Co.*, 155 F.2d 433; *Parmelee v. Chicago Eye Shield Co.*, 157 F.2d 582; *Sartor v. Arkansas Natural Gas Corporation*, 134 F.2d 433; *Rogers v. Girard Trust Co.*, 159, F.2d 239; *Peckham v. Ronrico Corporation*, D.C., 7 F.R.D. 324; *Merchants Indemnity Corporation of New York v. Peterson*, 3 Cir., 113 F.2d 4; *Toebelman v. Missouri-Kansas Pipe Line Co.*, 3 Cir., 130 F.2d 1016.

Summary judgment is a request that the court enter judgment without a trial because there is no genuine issue of “material fact” to be decided by a fact-finder, that is, because the evidence is legally insufficient to support a verdict in the non movant's favor.

All doubts as to the existence of a genuine issue as to a material fact must be resolved against the party moving for a summary judgment. *Sarnoff et al. v. Ciaglia*, 3 Cir., 165 F.2d 167; *Weisser v. Mursam Shoe Corporation*, 2 Cir., 127 F.2d 344, 145 A.L.R. 467; *Doehler Metal Furniture Co., Inc., v. United States*, 2 Cir., 149 F.2d 130.

In passing upon a motion for summary judgment, it is no part of the Court's function to decide issues of fact but solely to determine whether there is an issue of fact to be tried. *Walling v. Fairmont Creamery Co.*, 8 Cir., 139 F.2d 318; *Belanger et al. v.*

Hopeman Bros., F.R.D. 459; *Norton v. Schotmeyer*, D.C., 72 F.Supp. 188; *Ulen v. American Airlines*, D.C., 7 F.R.D. 37.

An issue of this kind precludes entry of summary judgment. A party moving for summary judgment may refer to any evidence that would be admissible if there were to be a trial such as, dispositions, party admissions, documents received during discovery (such as contracts, e-mails, letters and certified government documents). Each party may present to the Court its view of applicable law by submitting a legal memorandum in support of, or in opposition to, the motion. The Court may allow for oral arguments of the lawyers generally where the judge wishes to question the lawyers on issues in the case.

Issuance of summary judgment can be based only upon the Court's finding that:

1. There are no issues of "material fact" requiring a trial for their resolution;
and
2. In applying the law to the undisputed facts, one party is clearly entitled to judgment.

In the instant case the summary judgment was granted in the favor of ConDevel in spite of the presence of "material facts" clearly indicating that the tort of invasion of privacy in the form of intrusion upon seclusion was committed and there was a clear breach of personal security which is actionable under the Marshall Data Protection Act, 17 Marshall Code, § 105 (2006).

The "material facts" which indicate that the tort of intrusion upon seclusion was committed include:

1. Nesbit "eavesdropped" on Baylor's telephonic conversation. He overheard him say that he was leaving for a meeting "right now" and was therefore able to gain easy access to Baylor's office once he left.

2. The fact that Nesbit in the absence of Baylor entered his office and installed a keylogger program on his computer.

The “material facts” that indicate that there was a violation of the Marshall Data Protection Act include:

1. The e-mail address that sent the data every midnight from the keylogger program that was installed on Baylor’s computer was traced to Nesbit.
2. It was because Nesbit had access to the employees’ personnel data files that contained classified information such as their social security numbers, driver’s license numbers, employee benefits information, etc, that he was able to avail of membership at exclusive clubs and lounges on Baylor’s name.
3. On receiving the data via the keylogger program by a private e-mail address, Nesbit downloaded the entire human resource database of ConDevel onto his home computer.

In view of the existence of the above “material facts” the Grant County District Court and the Fourth Circuit Court of Appeals in the State of Marshall erred in granting a summary judgment in favor of Defendant / Appellee ConDevel.

B. The Fourth Circuit Court of Appeals has erred in admitting whilst denying the tort of intrusion upon seclusion and has further erred in holding that if Baylor’s claim was to be recognized, it would fail as a matter of law.

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. Restatement (Second) of Torts § 652B.

The Fourth Circuit Court of Appeals erred in affirming the Order of the Grant County District Court and subsequently failed to recognize the tort of intrusion upon seclusion.

It is submitted that the tort of intrusion upon seclusion under the Restatement (Second) of Torts § 652B is recognized by majority of the States in the United States of America. In tort law, the right of privacy has been defined as “the right to be let alone”. Restatement (Second) of Torts § 652A cmt. a (1977).

The United States Supreme Court has recognized the existence of zones of privacy inherent in the First, Fourth, Fifth, Ninth and Fourteenth Amendments which deserve Federal protection. *Paul v. Davis*, 424 U.S. 693, 712-13 (1976).

The Constitutional right to privacy is limited to restricting the Government’s power to regulate private conduct in matters relating to marriage, procreating, contraception, family relationships, child-bearing and education.

As for other areas of privacy, the Court stated “the protection of a person’s general right to privacy – his right to be let alone by other people – is like the protection of his property and of his very life, left largely to the law of the individual States.” *Katz v. United States*, 389 U. S. 347, 350-351 (1967).

Therefore, it is imperative for a State to recognize a citizen’s right to privacy in order to protect his “right to be let alone”.

A similar situation currently exists in the State of Illinois, where in the Courts have had a difficulty in recognizing the tort of intrusion upon seclusion. There is a conflict amongst the State, District and Federal Courts as to who does or does not recognize this tort.

In *Lovgren v. Citizens First Nat'l Bank of Princeton*, 534 N.E.2d 987 (Ill. 1989), Lovgren brought an invasion of privacy action for unreasonable intrusion on seclusion. The trial Court granted the bank's motion to dismiss. The Third District Illinois Appellate Court reversed and remanded, holding that it recognized the tort in Melvin, and that Lovgren had pled sufficient facts to support an action.

Disagreeing with the Appellate Court, the Illinois Supreme Court found that Lovgren failed to state a cause of action for invasion of privacy based on unreasonable intrusion on seclusion. As a result, the Supreme Court vacated the Appellate Court's decision. The Supreme Court found, however, that Lovgren did state a cause of action for invasion of privacy based on false light.

The court reached this conclusion based on § 652B of the Second Restatement. The court acknowledged Prosser's four-branch model of invasion of privacy, which the Second Restatement embodies. Examining § 652B and the accompanying comments, the court noted that the gravamen of the privacy tort of intrusion on seclusion is “some type of highly offensive prying into the physical boundaries or affairs of another person. The basis of the tort is not publication or publicity. Rather, the core of this tort is the offensive prying into the private domain of another.” Turning to Lovgren's complaint, the court concluded that the offense and the harm caused by the offense were not the result of prying, but of publication.

Also in *Ludemo v. Klein*, 771 F. Supp. 260, 261 (N.D. Ill. 1991), the Federal District Court was presented with this question. After discussing Lovgren, the Court observed that the Illinois Supreme Court's decision was “disquieting.”

The Supreme Court expressly declined to decide whether the tort of invasion of privacy based on unreasonable invasion on seclusion existed in Illinois. Yet, the Supreme Court held that the specific facts of Lovgren did not meet the requirements for

an unreasonable intrusion upon seclusion. Thus, the District Court noted that the Supreme Court's holding seems to recognize the tort's existence. The District Court then held "that if forced to resolve this issue, the Illinois Supreme Court would hold that the tort exists."

Similarly, in the instant case the Court has stated that, "assuming arguendo, that we were to recognize this tort as actionable, Baylor's claim would fail because he cannot satisfy one or more elements of the cause of action. Therefore, the Fourth Circuit Court of Appeals of the State of Marshall infers that if Baylor can prove the requisite elements of the tort of inclusion upon seclusion then the claim of invasion of privacy would survive.

Further, where the Illinois Supreme Court has not directly confronted an issue, "[i]ntermediate Appellate Court cases are useful but not binding evidence of what the Illinois Supreme Court would do in a similar case." The local Federal Court must reach its decision based on the decisions of the Illinois Supreme Court, the Illinois Appellate Court, and other State Courts on the same issue.

Based on these principles, a local Federal Court, if faced with this question, should conclude that the tort of intrusion upon seclusion is viable in Illinois. Initially, the Illinois Supreme Court has expressly recognized both the general tort of the right to privacy and the Second Restatement branch of false light. Additionally, examining the four Appellate Court decisions on the question, the two decisions that refused to recognize the tort are older (at least twenty years), while the two decisions that recognize the tort are more recent. Also, most American jurisdictions have adopted Prosser's four-branch model formulated in the Second Restatement. From this weight of authority, it is logical to conclude that the Illinois Supreme Court should recognize the tort of inclusion upon seclusion. 30 Loy. U. Chi. L.J. 601.

In order to establish the tort of intrusion upon seclusion the burden lies upon the Plaintiff / Appellant Ron Baylor to prove the following elements of the tort of intrusion upon seclusion: (1) unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion is offensive or objectionable to a reasonable person, (3) the matter of the intrusion is private; and (4) the intrusion causes anguish and suffering.

(i) The Plaintiff / Appellant submits that Steve Nesbit's intrusion upon Plaintiff / Appellant Ron Baylor's seclusion from his private place of working was unauthorized.

In making the determination of intrusion upon seclusion, the Court should consider all the circumstances including "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruders motives and objectives, the setting into which he intrudes and the expectations of those whose privacy is invaded." *Berosini*, 895 P.2d at 1282 (quoting *Miller*, 232 Cal. Rptr. at 679).

Baylor was an executive vice president at ConDevel. He was responsible for operations, sales and human resources department. He had worked hard and climbed up the ranks at ConDevel from a sales associate position at which he started twenty-five years ago, to his status as vice president. He was a valued employee and over the years, has helped grow the company's revenue several fold. By virtue of his position, Baylor has access to all employees' electronic personal files including his own. Such files contained employee contact information, social security numbers, drivers license numbers, employee performance evaluation, employee personal data, employee benefits information, employee awards and honors and other personal data. (R. 2).

Therefore, Baylor held a key position in ConDevel, and had access to information which only he is entitled to by virtue of his seniority and position of responsibility.

Nesbit was a young sales associate at ConDevel. He graduated from college just a couple of years ago. He was considered smart, very ambitious and was also quite tech savvy. He enjoyed many forms of hi-tech information including computer gaming, blogging and social networking websites. He felt that information should be free and was a big fan of the so-called “security sites”. Through these illicit sites that make public information about computer vulnerabilities and provide instructions for hackers, Nesbit had gained a basic understanding of various security exploits and had dabbled with some very basic hacks. (R. 2)

Nesbit also wanted to take a quick ladder to the top of his company and enjoy all the benefits and perks of the executives. He had frequently expressed to his colleagues his disappointment that he would have to wait for years before enjoying any of the benefits restricted to the high level employees. He had been heard to say jokingly, “I wonder if there is any other way to enjoy the good life reserved to the executives.” (R. 2)

In light of the above facts, it is stated that Nesbit’s intention was to attain success in a short time. Privacy torts are intentional torts; therefore, it is axiomatic that the actor must have intent. The three most basic elements of intent are:

- (i) It is a state of mind;
- (ii) About the consequences of an act (or omission) and not about the act itself;
- (iii) It extends not only having in mind a purpose or desire, to bring about a given consequence but also to having in mind a belief (or knowledge) that given the consequences are substantially certain to result from the act. It is also essential

that the state of mind exists when the act occurs. W. Page Keeton, et al. Prosser and Keeton on Torts § 8, p.34.

On or about April 25, 2005, Nesbit eavesdropped on Baylor's telephonic conversation and overheard him saying that he would be leaving for a meeting "right now." Nesbit realized that none of the other employees were in the vicinity of Baylor's office, so he stepped into Baylor's office to look around. (R. 3). Prima facie, the conduct of Nesbit was unauthorized and he ought not to have intruded into Baylor's office. In *Judith Ann Harkey v. Michael Abate*, 131 Mich App. 177; 346 N.W.2d 74; 1983 Mich. App. LEXIS 3498, a mother and daughter claimed an invasion of their privacy. The court held that the installation of the hidden viewing devices could itself constitute a sufficient wrongful intrusion so as to permit recovery, because it consisted solely of an intentional interference with their interest in solitude or seclusion of a kind that would be highly offensive to a reasonable person. The court held that the trial court erred in granting the summary judgment. After the applicable statute of limitations had expired, mother and daughter determined that the title to the roller-skating facility was held by a corporation, and sought leave to add the corporate entity as a defendant. The court held that because operator was the resident agent for the corporate entity, was its sole officer, and that he had knowledge, both personally and in his representative capacity of the corporate entity, of the litigation and of the intent to bring suit against the owner of the roller-skating facility, that the trial court abused its discretion in denying leave to amend; see also *Rhodes v. Graham*, 37 S.W.2d 46, 47 discussing how common-law eavesdropping gives rise to a cause of action for invasion of privacy; see also *Souder v. Pendleton Detectives, Inc.*, 88 So. 2d 716, 718 (La. Ct. App. 1956) discussing how a

plaintiff has a cause of action for invasion of privacy when he or she shows that a defendant may have violated a “Peeping Tom” statute.

Further in the case of *Dietemann v. Time, Inc.*, 284 F. Supp. 925, 932 (C.D. Cal. 1968), aff’d, 449 F.2d 245 (9th Cir. 1971), speaking of such electronic eavesdropping, a local federal court similarly reasoned: “In plain language, it ruins the privacy. One would never obtain the full benefits accorded to a private place if he or she reasonably believed someone would or could be listening.” *Amati*, 829 F. Supp. at 1010.

Common Law liability for the invasion of privacy is limited to acts that constitute an “unreasonable intrusion into seclusion” because both Constitutional violations and tort liability are based on the reasonableness of the search or the intrusion; Courts often use the facts patterns and legal rationale of one in an analysis of the other. In cases involving privacy issues arising in searches of a work place, a seminal case is *O’Connor v. Ortega*, 480 U.S. 709, wherein the Court concluded that the record had not been developed to the extent that it could determine whether the access that hospital officials had to the plaintiffs office rendered any expectation of privacy to be unreasonable, it remanded the case. However, the Court held that the plaintiff had a reasonable expectation of privacy in his desk and file cabinets.

The application of the rationale of *O’Connor v. Ortega*, can be seen in the case of *Schowengerdt v. General Dynamics Corporation*, 823 F.2d 1328 (9th Cir. 1987) which was a case in a private employment setting. The Court found that the employee had a reasonable expectation of privacy in a locked desk containing correspondence and sexually explicit photographs.

Therefore, Baylor had reasonable grounds to expect absolute privacy in his personal office and did not expect anybody to intrude in his office and access confidential information. Nesbit out rightly breached Baylor’s privacy. It is an

established principle of law that corporate entities cannot claim breach of privacy. It is reasoned that a corporation cannot have the emotional feelings which are damaged in the privacy tort. *Felsher v. University of Evansville*, 755 N.E.2d 589 (Indiana 2001); see also *Austin Eberhardt & Donaldson Corp. v. Morgan Stanley Dean Witter Trust*, 2001 U.S. Dist.

In the case of *Doe 2 v. Associated Press*, 311 F.3d 417 (4th Cir. 2003) it was held that a defendant may be liable for a wrongful intrusion into private affairs if he or she has engaged in conduct that resembles watching, spying, prying, besetting or overhearing and the intrusion has invaded an area which one normally expects will be free from exposure to the defendant.

The Texas Court in the case of *Blanche v. First Nationwide Mortgage Corp.*, 74 S.W.3d 444 (Tex. App.Dallas 2002) held that the core of an invasion of privacy claim based upon intrusion into a plaintiff's solitude is the offence of prying into the private domain of another, not publication of results of such prying.

Nesbit designed a keylogger program that could be installed in someone else's computer (the target computer), where it could run unnoticed by an average user. The keylogger would record keystrokes made on the target computer and store them in a plain text file. Each day at midnight, the program would e-mail the day's text file back to Nesbit. He could then read the text file at his leisure and use it to discover user names, passwords and any other information entered via the target computers keyboard. Nesbit had set the program to send the e-mail to a private e-mail address which he maintained. It was his belief that using an address outside of ConDevel's network would make him more difficult to catch.

Further, an action for the intrusion upon seclusion theory of invasion of privacy focuses on the manner in which the information was obtained, not on the information's

publication; in this respect, the claim is analogous to a trespass except that a physical intrusion of property is unnecessary. *Lewis V. LeGrow*, 258 Mich. App. 175, 670 N. W. 2d 675 (2003). Nesbit obtained information from Baylor's computer surreptitiously i.e. he was marked by quiet and caution and secrecy and he did that in an unauthorized manner, thereby satisfying the first ingredient of intrusion upon seclusion which is that the intrusion was "unauthorized."

(ii) The Plaintiff / Appellant Baylor submits the following:

- 1. That the intrusion by Nesbit in his private place of working is objectionable or offensive to a reasonable man.**

- 2. That the intrusion upon seclusion so caused has defamed and damaged his reputation in Executive and Premier Clubs in the State of Marshall thereby causing him mental agony, anguish, stress and suffering.**

The Plaintiff / Appellant Baylor submits that in order for a claim of intrusion upon seclusion to be sustainable, it must be proved that the intrusion so alleged is objectionable or offensive to a reasonable man.

The privacy torts have been imported into the employment sector with one exception – seclusion claims. Regardless of the methods used to intrude in the plaintiff's seclusion, and there are many, the plaintiff must have had a reasonable expectation of privacy in order to recover. *Medical Laboratory Management Consultants v. ABC, Inc.*, 30 F.Supp. 2d 1188 (D. Ariz. 1998).

Courts have generally held that there is a reduced expectation of privacy in the work place. *Ali v. Douglas Cable Communications*, 929 F.Supp. 1362, 1382 (D. Kan. 1996). However, this is not the case if there exists a matter which is of an intimate or highly personal nature. In the case of *Sarah Borse v. Piece Goods Shop Inc.*, 963 F.2d 611, the court held that "there are areas of any employee's life in which his employer has no legitimate interest. An intrusion into one of these areas by virtue of the employer's power of discharge might plausibly give rise to a cause of action, particularly where some recognized facet of public policy is threatened." Further, the

Court held that “if discharge was related to a substantial and highly offensive invasion of the employee’s privacy, we believe that it would conclude that the discharge violated public policy.”

The intrusion must be highly offensive to a reasonable person. Restatement (Second) of Torts S. 652B cmt. d. To establish that an intrusion was objectively highly offensive, the evidence must show that the intrusion would cause mental suffering, shame or humiliation to a reasonable person. *Wolsen v. Lewis*, 924 F.Supp. 1413, 1420-21 (E. D. Pa. 1996). The concept of an intrusion being highly offensive to a reasonable person, is a part of the Restatement rule that many Courts have adopted in some variation or the other. *Wilcher v. City of Wilmington*, 139 F.3d 366, 40 Fed. R. Serv. 3d 934 (3d. Cir. 1988); see also *Lake v. Wal-Mart Stores, Inc.*, 582 N. W. 2d. 231 (Mimm. 1998); *Mauri v. Smith*, 324 Or. 476, 929 P.2d 307 (1996).

To state a cause of action for invasion of privacy, a Plaintiff must aver that there was an intentional intrusion on the seclusion of his or her private concerns which was highly offensive to a reasonable person, and must aver sufficient facts which could establish that the information disclosed was offensive. *McGuire v. Shubert*, 722 A.2d 1087 (Pa. Super. Ct. 1998).

The determination of what is highly offensive to a reasonable person is usually a question for the fact finder. A trial Court, however, must make a threshold determination of 'offensiveness' in discerning the existence of a cause of action for intrusion upon seclusion. *Miller v. National Board. Co.*, 232 Cal Repr. 668, 678-679.

In making this determination, the Court should consider all of the circumstances, including degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he

intrudes, and the expectation of those whose privacy is invaded. *Berosini*, 895 P.2d at 1282.

As also contended before, the intrusion must be into something that is considered private. Restatement (Second) of Torts § 652B cmt. c (1977). Thus, there is no liability for examining a public record concerning the plaintiff, or documents that the plaintiff is required to keep and make available for public inspection. *Id.*

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

After this incident, Nesbit decided to keep a low profile and refrained from using the membership card that had been issued in Baylor's name. Unbeknownst to Nesbit, many exclusive restaurants, social clubs and other establishments in the State of Marshall share a common "blacklist." When the Marshall League Club informed the other establishments that it had barred Baylor, other clubs revoked his membership, effectively blacklisting Baylor. Plaintiff /Appellant Baylor did not begin to suspect that his personal information had been misused until he tried to take some friends to play golf at Shady Links, a local private course, on June 1, 2005. Baylor was informed that

his membership had been revoked due to his behavior at the Marshall League Club. Baylor was deeply embarrassed and angry that he had never been informed of such a development. He wondered how he could have been barred from the Club when he was not a member and not been there in years.(R.4)

The following week, Baylor, attempted to take his family to Les Deux Pommes, an upscale restaurant. He was told that he was not welcome in the restaurant and informed that his inappropriate conduct at the Marshall League Club was the reason. Baylor demanded to see the manager.

The conversation became a heated argument and the restaurant manager shouted, “We do not want drunks and makers in our restaurant”.

Following this second embarrassment incident, Baylor concluded that someone must be posing and using his VIP benefits. (R.5)

In the case of *McGuire v. Shubert*, 722 A.2d 1087 (Pa. Super. Ct. 1998) it was held that “to state a cause of action for invasion of privacy, a plaintiff must aver that there was an intentional intrusion on the seclusion of his or her private concerns which was substantial and highly offensive to a reasonable person, and aver sufficient facts which could establish that the information disclosed would have caused mental suffering, shame, or humiliation to a person of ordinary sensibilities.”

Baylor at the first instance was embarrassed at the Shady links with his friends and subsequently at Les Deux Pommes when he went with his family. He was humiliated on two occasions.

For an employer to be found liable for an intrusion upon seclusion, some courts require a physical intrusion by the employer. *Gretencord v. Ford Motor Co.*, 538 F. Supp. 331 (D. Kan. 1982).

In the instant case Baylor was embarrassed for acts done by Nesbit. The case prima facie proves that Baylor went through anguish , humiliation and mental suffering because of the acts done by Nesbit.

(iii) The Plaintiff / Appellant Baylor submits that the matter intruded upon by Nesbit was from Baylor's zone of solitude and of a highly confidential nature and included files containing employees' electronic personnel files, including his own, contact information, social security numbers, driver's license numbers, employees performance evaluations, employees salary data, employees benefits information, employee awards and honors and other personal data by virtue of which the information so intruded upon is private.

In the case of *Wolf v Regardie*, 553 A.2d 1213 D.C.,1989, the court held that "Appellant brought suit alleging that the research done by the *Regardie's* staff in preparing the articles "intentionally and maliciously intruded on [his] private affairs and concerns ... in willful disregard for [his] rights to privacy, seclusion, and to be let alone." After protracted discovery, appellees moved for summary judgment. The trial court granted the motion on April 30, 1987. This appeal followed."

Nesbit had also accessed social security numbers. In a very important judgment *Bodah V. Lakeville Motor Express, Inc.*, 649 N.W. 2d 859 the court came across the situation where "Employees and former employees stated claim for invasion of privacy by dissemination of private information, where they alleged that employer sent their social security numbers to 16 affiliated business sites in six states" The court held that "Although social security numbers are private, they are available in a wide range of contexts in our society. We provide them to others continuously. One is daily exposed to the risk that someone at work, a government office, school, an accountant's office, a financial institution, or dozens of other settings may improperly use our social security numbers or provide these numbers to others who will do so. Misappropriation of social

security numbers is a pervasive risk of modern life. In all of the settings where these numbers are available, however, the entities with that information and their employees are bound by contractual and legal constraints to hold our social security numbers in confidence. Given the very sensitive and important nature of the social security numbers, these constraints are important to a functioning society. Social security numbers are not embarrassing personal-life details like an extramarital affair, nude photos, bad grades, an abortion, mental health problems, or financial difficulties depicted in many of the cited cases. Plainly, one does not want such tantalizing information publicized. Social security numbers are dry, sterile figures. But they are a private detail that enables the data voyeur to snoop or the thief to access financial details. A rash of identity theft incidents may flow from one disclosure. On the other hand, widespread dissemination of social security numbers within a business setting may not lead to any untoward results. Moreover, a person's bank account numbers, credit card numbers, personal identification numbers (PIN), and other similar identifiers may be considered just as sensitive as social security numbers. The damage is the substantial risk for misuse or illegal use of an individual's identity or financial information, not personal embarrassment.” For a defendant to be liable for invasion of privacy, his or her conduct must have been such that he or she should have realized that it would be offensive to persons of ordinary sensibilities. *Remsburg v. Docusearch, Inc.*, 149 N.H. 148, 816 A.2d 1001 (2003)

II. The Court of Appeals erred in holding that Appellee ConDevel was exempt from the notification provision of the Marshall Data Protection Act, 17 Marshall Code § 105 (2006).

Today in the United States, there are continuous instances of data breach occurring on a daily basis. A recent survey showed the methods of loss of information and the cost incurred to the company to gain the same data again. In light of this, security breach notification laws continue to multiply and security breaches have become common. Companies on the other hand face increasing pressure not only to address security breaches promptly and effectively, but also to implement systems and procedures to prevent them from occurring in the first place.

Some States within the United States of America accept the general principles of data protection from the various federal laws available on the subject. However, each State has their own interpretation and judgments of the theories and concepts of data protection law.

There are a few federal statutes available on this subject. § 1408 of The Identity Theft Protection Act requires private companies to take certain precautions to safeguard the personal information of consumers and to notify consumers whenever there is a breach in the security of their personal information. Section 2 would require covered entities to develop, implement, maintain, and enforce a written program containing administrative, technical, and physical safeguards to secure sensitive personal information.

Under § 1326 of the Notification of Risk to Personal Data Act, there is a requirement for agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

One of the relatively recent Bills by the Senate Committee on this subject is the Personal Data Privacy and Security Act of 2005. § 1789 of this Act proposes to establish new federal crimes relating to unauthorized access of sensitive personal information. The Bill would also require most government agencies or business entities that collect, transmit, store, or use personal information to notify any individuals whose information has been unlawfully accessed.

There also exists a Financial Data Protection Act of 2005, the main object of which is to protect the security of sensitive information relating to consumers in order to limit account fraud and identity theft. It lists down various data protection safeguards and its main focus is the protection of data pertaining to financial information.

H.R. 3997 – the Data Accountability and Trust Act (DATA) of 2006 would require private companies with access to consumers' personal information to take certain precautions to safeguard that information. Under the Bill, private companies would be required to notify consumers and the Federal Trade Commission (FTC) whenever there is a breach in the security of a consumer's personal information. Section 3 would require those private entities to notify each United States citizen or resident following the discovery of a security breach in which the individual's personal information was acquired by an unauthorized person.

Thus, through a few sections of these Acts, it can be seen that there are certain general principles which are universal to the subject of data protection. For example, for any form of data breach it is mandatory to inform the concerned parties of the breach. Also, there are obligations on companies to ensure that certain safeguards are in place to ensure that a breach does not occur in the first instance. In light of the same, the provisions of the Marshall Data Protection Act, 17 Marshall Code § 105 (2006) are

legally sound. The Act enumerates some of the basic principles of data protection that are followed throughout the United States of America.

The Federal Trade Commission (FTC) is a governing body on these laws. It lays down certain measures wherein companies and government agencies are accountable to the FTC. The FTC is particularly sensitive to companies that do not even take basic steps to protect personal information. If common, inexpensive security measures are not taken, businesses are at more risk of FTC action in the event of a breach or complaint. Companies should utilize all reasonable technological and security measures available, especially those that can be implemented at a reasonable cost. These include limiting employee access to computers with personal information to employees who require such access to perform their duties, limiting the access of those computers to the internet and installing low-cost but effective anti-hacking software on those computers containing sensitive customer information.

There are several International data protection laws like the Data Protection Act, 1998 of UK; The Norwegian Personal Data Regulations; The Hungarian Data Protection Act (Act LXIII Of 1992); German Data Protection Act and the EU Data Protection Act of 1998. These govern data protection laws within their countries and sometimes have provisions for international data breach situations.

A. § 105 (d) of the Act reads as follows, “For purposes of this section, ‘breach of the security of the system’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good Faith acquisition of personal information by an employee or agent of the agency is

not a breach of the security of the system, provided that the personal information is used for the purposes designated by the agency and / or is not subject to further unauthorized disclosure.”

§ 105 (d) of the Marshall Data Protection Act highlights a “breach of the security of the system”. As per the Act, a breach is considered to occur when there is any unauthorized acquisition of computerized data. The actions of Nesbit were clearly unauthorized and he did not have the right to access the computerized data from the computer of Baylor.

Nesbit was a young sales associate at ConDevel. On the other hand, Baylor was the executive vice-president of ConDevel and had been working there for the past twenty-five years. He was responsible for the operations, sales and human resources department. By virtue of his current position, Baylor had access to all employees’ electronic personnel files containing employee contact information, social security numbers, driver’s license numbers, employee performance evaluation, employee personal data, employee benefits information, employee awards and honors and other personal data. (R. 2).

Therefore, it can be clearly seen that Baylor was legitimately allowed access to these files as they formed a part of his job profile at ConDevel. However, this did not apply to Nesbit who was only a young sales associate in the company. Nesbit was unauthorized to access information of such a high security level which contained personal data of all the employees of ConDevel. This information was only meant for Baylor and no other person was authorized to access it.

Further, the Act reads that if data which compromises the security, confidentiality, or integrity of personal information is acquired it would result in a cause of action for breach of the security system of the agency.

Information such as employee contact information, social security numbers, driver's license numbers, employee performance evaluation, employee personal data, employee benefits information, employee awards and honors was all data that fell within the ambit of personal information. As mentioned above, Nesbit was unauthorized to have access to this information.

By installing the keylogger program in Baylor's computer, Nesbit gained access to all this personal information. Further, Nesbit was able to install this keylogger program only in a deceptive manner. It was only when he over heard a telephonic conversation that Baylor was engaged in, that Nesbit realized he could make use of his hacking and spyware knowledge.

On hearing that Baylor was leaving for a meeting "right now", Nesbit waited for Baylor to leave. As soon as he realized that there were no other employees in the area, he stepped into Baylor's office. Seeing that Baylor had left his computer on, Nesbit seized the opportunity presented to him and surreptitiously installed his keylogger on Baylor's computer. After doing this, Nesbit now had access to every keystroke that Baylor entered. This information helped Nesbit to gain access to Baylor's login and passwords including those which were used to access the employees' electronic personnel files.

It is stated that after installing the keylogger program, Nesbit got access to the personal information of the employees of ConDevel. He immediately became fascinated by the opportunities that the executives at ConDevel were given and had a "change of heart." This clearly shows that there was no "good faith" and the District Court and

Court of Appeals have erred in holding that ConDevel's employee Nesbit acquired information in "good faith."

Further, Nesbit was always aware and in want of the privileges and benefits that were derived from ConDevel's "VIP Program." Due to the information gained by his unauthorized access he was now tempted to use the provisions of the "VIP Program" to his benefit. In accordance with this intention, Nesbit started using the benefit system and issued several membership cards and other services in Baylor's name, but for his own personal use.

The above facts and Nesbit's actions and intentions are *res ipsa loquitor* that the breach of the security of the system was a result of an unauthorized acquisition of computerized data. Nesbit was clearly unauthorized to access this data and therefore the provisions of § 105 (d) of the Marshall Data Protection Act apply in this instant case.

Nesbit's acts are also unauthorized because he downloaded all the data on his personal computer which is outside the periphery of the company's management. It is needless to mention that no company can ever expect an employee to download sensitive company data on one's personal home computer. This act of Nesbit's is clearly outside the scope of the company's affairs and constitutes unauthorized access and therefore it is a "true" data breach contrary to the belief of the management of ConDevel.

Further, § 105 (d) of the Marshall Data Protection Act, talks of "good faith acquisition of personal information." This section emphasises that if the personal information is acquired by an employee or agent of the agency in good faith then such an acquisition is not considered to be a breach of the security system. Therefore, this section lays down the exception of the "good faith" criteria in determining the intention behind the acquisition of the data. Such acquisition is further allowed only if it is used

for the purposes designated by the agency and / or is not subject to further unauthorized disclosure. 17 Marshall Code § 105 (2006) of the Data Protection Act § 105 (d).

“Good Faith” is a state of mind consisting in:

- (i) honesty in belief or purpose,
- (ii) faithfulness to one's duty or obligation,
- (iii) observance of reasonable commercial standards of fair dealing in a given trade or business, or
- (iv) absence of intent to defraud or to seek unconscionable advantage. Black's Law Dictionary (8th ed. 2004).

As per the Black's Law Dictionary, “good faith” reflects honesty in belief or purpose. From the facts stated above, it has clearly been proved that there was no honesty either in belief or purpose in the actions of Nesbit. Nesbit deceptively, without anyone’s knowledge installed the keylogger on Baylor’s computer. Once he had access to ConDevel’s “VIP Program” he instantly misused the privileges available therein and became a member of various exclusive private social clubs in the State of Marshall. He began frequenting these clubs and several other establishments, gaining entry by using the credentials issued in Baylor’s name. These facts are self-explanatory of Nesbit’s true intentions. It clearly reflects that there was no honesty in belief or in purpose of the actions of Nesbit. His surreptitious installation of the keylogger program on Baylor’s computer was thus not done in “good faith.”

The second criterion of an action carried out in “good faith” is that there should be faithfulness to one’s duty or obligation. Nesbit was a young sales associate at ConDevel. By virtue of his job he did not have access to the human resource database of ConDevel that contained employees’ electronic personnel files. However, it had always been the desire of Nesbit to take the quick ladder to the top of the company and enjoy

all the benefits and perks of the executives. (R. 2). Nesbit had often expressed this intention of his to his colleagues and was heard to say, “I wonder if there is another way to enjoy the good life reserved to the executives.” (R. 2).

Keeping these facts in mind, the action of Nesbit installing the keylogger program in Baylor’s computer was not done in “good faith” and therefore ConDevel ought to have informed the other employees about the data breach that had occurred. Nesbit’s claim that he installed the keylogger program for the benefit of ConDevel – to expose the inefficient data security provisions they had - is untrue. On acquiring the very data that he claimed to have desired to prove to his seniors that “ConDevel was a data-breach waiting to happen”, Nesbit did not use it for this purpose. Instead, after the “change of heart” he misused the information to his own advantage and made use of as many benefits from this as he could avail of.

However, the “good faith” exception only operates provided there was no unauthorized disclosure. In the instant case Nesbit disclosed this information in disguise of Baylor and availed benefits which were meant only for top-ranked executives at ConDevel. This clearly shows that the breach cannot protect itself under the “good faith” clause.

If Nesbit desired, he could have used his advanced technological knowledge for the betterment of ConDevel. He could have proved that the corporate technology policies of ConDevel were not up to date and that the corporate information security measures were lacking. Nesbit was well aware of the fact that the current technology infrastructure of ConDevel and the prevailing minimal security mindset were naïve and not worthy of a company the size of ConDevel.

Being a bonafide employee of ConDevel, it fell within Nesbit’s ambit to owe a duty and obligation to his employers – ConDevel. Nesbit should have been faithful to

the company of which he was an employee. It is one of the basic duties and obligations that an employee owes to his employers. Nesbit owed an obligation to work and think for the benefit of the company. Upon learning of a method to cause a data breach, Nesbit should have pursued in his intention to make the management aware of the lack of data security measures in the company.

Nesbit's change of heart, wherein he misused the information regarding ConDevel's "VIP Program" to his own benefit, clearly shows that he was not faithful to one of the basic duties and obligations that an employee owes to his employer. Therefore, Nesbit was not faithful to his job as was required and further he failed in the basic duties and obligations that he owed the company.

This characteristic trait of Nesbit was realized by the management of ConDevel and therefore on learning that he was the person who had surreptitiously installed the keylogger program and caused the data breach, they fired him. This action of the management is self explanatory of the fact that Nesbit had been unfaithful to the company and could not be trusted as he had failed to prove himself in one of the core and basic duties that he owed to the company. Further, this action makes it clear that Nesbit's action were not those done in "good faith" and it was not a case where the personal information acquired was used for the purposes designated by the agency as per the requirements of § 105 (d) of the Marshall Data Protection Act. Therefore Nesbit can not guise his action under the exception provided in this section. His act was not done in "good faith."

Lastly, the fourth criterion in the definition mentions an absence of intent to defraud or to seek unconscionable advantage, if something is believed to be done in good faith. Nesbit's actions in the instant case are clear indications that he definitely had the intent to defraud. The fact that Nesbit took advantage of a conversation which he

over heard and then surreptitiously installed the keylogger program after entering Baylor's zone of solitude instead shows the presence of his intent to defraud, and not an absence of the same. After installing the keylogger program, Nesbit gained access to the personal information of Baylor and used Baylor's name to access ConDevel's "VIP Program." He misused the power that he had gained by his surreptitious installation and thus gained an unconscionable advantage for himself. Therefore, his action can not be held to be done in "good faith."

As per the definition of "good faith" Nesbit's actions cannot be said to be done with any good faith. Therefore, the exception provided for under the Data Protection Act under § 105 (d) cannot save Nesbit and his actions from punishment.

B. § 105 (g) of the Act reads as follows, "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."

§ 105 (g) of the Data Protection Act gives the right of civil action to subjects of the State of Marshall. It further lists down penalties for the same ranging from monetary damages and injunctive relief's to punitive damages.

After Baylor faced two consecutive instances of insult and defamation in two different executive clubs in the State of Marshall he realized that something was amiss. He soon drew the conclusion that some person must have obtained his personal details through ConDevel's human resource database. Upon investigation he found out that many membership cards had infact been issued on his name, more so which were allegedly issued by Baylor himself. He then thought that it could be possible that some

sort of corporate security breach had occurred. He informed the appropriate managers of the same and enlisted the help of the director of the technology support department. A full scan of Baylor's hard drive revealed the presence of a keylogger program and the source led to an email address which was Nesbit's. (R. 5).

On finding this out, ConDevel's management fired Nesbit. This act of theirs is proof that Nesbit indeed was guilty of the crime. However, the management decided that it was in the interest of the reputation of the company not to let anyone know that indeed a security breach had happened. They feared a lawsuit or a scandal and so the company's chief operation officer and the director of the technology support department decided that this information was best kept concealed.

This act of hiding the fact that a data security breach had occurred makes ConDevel directly liable under § 105 (g) of the Data Protection Act. Following their discovery, ConDevel's management tightened the security system and did not inform any one about the incident. Further, they did not offer any investigation details to Baylor and neither did they offer to assist Baylor in rebuilding his good name. The facts are clear that ConDevel made an informed choice not to inform the data subjects of a breach. Therefore they are guilty of the violations of the provisions of the said Act and are therefore liable to pay Baylor monetary and punitive damages as the section provides.

CONCLUSION AND PRAYERS

For the reasons set above, Plaintiff / Appellant Ron Baylor requests this Court to reverse the decision of the Fourth Circuit Court of Appeals of the State of Marshall, affirming the Order of the Grant County District Court, granting summary judgment in favor of Defendant / Appellee, ConDevel, Inc.

Further, the Plaintiff / Appellant, Ron Baylor requests this Court that it be held that:

(a) The Court of Appeals erred in holding that the surreptitious installation of a so called “keylogger” on the Appellant’s computer did not state a claim for a recognized claim of invasion of privacy under the theory of intrusion upon seclusion; and

(b) The Court of Appeals erred in holding that Appellee ConDevel was exempt from the notification provision of the Marshall Data Protection Act, 17 Marshall Code § 105 (2006); and

(c) The Plaintiff / Appellant Ron Baylor be awarded monetary damages of USD 100,000 as contemplated under the Marshall Data Protection Act, 17 Marshall Code § 105 (g) (1);

And any other orders that this Honorable Court may deem fit to give.

Respectfully Submitted

Counsel for the Plaintiff / Appellant