UIC John Marshall Journal of Information Technology & Privacy Law

Volume 24
Issue 1 *Journal of Computer & Information Law - Fall 2005*

Article 6

Fall 2005

2005 John Marshall International Moot Court Competition in Information Technology and Privacy Law: Brief for the Respondent, 24 J. Marshall J. Computer & Info. L. 133 (2005)

Cherish M. Keller

Elaine Wyder-Harshman

2005 MOOT COURT COMPETITION

BENCH MEMORANDUM

RICHARD C. BALOUGH
PIRYA KRISHNAMOORTHY VENKAT
DOUGLAS MACLEAN
LARISA V. MORGAN
MICHAEL ROGALSKI

IN THE SUPREME COURT OF THE STATE OF MARSHALL

BESS MARION, Defendant-Appellant,	)	
v.	)	No. 2005-CV-0237
EDDIE CAFKA AND ECC ENTERPRISES, INC. Plaintiffs-Appellee.	)	

I. INTRODUCTION

To help protect his trade secret, an inventor implanted a chip that controlled access to the information in his arm and in the arms of his employees. In spite of his efforts, the secret was misappropriated by a former employee along with other private information concerning the inventor. The secret ultimately was ultimately made public on the Internet. The inventor, Eddie Cafka ("Cafka"), filed suit against the employee, Bess Marion ("Marion"), for two counts of invasion of privacy (intrusion upon seclusion and public disclosure of private facts), as well as violation of the State of Marshall's anti-circumvention statute and misappropriation of trade secrets.[1] Defendant Marion filed a motion for summary judgment, which that the trial court granted. The appellate

1. R. at 3.

court of Marshall reversed the trial court and reinstated all four counts.[2] Marion appealed.

II. ISSUES PRESENTED FOR REVIEW

The Marshall Supreme Court granted leave to appeal on four issues:

1. Whether an unauthorized scanning of an implanted RFID chip is an invasion of the chip bearer's privacy.
2. Whether public disclosure of facts relating to a person's association with an anti-abortion group is actionable.
3. Whether breaking the encryption algorithm used by an RFID chip to generate serial numbers violates this state's anti-circumvention statute.
4. Whether the use of an RFID-based system and other measures is sufficient to protect a trade secret.[3]

III. STATEMENT OF THE CASE

The undisputed facts are as follows:[4] Eddie Cafka is a computer programmer and the sole shareholder of ECC Enterprises, Inc. ("ECC"), a company incorporated in the State of Marshall. The main business of ECC is to design and to build the next generation of computers using a technology where the image created by the computer is displayed into the user's brain, thereby eliminating the need for a computer screen. Cafka code- named the project "Music Man."

Being somewhat paranoid, Cafka attempted to conduct the project in total secrecy. To this end, he divided his employees into small work-groups so that no one employee knew the entire scope of the project. The workers were in different physical locations and were not given either the names or telephone numbers of the other employees. Each employee was required to have an Radio Frequency Identification ("RFID")[5] chip implanted in his or her right arm. The chip was activated when it sensed a radio frequency signal transmitted by a transponder located within a few meters. It responded to the signal by sending back a unique serial number. The serial numbers were protected using a cryptographic al-

---

2. R. at 8.

3. Order Granting Leave to Appeal, R. at 9.

4. The undisputed facts are set forth in the Appellate Court's decision in the RecordR. at 1-4.

5. *Wikipedia*, http://en.wikipedia.org/wiki/RFID (accessed June 15, 2006) (defining a Radio Frequency Identification (RFID) ais a method of identification, relying on storing and remotely retrieving data using devices called RFID tags, chips or transponders. An RFID chip is a small object that can be attached to or incorporated into a product, animal, or person).*Wikipedia*, http://en.wikipedia.org/wiki/RFID (accessed June 15, 2006).

gorithm.[6] The end result was that an employee could access only his or her computer. The doors to the office suites also were also controlled by the implanted RFID chip.

The normal procedure at ECC was to have each employee sign a non-disclosure agreement ("NDA") at the time of hire to prevent the actual or threatened disclosure of ECC's confidential and trade secret information.

Cafka routinely visited all of the ECC locations where the research and programming was occurring. Cafka himself had an RFID chip implanted;. h However, whereas an employee could only access his or her computer and see only the portion of the project that the employee was working on, Cafka's chip allowed him access to all employees' computers and the ability to view all of the research and programming.

Defendant Marion was one of the employee-researchers for ECC. By chance, her office was located next to Cafka's office. Marion was an excellent programmer. She had known Cafka since high school but her memories of him were negative. She took accepted the position at ECC not just only for the money, but also for the potential opportunity to learn about the Music Man project and to beat Cafka to market with a similar product. She resented Cafka's success and believed she knew more than he. Marion worked at ECC for six months before Cafka realized that she had not signed the NDA. He had her sign it immediately but did not give her any additional compensation for signing.[7]. Marion had an RFID chip implanted in her as a requirement for her continued employment.

While away from the office, Marion experimented with the implanted ECC RFID chip and reverse engineered the cryptographic algorithm that the chip generated. She built a transponder to simulate the transponder at the office. She then took her transponder to her office at ECC to collect information from Cafka's RFID chip as he passed by or entered her office. One night she returned to the ECC office to enter his office and to access the files on his computer. She downloaded the files to a thumb drive that she then took home. Upon reviewing the data, she was able to determine the scope of the Music Man project. In addition, she found a file that contained the membership list for an organization called Bash Abortion Now ("BAN"), an anti-abortion group that

6. *Webopedia,* http://www.webopedia.com/TERM/c/cryptography.html (accessed June 15, 2006) (explaining that cryptographic algorithm is aA method or formula used to protect information by transforming it (i.e., *encrypting* it) into an unreadable format, called cipher text. Only those who possess the formula or secret key can decipher (or *decrypt*) the message into plain text).*Webopedia,* http://www.webopedia.com/TERM/c/cryptography.html (accessed June 15, 2006).

7. R. at Appendix A to .

threatened doctors who performed abortions. Cafka was listed as the Grand Nowest of the group.

Shortly after Marion obtained the BAN list, the names of its members were anonymously posted on web blogs,[8] including Cafka's position with the group. These postings caused great embarrassment to Cafka. It also and caused him to lose funding for the project.

Two weeks after the BAN information appeared on the Internet, Marion quit working for ECC and started working for ECC's competitor, Softer Microns ("SM"). Three months later, SM announced it was developing a new product that displayed images directly in the brain of the users.

Cafka became suspicious of the BAN revelation and the new product announcement. He then searched through his computer logs and found that the files were downloaded at a time when Marion was in the office. He filed the present lawsuit against her alleging:

1. Intrusion upon his seclusion by her unauthorized scanning through his body to read his implanted chip.
2. Public disclosure of private facts by her publication of the BAN list.
3. Violation of the State of Marshall statute that prohibits the circumvention of any technological means that controls access to data.
4. Misappropriation of trade secrets.

Marion filed a motion for summary judgment. She argued that: (1) there was no unauthorized intrusion upon Cafka's seclusion as a result of scanning the chip;, (2) the disclosure of the facts concerning Cafka's membership in BAN was not offensive to a reasonable person and was of legitimate concern to the public (i.e., was a newsworthy event subject to a publisher's privilege);, (3) the encryption used in the RFID chip was insufficient to meet the statutory definition of "trade secret"; and (4) there was no misappropriation of trade secrets since Cafka did not take reasonable precautions under the circumstances to maintain the information's secrecy.

The trial court granted Marion's motion in full. Cafka appealed and the appellate court reversed, reinstating all four counts. Marion appealed and this court granted leave to appeal on the four issues.

IV. ANALYSIS

A. Invasion of Privacy: Intrusion Upon Seclusion

Under the umbrella of the right of privacy, there are four distinct torts: intrusion upon seclusion, public disclosure of private facts, false light

8. *Wikipedia,* http://en.wikipedia.org/wiki/Blog (accessed June 15, 2006) (stating that a blog or weblog is a web-based publication consisting of periodic postings or entries. Blogs range in scope from individual commentaries or diaries to full-length articles and range in scale from the writings of a single author to the collaberation of a community of writers.).

and misappropriation. This case deals with three of the four and each will be discussed separately.

The State of Marshall has enacted a statute that follows the *Restatement (Second) of Torts* § 652B (1977) governing intrusion upon seclusion. The applicable section states:

> 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.

Marshall Revised Code § 439(A).

Intrusion upon seclusion deals with the gathering and, not the distribution, of information about an individual. Publication is not a requirement for the tort "but generally consists of an intentional physical or sensory interference with, or prying into, a person's solitude or seclusion or his private affairs." *Broughton v. McClatchy Newspapers, Inc.*, 588 S.E.2d 20, 27 (N.C. App. 2003). Thus, Cafka is not required to show that the information was published or made public. To prevail, Cafka must allege that: (1) there was an unauthorized intrusion or prying into his seclusion;, (2) the intrusion was offensive to or objectionable to a reasonable person;, (3) the matter upon which the intrusion occurs must be private; and (4) the intrusion causes anguish and suffering. *Melvin v. Burling*, 490 N.E.2d 1011, 1012 (Ill. App. 3d Dist. 1986).

As to the first element, Cafka will likely argue that the scanning by Marion of the RFID chip implanted in his arm was an unauthorized intrusion. He should concede that the chip was implanted voluntarily and that it is programmed to give out certain information when scanned; h. However, he should argue that the scanning by Marion was not authorized and therefore her scanning is an intrusion upon his seclusion.

CafkaHe may argue that even though implanting the RFID chip implies that he gave consent to his own scanning, he certainly did not give consent to any third party to scan the RFID chip. He may argue that Marion's scanning is a disclosure obtained through deception. This argument is enhanced by the fact that in order to scan the RFID chip, Marion had to reverse engineer the encrypted program that was intended to keep the information secluded from the public. "A disclosure obtained through deception cannot be said to be a truly voluntary disclosure." *Johnson v. K Mart Corp.*, 723 N.E.2d 1192, 1196 (Ill. App. 1st Dist. 2000). In *Johnson*, employees sued for intrusion upon seclusion when their employer used private detectives, posing as fellow employees, to obtain personal information on the employees. K Mart argued that since the plaintiff-employees voluntarily disclosed the information to the under- cover investigators, there could be no intrusion upon seclusion. "It is true, as defendant argues, that plaintiffs willingly provided these personal details to the investigators. However, we believe that the

means used by defendant to induce plaintiffs to reveal this information was deceptive." *Id.*

Cafka may further argue that consent to scanning for his own purpose is not consent to have the chip scanned by others for an unapproved purpose. He may use, by analogy, *Lewis v. Legrow*, 670 N.W.2d 675 (Mich. App. 2003). In *Lewis*, a woman sued for intrusion upon seclusion over the videotaping of a consensual sexual encounter. Defendant argued that she had waived her rights because the sexual encounter was voluntary. The court stated, "AAlthough waiver or consent may be implied, 'an implied waiver requires a clear, unequivocal, and decisive act of the party showing such a purpose.'" *Id.* at 695. The woman could maintain her cause of action because her consent went to the act and, not the taping of it.

The second element concerning the offensive nature of the intrusion "focuses on the manner in which the information was obtained." *Tobin v. Mich. Civil Service Comm.*, 331 N.W.2d 184 (Mich. 1982). Cafka may argue that while he was aware that technology existed to read his RFID chip, he had a reasonable expectation that he alone could control access to the encrypted information contained in the RFID chip, (i.e., he had a reasonable expectation of privacy and thus, seclusion). He may analogize scanning of the RFID chip to cell phone interception. While most people would agree that technology exists to listen to a cell phone conversation, it is offensive to do so. Moreover, iit is not unreasonable to expect privacy even though "technology makes it possible for others to eavesdrop." *People v. Stone*, 621 N.W.2d 702, 706 (Mich. 2001). In order to scan the RFID chip, Marion had to take affirmative action to reverse engineer the program controlling the chip.

Cafka may argue that when the focus is on how the information was obtained, then the court should find that an unauthorized scanning is offensive for two reasons: (1) the intrusion was a scan through a portion of his body; and (2) Marion had to break a code to obtain the information. In support of the first point, Cafka may argue that since the scanning occurred through a portion of his body, it is highly offensive. Courts have found that "there is a generally recognized privacy interest in a person's body." *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060, 1068 (Colo. App. 1998).

Cafka should argue that Marion's failure to obtain permission to the scanningto gain access to the RFID chip and her use of an unauthorized code- breaking device adds to the level of offensiveness of her actions. In *Corcoran v. Southwestern Bell Tel. Co.*, 572 S.W.2d 212 (Mo. App. 1978), the defendant obtained the telephone bill of her in-laws by deception and opened the sealed envelope without the their permission of the in-laws. *Corcoran v. Southwestern Bell Tel. Co.*, 572 S.W.2d 212 (Mo. App. 1978). The court found it to be an intrusion because the information obtained

was of a private subject matter. *Id.* at 215. In a similar fashion, Marion obtained the information from Cafka's chip by deceptively experimenting with her own RFID chip in order to learn the technology and use it to gain access to Cafka's files.

Concerning the third element of the offensive nature of the intrusion, Cafka will likely contend that the information obtained from the intrusion was private. He may point out that ECC used the RFID chips within his company to keep his business secret. He may argue that Marion acknowledged the existence of his claim to a trade secret by signing the non-disclosure agreement. Marion's use of the RFID chip to gain access to Cafka's files was a clear breach of this agreement and an intrusion into his private affairs.

Finally, Cafka should argue that there was actual harm to him as a result of the intrusion. Softer MicronsSM was able to beat him Cafka to the market with his trade secret after he lost funding for the project. In addition, he was greatly embarrassed by the disclosure of his membership and leadership role in BAN.

Marion will argue that there was no unauthorized intrusion or prying. She may argue that her scanning was not unauthorized because Cafka had no reasonable expectation of privacy. "To prove actionable intrusion, the plaintiff must show the defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff." *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 490 (Cal. 1998). Here, Cafka knew that the RFID chip could be scanned. In fact, he scanned it himself. He knew, or should have known, that the technology employed allowed for scanning and his expectation of privacy was not warranted.

She may argue that there was no physical invasion of Cafka's privacy because the scanning was non-intrusive. She may counter Cafka's argument concerning the privacy given to the body by arguing it that bodily privacy is inapplicable in this case. Generally, it is medical information, not the body itself, that the courts are protecting. Thus, while the court in *Doe v. High-Tech Institute* did find an invasion upon seclusion, the result was based on an unauthorized blood test for HIV when the plaintiff had given consent only for a test for rubella. In addition, in a case involving a body scan of a shopper at a retail store, the court found that the intrusion of the scan "would not be so highly offensive to the reasonable person as to constitute an invasion of privacy action." *Smith v. Jack Eckerd Corp.*, 400 S.E.2d 99, 100 (N.C. App. 1991).

Lastly, Marion may argue that Cafka is in error in arguingwrong to argue that the loss of his product and the disclosure of his membership in BAN are injuries caused by the intrusion. "The tort of intruding upon the seclusion of another is aimed at the discomfort caused by the intru-

sion itself—for example, someone enters your bedroom. . . ." *Thomas v. Pearl,* 998 F.2d 447, 452 (7th Cir. 1993). In *Thomas*, the court rejected the intrusion because the injury occurred as a result of a subsequent publication and not the intrusion.

B. Invasion of Privacy: Public Disclosure of Private Facts

Unlike intrusion upon seclusion, the tort of public disclosure of private facts requires that publicity be given to the actual disclosure of the facts at issue. Publicity (as opposed to the narrower "publication" requirement in defamations cases) requires that there be some showing of actual knowledge of the disclosure by the public. To state a cause of action for public disclosure of private fact, "the information must be communicated to the public at large or to so many persons that it must be regarded as a communication to more than a small group."[9] In his complaint, Cafka alleged that Marion gave publicity to a private fact by disclosing that Cafka was the Grand Nowest of BAN.; namely, that he was the Nowest of BAN.[10] The revelations disclosure of Cafka's membership and rank were was made through anonymous postings on several Internet blogs potentially accessible to anyone having an Internet connection.[11]

The State of Marshall has enacted a statute that follows the *Restatement (Second) of Torts* § 652D (1977) governing claims for invasion of privacy through the public disclosure of private facts. The applicable section states:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his/her privacy, if the matter publicized is of a kind that:
>
> a) would be highly offensive to a reasonable person, and
>
> b) is not of legitimate concern to the public.

Marshall Revised Code § 562(B).

In order to prevail, Cafka must allege that: (1) the disclosure was widespread, i.e., given publicity;, (2) the information disclosed was private in nature;, (3) the disclosure would be highly offensive to a reasonable person;, and (4) the matter is not of legitimate concern to the public.

First, Cafka will argue that the publicity requirement is easily satisfied. He will argue that sSimply posting the information concerning his membership and leadership position in BAN on the Internet satisfies the

---

9. Michael J. Polelle & Bruce L. Ottley, *Illinois Tort Law* §6.01[2] 6-8 (3d ed., Mathew Bender 2005)

10. For purposes of the summary judgment motion, his membership and rank in BAN were assumed to be true.

11. For purposes of the summary judgment motion, Marion conceded that the posts were made by her or under her supervision.

publicity requirement. "Publicity includes publication in a newspaper, posting in a window, on a public street, or crying it aloud in the highway [citation omitted] and generally requires communication to the public at large, to a large group of people, or to a person or persons so that it is substantially certain to become one of public knowledge." *Hill v. MCI Worldcom Comm., Inc.,* 141 F. Supp. 2d 1205, 1211 (S.D. Iowa 2001). Thus, Cafkahe may argue that posting on the Internet was at least equivalent to, and potentially more widespread than publication in a newspaper, posting in a window or crying it aloud since because the posting was available to anyone surfing on the World Wide Web. AsSo long as the nature of the publicity ensures that it would reach the public, there is publicity. *Vassiliades v. Garfinckel's, Brooks Bros., Miller & Rhoades, Inc.* 492 A.2d 580, 588 (D.C. 1985).

The second element of public disclosure of a private fact requires a showing that the information disclosed concern the individual's private, as opposed to public, life. The tort of public disclosure has been described as an individual's "right to be free from unwanted publicity about his private affairs, which although wholly true, would be offensive to a person of ordinary sensibilities." *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 490 (1975).

The record is unclear regarding whether BAN's membership list was ever made public through any vehicle (or that there were any copies of the membership list other than the one on Cafka's hard drive). This is dissimilar to *Cox* where the information was in the public record. "[T]he prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record." *Cox*, 420 U.S. at 494-495. Thus, there is no "fading" of Cafka's privacy interest in this case.

Cafka may argue that the fact thatthe private nature of the information is reinforced because he kept the information in a secure location on his computer accessible only via his implanted RFID chip reinforces the private nature of the information. Moreover, he may argue that the unauthorized disclosure of the BAN membership list has a chilling effect on his freedom to associate and freedom of speech. *See NAACP v. Alabama,* 357 U.S. 449, 461 (1958). "[T]he First Amendment is implicated by government efforts to compel disclosure of names in numerous speech-related settings, whether the names of an organization's members, the names of campaign contributors, the names of producers of political leaflets, or the names of persons who circulate positions." *Church of the Amer. Knights of the Ku Klux Klan v. Kerik,* 356 F.3d 197, 209 (2d Cir. 2004).

The third element, whether or not the publication was highly offensive to a reasonable person, is a factual question usually left for a jury. *Doe v. Mills*, 536 N.W.2d 824, 829 (Mich. App. 1995). For this element,

Cafka may reassert the argument concerning his freedom to associate without fear of retribution. The release of his membership and position was a fact that he intended to keep secret. His loss of funding for the project and his embarrassment underscores the fact that the disclosure was offensive to a reasonable person.

Cafka may argue that the Supreme Court has protected individuals from disclosure of their political associations and beliefs. "Such disclosures can seriously infringe on privacy of association and belief guaranteed by the First Amendment." *Brown v. Socialist Works '74 Campaign Comm. (Ohio),* 459 U.S. 87, 91 (1982). *Brown* dealt with state action that the court said requireds strict scrutiny. *Id.* "The right to privacy in one's political associations and beliefs will yield only to a subordinating interest of the State that is compelling, and then only if there is a substantial relation between the information sought and an overriding and compelling state interest." *Id.* In a similar manner, the court in *Averilll v. City of Seattle,* 325 F. Supp.(add space)2d 1173 (W.D. Wash. 2004), found that the membership list of the Freedom Socialist Party was exempt from disclosure under a city ordinance where the applicant for the exemption shows a reasonable probability that disclosure will subject the persons "to threats, harassment, or reprisals from either Government officials or private parties." *Averill v. City of Seattle,* 325 F. Supp. 2d 1173, 1179 (W.D. Wash. 2004)*Id.* at 1179.

Cafka may argue that the First Amendment freedom of association can be applied to actions by individuals as well. For this point, he may argue that in private litigation, courts are reluctant to require the disclosure of the names of members of organizations even under a subpoena to an adverse party. Certainly, Cafka may argue that, Marion was an adverse party whose sole intent was to make the list public to embarrass and harass Cafkahim. "The First Amendment associational privilege emergences when a discovery request specifically asks for a list of a group's anonymous members." *Anderson v. Hale,* 2001 U.S. Dist. LEXIS 6127, *9 (N.D. Ill. May 10, 2001). This privilege requires a careful balancing of the parties interests under heightened scrutiny. "This same balancing test equally applies to cases involving two private parties." *Id.* at *10. Anderson has requested subscription account information from several Iinternet service providers for anonymous WCOTC members who posted on the Internet or whose e-mail addresses were on WCOTC literature. In attempting to quash the subpoenas, the defendants argued that the disclosure of the information would unjustifiably infringe upon the members associational rights and that disclosure threatens to expose them to harassment, threats and reprisals. The court found that the WCOTC:

> ranks as one of the most despicable and hated organizations of this time. . . .It goes without saying that WCOTC members are under con-

> stant threat of harassment and harm. As a result, many members conceal their identity.
>
> And understandably so. Publicly identifying oneself as a WCOTC member gives rise to consequences. For instance, one member lost his job after his association became known, and Hale himself has been unable to obtain a law license because of his beliefs and association.
>
> In light of this, it is apparent that disclosure of anonymous WCOTC members' identities is likely to chill associational rights. That means heightened scrutiny applies. . .

Id. at *23. The subpoenas were quashed. Cafka may argue that in a similar manner, his membership was a highly private matter that Marion made public.

Finally, the fourth and last necessary element requires a showing of the lack of public concern or "newsworthiness" in the facts disclosed. Cafka must show that Marion gave publicity to private matters in which the public had no legitimate concern, because ifhad the subject matter is ofbeen a legitimate public concern, then there would be no invasion of privacy with its disclosure.is no invasion of privacy. *Wasser v. San Diego Union*, 191 Cal. App.3d 1455 (Cal. App. 4th Dist. 1987). The public disclosure tort is subject to a newsworthy privilege to protect the First Amendment freedom to report on matters of public concern. *Michaels v. Internet Ent. Group*, 1998 U.S. Dist. LEXIS 20786, *19 (C.D. Cal. Sept. 10, 1998). This privilege is not without limit. *Id.* As the Court quoted in the *Michael's* opinion, "[w]here the publicity is so offensive as to constitute a morbid and sensational prying into private lives for its own sake, it serves no legitimate public interest and is not deserving of protection." *Id.* Cafka has the burden of proof to demonstrate that the matters publicized are not newsworthy, or that the depth of the intrusion in private matters was "in great disproportion to their relevance" to matters of public concern. *Id.*

Guidance concerning public concern or "newsworthiness" can be found in the three-part test adopted by the California Supreme Court in *Shulman, v. Group W Prod.*, 18 Cal. 4th 200 (Cal. 1998)955 P.2d at 502. The California court found that newsworthiness is evaluated by balancing the depth of the intrusion against the relevance of the matters broadcast to matters of legitimate public concern. *Id.* The factors to consider include: (1) the social value of the facts published;, (2) whether the person voluntarily became involved in public life;, and (3) for private persons involuntarily caught up in events of public interest, whether a substantial relationship or nexus exists between the matters published and matters of legitimate public concern.

Cafka may argue that there is slight social value, if any, in the fact that he is a member in BAN. As stated in *Michaels,* the social value of newsworthiness is not limited to news in the narrow sense of reports of

current events. *Michaels,* 1998 U.S. Dist. LEXIS 20786 at *25. It extends to facts giving information to the public for purposes of education, amusement or enlightenment, when the public may reasonably be expected to have a legitimate interest in what is published. *Id.* at *26. Cafka may argue that this broad definition as implied in many decisions including *Michaels* gives deference to the media and newspapers in distributing information, and does not to protect publishing that ispublications that are maliciously done by a private individual. *Id.* at *25.

Moreover, heCafka may argue that this broad definition does not apply to this casethe case at hand because it was published maliciously, and for none of the purposes stated abovereasons previously mentioned except , other than to embarrass Cafkahim personally and to destroy his business. There is no social value in something that is merely to embarrass and harass a person. Furthermore, although some may have an interest in these facts, the reasonable person (which is the standard set out above) would not. This publication was of no public concern. Although Cafka is a leader in an anti-abortion group, his leadership role has been conducted in private. There is no "newsworthiness" in his activities. The group has been charged with no crimes nor has Cafka sought publicity for his role in the group. Cafka also may also argue that the activities of BAN are within constitutional boundsthe bounds of the Constitution. The only allegations linking BAN to negative conduct, including it to following or threatenings to doctors, comes from news reports.[12] The organization has not engaged in any "true threats" to individuals and thus its statements are political in nature. The First Amendment protects speech that advocates violence so long as the speech is not directed to inciting or to producing imminent lawless action and is not likely to incite or produce such action. *Brandenburg. v. Ohio*, 395 U.S. 444, 447 (1969).

In addition, Cafka may argue that a weblog is not considered part of the media by relying onand attempt to use the pending case of *Apple Comp., Inc. v. Doe 1 through 25*, Superior Court for the, State of California, County of Santa Clara, No. 1-04cv032178., No. 1-04CV032178 to bolster this argument. (Recheck Citation) The question of whether bloggers are journalists has been raised but has not yet been answered in the *Apple* case. ThisThe *Apple* case involves the alleged posting of certain Apple trade secrets on several Iinternet sites. In order to obtain the identity of the sources of the information, Apple sent subpoenas to certain email service providers. Several non-parties objected to claiming , among other things, that theybloggers wereare journalists who were are entitled to protect their sources under both common law and California's "shield law." In denying their motion, the court stated:

12. R. at 3.

> Movants contend they are journalists. They make this claim because they seek protection of the privilege against revealing their sources of information. Defining what is a "journalist" has become more complicated as the variety of media has expanded. But even if the movants are journalists, this is not the equivalent of a free press. The journalist's privilege is not absolute.

Slip Opinion at 8-9 (Mar. 11, 2005).

The court found that the issue of whether the movants fit "the definition of a journalist, reporter, blogger, or anything else need not be decided at this juncture for this fundamental reason: there is no license conferred on anyone to violate criminal laws." *Id.* at 11.

Marion may argue that there has been no evidence of publicity. She may argue that publicity is more than merea mere publication and that, at best, in this case, at best a publication has occurred. only a publication has been shown. "In a case involving the public disclosure of private facts, 'publicity' means 'communicating the matter to the public at large or to so many persons that the matter must be regarded as one of general knowledge." *Wynn v. Loyola Univ. of Chicago*, 741 N.E.2d 669, 677 (Ill. App. 1st Dist. 2000). Marion may argue that posting on a web- blog is not sufficient publicity because generally blogs are read by special interest groups and , not the public at large. Marion may further argue that the publicity element is not satisfied because only a very limited number of people having a "common interest" would likely have read any of the blogs. *Zinda v. Louisiana Pac. Corp.*, 440 N.W.2d 548, 552 (Wis. 1989). (probably would be more proper to use citation of Wisconsin Supreme Court reporter.).

As to the element requiring that the information disclosed wasbe private in nature, Marion may argue that the meremere membership in a group such as BAN is not private in nature. The activities of BAN have been reported in the media, which is inconsistent with a right of privacy for the group and its members. Marion may argue that Cafka was active in the organization and was in a leadership role and therefore, a public role as well, and therefore, public role. As such, his activities were public to the group. "There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public."[13] Moreover, Marion should argue that the First Amendment cases are not applicable. The First Amendment "is implicated by government efforts to compel disclosure of names in numerous speech-related settings . . ." *Church of the Amer. Knights of the Ku Klux Klan v. Kerik*, 356 F.3d 197,at 209 (2d Cir. 2004). . Here, there is no state action; and thus, the First Amendment is not at issue.

13. *Restatement 2d of Torts* § 652D.

To the extent that Cafka's membership is a private fact, Marion should argue that the newsworthiness of his leadership in a public group outweighs any privacy rights concerning the information. If the subject matter is of legitimate public concern, there is no invasion of privacy. *Wasser v. San Diego Union*, 191 Cal. App.3d 1455at 1461 (Cal. App. 1987). .

The reported threatening activities of BAN make any information on its members newsworthy and a matter of legitimate public concern. She may argue that the reported positionactivities of BAN, which include intimidating and threatening doctors, to intimidate and threaten doctors areis activitiesn activity that is against against public policy. As a result, the identity of individuals and those who engage in such activities should be made known to the public.

She may argue that BAN's activities are similar to the activities of the American Coalition of Life Activists who created and distributed "Wanted" posters for doctors who performed abortions. The posters included the doctors namess, picturess and addressaddresses of various doctorses. The court found the posters to be true threats since it wasbecause they were "a statement which, in the entire context and under all the circumstances, a reasonable person would foresee would be interpreted by those to whom the statement is communicated as a serious expression of intent to inflict bodily harm upon the person." *Planned Parenthood of the Columbia / Willamette, Inc v. Amer. Coalition of Life Activists,* 290 F.3d 1058, 1077 (9th Cir. 2002). SinceBecause activities that are potentially "true threats" are newsworthy, information about the group also is also newsworthy.

Marion may additionally argue that Cafka, if not a public figure based on his role in BAN, is at least is an involuntary public figure. A and as such, a public interest in information pertaining to Cafka's BAN activities existsinformation concerning his BAN activities create a public interest in his activities. Involuntary public figures are individuals who have not sought publicity or consented to it, but through their own conduct or otherwise, they have become a legitimate subject of public interest. They have, in other words, become "news." *Restatement (Second) of Torts* §652D. Involuntary public figures appeal to the public interest and publishers are permitted to satisfy the curiosity of the public as to its heroes, leaders, villains and victims and those who are closely associated with them. *Virgil v. Time*, 527 F.2d 1122, 1129 (9th Cir. 1975).

Lastly, Cafka may counter that from a policy perspective, the court should look to the method by which the information was obtained. As an employee, Marion was in a position of trust and she had signed a nondisclosure agreement. Contrary to her responsibilities, Marion first reversed engineered the RFID chip to bypass Cafka's safeguards to his private information and then posted what she found on the Internet. As a

result, she should be held accountable for her actions and the public disclosure of Cafka's private facts.

In response, Marion may argue that because the information is newsworthy, it does not matter how the information was obtained. "[W]here the claim is that private information concerning plaintiff has been published, the question of whether that information is genuinely private or is of public concern should not turn on the manner in which it has been obtained." *Pearson v. Dodd,* 410 F.2d 701, 705 (D.C. Cir. 1969).

C. Violation of the Anti-Circumvention Act

The Marshall Anti-Circumvention Act contains a provision that prohibits the circumvention of technology designed to prevent access to data. The intent of the provision is to impose legal penalties on those who penetrate or bypass encryption and other technological measures used to protect property (including data). The applicable section of the statute states:

> No person shall circumvent a technological measure that effectively controls access to data. As used in this section:
>
> a. To "circumvent a technology measure" shall mean to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the owner of the underlying data.
>
> b. A technological measure "effectively controls access to data" if the measure, in an ordinary course of its operation, requires the application of information, or a process, or a treatment, with the authority of the owner of the underlying data, to gain access to the data.
>
> It shall not be a violation of this provision
>
> a. if the technology measure is "reverse engineered" by a person who has lawfully obtained the right to use the computer program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, or
>
> b. if the decryption is part of "encryption research" which means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies protecting data if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products. For purposes of this provision, "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

Marshall Revised Code § 1492. The statute also provides for a private right of action for any person aggrieved by a violation of §1492.

Cafka may argue that he took technological measures to control access to his data; namely, the RFID chip. Under normal usage, the RFID chip limited access to the data stored in his computer. The signal from the RFID chip to the transponder and the authorization by the transponder were "processes" as defined by the Marshall statute.

Cafka may argue that the statute is similar to the Federal Digital Millennium Copyright Act ("DMCA") provisions dealing with anti-circumvention. 17 U.S.C. § 1201(a)(1)(A). Under the DMCA, the data to be protected must be copyrighted, which is not the case in the State of Marshall statute. In reviewing the DMCA, courts have found that

> The question of whether a technological measure "effectively controls access" is analyzed solely with reference to how that measure works "in the ordinary course of its operation."

Pearl Investments, LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326, 350 (D. Maine 2003).

In *Pearl,* the issue was whether an encrypted, password-protected, virtual private network was a technological measure. The court found in the affirmative. The court also found that it was irrelevant whether the defendant had alternate legitimate means to the data; thus, Cafka may argue that while defendant had access to some data through legitimate means, she was not entitled to all the data protected by the RFID chip. The reverse engineering was not for the purpose of establishing interoperability of another computer program or for encryption research, but rather for the sole purpose of stealing ECC's trade secret.

The court in *Universal City Studios, Inc. v. Corley,* 273 F.3d 429 (2d Cir. 2001) observed that

> . . . the essential purpose of an encryption code is to prevent unauthorized access. Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.

Id. at 452. Cafka may argue that his RFID chip was similar to a lock and that it was picked (i.e., circumvented) by the Marion's unauthorized reverse engineering.

Marion may argue that in the ordinary course of operation, the RFID system was ineffective and therefore the anti-circumvention statute does not apply. She may argue that the RFID chip activation of the transponder is analogous to a password and therefore does not meet the definition of a technological measure. She may cite *I. M. S. Inquiry Mgmt. Systems, Ltd. v. Berkshire Info. Systems,* 307 F.Supp. 2d 521

(S.D.N.Y. 2004). In *I.M.S.*, the court found that there was no circumvention of a technological measure under the DMCA when a password protection system was breached. Rather, the court found that "what defendant avoided and bypassed was *permission* to engage and move through the technological measure from the measure's author. . . [A] cause of action under the DMCA does not accrue upon unauthorized and injurious access alone; rather, the DMCA 'targets the *circumvention* of digital walls guarding copyrighted material.'" *Id.* at 533 (emphasis in original).[14]

She may argue that because her RFID chip and Cafka's chip were similar, Cafka made the program controlling the chip public and subject to reverse engineering by implanting the chips in his employees. Marion may point to *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004) to support her position. In *Chamberlain,* the technology was similar—a radio frequency transmitter that activated a receiver to open a garage door. Chamberlain claimed that Skylink, a competitor, violated the anti-circumvention provisions of the DMCA by manufacturing its own brand of transmitter that activates the Chamberlain garage door opener. What Chamberlain argued was that the rolling codes used in the garage door opener were "technological measures" that controlled access to its copyrighted programs. The court rejected Chamberlain's claim noting that there was no relationship between the access to the copyrighted programs and the use of the transmitters; thus, Marion can argue that in this case there is a similar disconnect between the RFID chips and the data that was on Cafka's computer.

Last, Marion may raise a First Amendment claim arguing that the statute regulates speech. Marion may argue that computer code is speech and that the restrictions of the statute are not content neutral and are overly broad. She may argue that there is no legitimate state interest in protecting all data.

First Amendment challenges were made to the DMCA. In *U.S. v. Elcom,* the court rejected the First Amendment claims. *U.S. v. Elcom Ltd.*, 203 F. Supp.2d 1111 (N.D. Cal. 2002). The provision of the DMCA at issue in *Elcom,* however, was the trafficking in anti-circumvention devices and not the direct circumvention of technological controls. *Id.* In *Elcom*, the court agreed that computer code can be speech. *Id.* The court had to determine whether the claim should be reviewed under the standard of strict scrutiny, where restrictions are permissible only if they serve a compelling state interest and do so by the least restrictive means, or intermediate scrutiny where the regulation will be upheld if it fur-

14. *Contra, Realnetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash. 2000) (finding that the "secret handshake" by a computer is a "technological measure" that effectively controls access to a copyrighted work).

thers an important or substantial government interest unrelated to the suppression of free expression. Under its analysis, the *Elcom* court found that the DMCA did not target speech. "[T]o the extent that the DMCA targets computer code, Congress sought to ban the code not because of what the code says, but because of what the code does." *Id.* at 1128. The court applied the intermediate scrutiny standard because the code did not target the content of speech. Under the DMCA, the court found three governmental interests: 1) preventing the unauthorized copying of copyrighted works; 2) promoting electronic commerce; and 3) preventing electronic piracy.

> Under intermediate scrutiny, it is not necessary that the government select the least restrictive means of achieving its legitimate governmental interest. By its very nature, the intermediate scrutiny test allows some impingement on protected speech in order to achieve the legitimate governmental objective. A sufficiently important government interest in regulating targeted conduct can justify incidental limitations on First Amendment Freedoms. [Citation omitted] Having considered the arguments asserted by the parties, the court finds that the DMCA does not burden substantially more speech than is necessary to achieve the government's asserted goals of promoting electronic commerce, protecting copyrights and preventing electronic piracy.

Id. at 1132.

To overcome the holding in *Elcom*, Marion may argue that while the DMCA prohibited circumventing technological measures that protect copyrighted material, the Marshall statute is overly broad because it prohibits circumventing technological measures protecting any data. As a result, the critical element of copyright protection is lacking. Marion might argue that there is no compelling state interest in protecting data since the data may or may not be copyrighted. The provision is thus overly broad and even if the less rigorous intermediate scrutiny standard were used, the statute must fail.

D. Misappropriation of Trade Secrets

In the instant case, when analyzing whether there has been a misappropriation of Cafka's trade secret, the court must consider both the statutory definitions of trade secret and misappropriation as well as the effect of the non-disclosure agreement signed by Marion.

Misappropriation of trade secrets is usually based on a two-part analysis. First, it must be determined whether a trade secret exists. Second, if the existence of a trade secret has been established, then it must be determined whether that trade secret has been stolen or misappropriated. The State of Marshall has adopted a statute that mirrors the language of the Uniform Trade Secrets Act and provides the applicable definitions. It states in part:

"Trade Secret" shall mean information including but not limited to technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or a list of actual or potential customers or supplies, that:

a. is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
b. is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

"Misappropriation" means:

a. acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret was acquired by improper means
b. disclosure or use of a trade secret of a person without express or implied consent by a person who
   i. used improper means to acquire knowledge of the trade secret. . .

Marshall Revised Code § 1947.

1. *Whether a Trade Secret Exists:*

Before there can be a misappropriation of a trade secret, there must be a trade secret. In determining whether a trade secret exists, courts generally consider six factors: (1) the extent to which the information is known outside the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the employer to guard the secrecy of the information; (4) the value of the information to the business and to competitors; (5) the amount of effort or money expended by the business in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. *ILG Industries, Inc., v. Scott,* 273 N.E.2d 393, 396 (Ill. 1971).

Applying these general factors, Cafka may argue that the information was not known outside of ECC and that no employee of ECC other than himself knew the full extent of the project. Furthermore, Cafka may argue that the use of the RFID chip and physical separation of employees were reasonable measures to guard the secrecy of the information. He might say that the information was valuable to ECC and to competitors. Finally, Cafka will argue that he spent considerable time, effort, and money in program development and that absent a misappropriation, duplicating the information would be difficult. Defendant Marion may concede that the information was generally not known outside ECC and that the RFID chip and physical separation of employees restricted the access to the information by other employees; however, she will likely argue that the use of the RFID chip was insufficient to guard against its appropriation.

The *Restatement (Third) of Unfair Competition* §39 (1995) defines a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford actual or potential economic advantage over others." To establish a trade secret under the Restatement approach, Cafka must demonstrate that the Music Man project's information was: (1) kept sufficiently secret to derive economic value; (2) was not generally known to other persons; and (3) ECC expended reasonable efforts to maintain its secrecy or confidentiality. *Ingersoll-Rand v. Ciavatta,* 110 N.J. 609, 637 (1988)(quoting N.J. Stat. Ann. 2C:20-1(i)).

First, Cafka must demonstrate that the information concerning the Music Man project was kept sufficiently secret to derive economic value. In *USM Corp.*, the court listed five adequate internal procedures for the protection of trade secrets: (1) the use of employee non-disclosure agreements; (2) using confidential markings; (3) physical security measures; (4) limiting information access to only those employees who are involved in the project; and (5) reinforcing the fact that particular matters should be kept secret during and after leaving employment. *USM Corp. v. Marson Fastner Corp.* 393 N.E.2d 895, 900 (Mass. 1979).

Cafka may argue that he took great measures to ensure the secrecy of the Music Man project and complied with the adequate internal procedures for protection of trade secrets as set forth in *USM Corp.* In addition to requiring employees to sign non-disclosure agreements and confidential computer log-in access, Cafka instituted several other physical security measures. For example, in order to create total secrecy, Cafka "divided his employees into two workgroups so that no one individual, except Cafka himself, would have knowledge of all aspects of the research and development."[15] Cafka also separated the assignments of each employee "so that no one employee knew the full extent of the project."[16] He limited the number of employees to three individuals located at each office and no employee had knowledge about the location or contact information about his or her colleagues, including telephone numbers and email addresses.[17] These actions satisfy the fourth criteria laid out in *USM Corp.* In order to reinforce secrecy on a daily basis, Cafka could argue that he was the only one with an RFID chip[18] allowing "total access to all offices, computers and files on all ECC computers, including all the files created by his employees."[19] With this unrestricted access, Cafka could periodically monitor the various locations and discuss the progress of the project, as well as accessing employee research files in the

15. R. at 2.
16. R. at 8.
17. R. at 2.
18. R. at 2.
19. R. at 2.

secured computers.[20] In response, Defendant Marion may argue that Cafka used an RFID encryption system that was similar to the one he used for his employees[21] and, therefore, did not sufficiently keep the information secret to derive economic value.

Second, Cafka must show that the Music Man project was not generally known to other persons. In order to satisfy this element, Cafka may show that to "access secured ECC offices and computers used for the research and design, each ECC employee was required to have implanted an RFID chip in his or her right arm."[22] The RFID chip activates by radio frequency transmission signals sent by a transponder within a few meters of the employee[23] and "responds to the signal by transmitting a unique serial number back to the transponder."[24] In addition to a confidential serial number, each of the RFID chips "incorporates a processor that uses a simple cryptographic algorithm to generate a 64-bit serial number based upon a 16-bit code number received from the transponder."[25] Cafka could argue that all of the doors were equipped with RFID tags to control access,[26] and all of the company computers contained RFID transponders that only allowed the authorized employees access to his or her assigned machine.[27] As such, it sufficiently protected the Music Man project from being generally known by others.

Third, Cafka will argue that he expended reasonable efforts to maintain the secrecy or confidentiality of the information in question. Two issues must be considered: (1) whether a valid non-disclosure agreement exists between the parties; and (2) whether reasonable measures were taken to ensure confidentiality.[28] Cafka may argue that Marion knew that the information surrounding the Music Man project was confidential in nature and not intended to be disclosed to others. Common law agency and tort theories suggest that even in the absence of a confidentiality agreement, an employer may be protected from an employee's damaging disclosures if the employee was on notice that the information was imparted in confidence and considered to be trade secrets.[29]

---

20. R. at 2.
21. R. at 2.
22. R. at 2.
23. R. at 2.
24. R. at 2.
25. R. at 2.
26. R. at 2.
27. R. at 2.
28. R. at 8.
29. *See generally Mercer v. C.A. Roberts, Co.*, 570 F.2d 1232, (5th Cir. 1978); *see, e.g., Aries Information Systems, Inc. v. Pacific Mgt. Systems Corp.*, 366 N.W.2d 366, 369 (Minn. App. 1985) (stating that "confidentiality agreements put employees on notice that information contained in computer programs was considered secret"); *Jostens, Inc. v. Natl. Computer Systems, Inc.*, 318 N.W.2d 691, 702 (Minn.1982); *Wesley Software Dev. Corp. v.*

It is a basic principle of contract law that confidentiality agreements are enforceable when supported by adequate consideration. *Pepsico, Inc. v. Redmond*, 54 F.3d 1262, 1271 (7th Cir. 1995). The Third District Court of Appeals considered the validity of the non-disclosure agreement signed by Marion.[30] The court found the agreement invalid because it was signed several months after Marion's initial employment date. Marion may now argue that since she worked for nearly six months before signing the standard non-disclosure agreement and was offered no additional compensation for signing it,[31] that the appellate court was correct in finding that the agreement is not valid and binding.[32]

The appellate court found that the existence of a confidentiality agreement was merely an insufficient attempt to protect the secrecy of the Music Man project;[33] therefore, Cafka could argue that the appellate court erred and that an employment relationship in and of itself satisfies the consideration issue. A well-developed body of law supports the premise that because a "preexisting contract of employment is terminable at will, no overt consideration is required to support an otherwise valid covenant not to compete." *Wesley*, 977 F. Supp at 144 (citing *Russo,* 1995 WL at *3. Moreover, the "law presumes that such a covenant is supported by the employer's implied promise to continue the employee's employment; or his forbearance in not discharging the employee then and there." *Id.* Cafka can show that his continued employment of Marion would have been enough consideration to validate the executed confidentiality agreement between them. In fact, employer's trade secrets are protectable under Illinois law. *Pepsico,* 54 F.3d at 1262. As such, "non-disclosure agreements may be viewed as simple redundant restatement[s] of trade secret law."[34] Moreover, Illinois courts have held that a "contractual or other duty to maintain secrecy or limit use of a trade secret shall not be deemed to be void or unenforceable solely for lack of durational or geographic limitation on the duty." *Pepsico,* 54 F.3d at 1272.

In spite of the confidentiality agreement, another issue that the parties may argue is whether the employment relationship gave rise to an independent duty of confidentiality in this case. Establishing the exis-

---

Burdette, 977 F.Supp 137 (D. Conn. 1997) (citing *Russo Assoc., Inc. v. Cachina*, No. 27 69 10, 1995 WL 94589, *3 (Conn. Super. 1995).

30. R. at 7.

31. R. at 2.

32. R. at 7.

33. R. at 8.

34. *See generally Chomerics, Inc. v. Ehrreich,* 421 N.E.2d 453 (Mass. App. 1981); *Dynamics Research Corp. v. Analytic Sciences Corp.* 400 N.E. 2d 1274, 1288 (Mass. App. 1980) (stating that "the non-disclosure agreement . . . can only affirm the intent of the parties to be bound by the common law of trade secrets"); *Motorolla Inc. v. Fairchild Camera & Instrument Corp.,* 366 F. Supp. 1173 (D. Ariz. 1973).

tence of a trade secret should stem from the level of an employer's secrecy and notice to employees, and not merely from a contract. The *Restatement (Third) of Unfair Competition* §41 (1995) explains when the duty of confidentiality arises in an employment context: (1) when there is an express promise to do so, and (2) when the person disclosing the information had a reasonable belief that there was consent to maintaining confidentiality based on the relationship of the parties. The *Restatement (Third) of Unfair Competition* §42 (1995) also makes clear that the duty of confidentiality even continues after termination of employment.[35] Under both the common law and §42 Comment (c), there is an inference that an employee has consented to the confidential relationship when the employee knows or has reason to know that the information given by the employer should be held in confidence.[36] The mere act of putting an employee on notice that they are receiving confidential information establishes a confidential relationship.[37]

Cafka can show that by implanting the RFID chip in his employees and segregating the computers and information available to discrete locations, he put employees on notice of the confidential nature of his trade secret.[38]

2. *Whether There Was a Misappropriation of Cafka's Trade Secret:*

The State of Marshall enacted a statute that follows the language of the Uniform Trade Secrets Act (Sec. 1947) governing claims for establishing trade secret misappropriation. Its applicable section states:

> Misappropriation means:
>
> a. acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret was acquired by improper means
>
> b. disclosure or use of a trade secret of a person without express or implied consent by a person who
>
> i. used improper means to acquire knowledge of the trade secret. . .[39]

To establish misappropriation, Cafka will likely argue that Marion knowingly acquired information about the Music Man project using improper means only to later disclose or use the trade secret without his express or implied consent. Cafka may argue that Marion acquired the

35. *See New England Overall Co. Inv. v. Woltmann,* 176 N.E. 2d 193 (Mass. 1961).

36. *Restatement of Unfair Competition* §42 (contending that "[t]he duty of confidentiality arises from the employer/employee relationship); *Amer. Stay Co. v. Delaney,* 97 N.E. 911 (Mass. 1912).

37. *Dynamics Research Corp.,* 400 N.E.2d at 1287; *see also Ostens, Inc. v. National Computer Sys. Inc.,* 318 N.W.2d 691 (Minn. 1982).

38. R. at 8.

39. R. at 7.

trade secret through improper means during the course of her employment at ECC. To balance an employee's right to seek continued employment and career advancement where an employee is highly skilled, the courts require a greater degree of specificity when identifying the protected trade secret. *Dynamics Research Corp.*, 400 N.E.2d at 1283. The United States Supreme Court in *Kewanee,* held that a trade secret owner can prevent an employee from using or disclosing the trade secret if that employee acquired the information through improper means. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475-76 (1974). The *Kewanee* court, however, did not expressly define improper means.[40] Even so, this court may be guided by the *Restatement of Torts* § 757 (1939), which states that, "except by the use of improper means, there would be difficulty in acquiring the [misappropriated] information."[41]

Marion could argue that she has a right to use the trade secret information despite the fact that ECC owns the information, if the skills she used to obtain it are part of her general knowledge and experience.[42] Moreover, *Restatement of Torts* § 757, Comment (f) notes that knowledge acquired through proper means exist in two situations: (1) discovery by independent invention; and (2) discovery by reverse engineering.

Marion built an RFID transponder at home to experiment with the RFID chip implanted in her arm by ECC. Through this process, she reverse engineered the cryptographic algorithm used to generate the confidential serial numbers.[43] The *Restatement of Torts* § 757, Comment (b) also requires that "a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information." Furthermore, in *E.I. DuPont*, the court stated: "Improper means will be found where one acquires another's trade secret information by utilizing extraordinary measures to overcome precautions designed and implemented to protect the secrecy of the trade secret." *E.I. DuPont de Nemours & Co. v. Christopher*, 431 F. 2d 1015, 1015-17 (5th Cir. 1970).

---

40. *See Kewanee Oil Co.*, 416 U.S. at 475-76 (stating that "the protection accorded the trade secret holder is against the disclosure or unauthorized use of the trade secret by those to whom the secret has been confided under the express or implied restriction of nondisclosure or non use. The law also protects the holder of a trade secret against disclosure or use when the knowledge is gained, not by the owner's volition, but by some 'improper means'").

41. *See Sun Dial Corp. v. Rideout,* 16 N.J. 252, 257 (citing *Restatement of Torts* § 757).

42. *See Structural Dynamics Research Corp v. Eng. Mechanics Research Corp.*, 401 F. Supp. 1102, 1111-12 (E.D. Mich. 1975) (stating that where employee's own skills, talents and experience were instrumental in developing the trade secret, the employee has unqualified right to use and disclose the secret unless the employee has contracted not to do so); *See also Mercer,* 570 F.2d at 1232.

43. R. at 3.

Marion will likely argue that she needed no extraordinary measures to obtain the information in question. The reverse engineering skills she employed were part of her general knowledge and the subject of her reverse engineering (i.e., her RFID chip) was easily accessible because it was implanted in her own body. Through the common, not extraordinary practice of reverse engineering, she was able to easily obtain the algorithm in Cafka's chip using the data her RFID transponder generated.[44] Marion may argue that she merely used this information to build a clone of Cafka's chip, which gave her access to the serial numbers protecting the security to his office and files.[45] As such, she could argue that she did not misappropriate anything through improper means. In fact, Marion will argue that she just used her knowledge and skill to acquire the information. She may argue that because the RFID chip was implanted in her, it was not a trade secret because it was publicly disclosed and subject to reverse engineering.

The second prong of the test for trade secret misappropriation hinges on the fact that the use or disclosure of the information was done without the consent of the owner. The Supreme Court has recognized the importance of confidentiality in the employment relationship and the responsibility of employees to maintain it. In *E.I. DuPont,* Justice Holmes concluded that: "Confidential information received during the course of fiduciary relationships may not be used or disclosed to the detriment of the one from whom the information is being obtained." *E.I. DuPont,,* 244 U.S. at 102.[46] Moreover, some courts take this principle further and hold that when employees have intimate knowledge of an employer's business, then a confidential employment relationship exists and, "the employer has a qualified right to secrecy that arises from the relationship and is required by principles of good faith." *Zoecon Indus. v. Amer. Stockman Tag Co.,* 713 F.2d 1174, 1178 (5th Cir. 1983).

Courts have also recognized situations where the employee is not bound by a signed confidentiality agreement protecting the employer's trade secrets. Under these situations, the doctrine of inevitable disclosure arises. In *National Starch,* the court found that an employer may be able to protect his trade secrets, even without a written agreement. *Natl. Starch & Chem. Corp. v. Parker Chem. Corp.,* 219 N.J. Super. 158 (App. Div. 1987). National argued that the employee had knowledge of many secret formulas that could be duplicated from memory. The court focused on the degree of harm to the Plaintiff, concluding "that under the circumstances there was sufficient likelihood of 'inevitable disclosure,' with consequent immediate and irreparable harm to Plaintiff." *Id.* at

44. R. at 3.

45. R. at 3.

46. *See also Numed Inc. v. McNutt,* 724 S.W.2d 432, 434 (Tex. App. 1987).

162. In *PepsiCo,* the court held that when determining threatened misappropriation, "The issue is not intent, the issue is whether the new employment will inevitably lead the employee to disclose or use his former employer's trade secrets – whether consciously or unconsciously." *PepsiCo*, 54 F.3d at 1262.

In the case of *Ingersoll-Rand Co. v. Ciavatta*, the court held that trade secret protection may be afforded to "highly specialized, current information not generally known in the industry, created and stimulated by the research environment furnished by the employer to which the employee has been "exposed to" or "enriched by" solely due to his employment." *Ingersoll-Rand Co.*, 110 N.J. at 637. In the instant case, ECC's main business is "to design and to build the next generation of computers using a technology where the image created by the computer is displayed via brainwaves thereby eliminating the need for a computer screen."[47] The novel concept of projecting images into the brain of the user had not yet been released to the public. Cafka may argue that Marion was "exposed to" or "enriched by" the technology at ECC, and therefore, misappropriated and disclosed that information without his consent.

Marion may argue that she brought the knowledge and skill to her employment like a "tradesman who brings his tools to his employer . . . or a scientist who has entered into an employment relationship with a head full of scientific data." *Coskey's T.V. & Radio Sales & Serv. Inc. v. Foti* , 253 N.J. Super 626, 637-38 (App. Div. 1992) (quoting *Corbin on Contracts* § 1391B, at 610 (Supp. 1989)). Marion may also argue that her knowledge "become[s] part of the employee's person. . . [and] belong to the employee as an individual for the transaction of any business in which the employee may engage." *Ingersoll-Rand Co.,* 110 N.J. at 635. The record can support that she was an excellent programmer.[48] Marion can argue that when employees are hired at ECC, "each employee was required to sign an employment agreement and non-disclosure agreement to prevent the threatened or actual disclosure of any confidential or trade secret information of ECC."[49] The agreement broadly defines trade secrets to include, "concepts, source code, computer programs, business plans, formulas and all other proprietary and secret materials."[50] Marion can argue that because she was not asked to sign a non-disclosure agreement until several months after her hire, and the agreement she subsequently signed contained broad categories of protection, that she did not have a duty to procure Cafka's consent prior to using and disclosing the information.

---

47. R.at 1-2.

48. R. at 2.

49. R. at 2.

50. R. at 2 (citing Exhibit A: *Nondisclosure Agreement Between ECC Enterprises, Inc. and Bess Marion).*

Cafka can show that he and Marion had known each other since high school,[51] and therefore already had a relationship of more than just employer-employee. Moreover, the facts in the record show that Marion did not have good intentions or motives for taking the programming position at ECC. Instead, by working for Cafka, "she could learn more about the Music Man and potentially beat Cafka to the market with a similar product."[52] Cafka can also show that Marion covertly downloaded confidential files onto a thumb drive from his office by using the clone of his chip late at night.[53] If the downloading of files were for a legitimate business use, then the task should have been done during the day and not after business hours using a device to bypass security measures protecting his confidential information. Finally, Marion did not have the knowledge regarding the Music Man project before working for ECC. In fact, she took the research compiled by her ECC colleagues to understand the complete workings of the Music Man project.[54] Cafka can argue that without this information, she would not have been able to contribute to her new employment at SM and help to develop "a new product that used brain waves as a control mechanism [. . . displaying] images directly in the brain of the users."[55]

51. R. at 2.
52. R. at 2.
53. R. at 3.
54. R. at 3.
55. R. at 3.

BRIEF FOR PETITIONER

NO. 2004-CV-1947

IN THE
SUPREME COURT OF MARSHALL
FALL TERM 2005

BESS MARION,
Petitioner,

v.

EDDIE CAFKA, *et al.*,
Respondent.

ON APPEAL FROM THE
THIRD DISTRICT COURT OF APPEALS
OF THE STATE OF MARSHALL

BRIEF FOR PETITIONER

Allyson Bennett
Christina Dallen
David Kestenbaum
Attorneys for Petitioner

QUESTIONS PRESENTED

I. Whether the Court of Appeals erred in holding that the undetected, passive scanning of a voluntarily implanted RFID chip is so highly offensive to qualify as an invasion of the chip bearer's privacy.

II. Whether the Court of Appeals erred in holding that disclosure of an individual's high rank in a controversial organization is private such that its disclosure is offensive to a reasonable person and thus actionable.

III. Whether the Court of Appeals erred in holding that reverse engineering the encryption algorithm used by a RFID chip to achieve interoperability is a violation of this state's Anti-Circumvention Statute.

IV. Whether the Court of Appeals erred in holding that a RFID-based system is sufficient to protect a trade secret, absent a confidentiality agreement or notice.

CERTIFICATE OF INTERESTED PARTIES

The undersigned counsel of record certify that the following listed parties have an interest in the outcome of this case. These representations are made so that the Justices of this Court may evaluate any possible disqualification or necessary recusal.

BESS MARION ..... *Petitioner*
EDDIE CAFKA, ECC ENTERPRISES, INC. ..... *Respondent*

ATTORNEYS FOR BESS MARION
PETITIONER
(Signatures omitted in accordance with section 1020(5) of the Rules of the Twenty-Fourth Annual John Marshall Moot Court Competition in Information Technology and Privacy Law)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT

UNITED STATES COURT OF APPEAL

UNITED STATES DISTRICT COURT

STATE SUPREME COURT

STATE COURT OF APPEALS

STATE SUPERIOR COURT

STATE OF MARSHALL STATUTES

FEDERAL STATUTES

RESTATEMENTS

ARTICLES

TO THE SUPREME COURT OF THE STATE OF MARSHALL:

Appellant, Bess Marion, respectfully submits this brief in support of her request for reversal of the judgment of the court below.

OPINION BELOW

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

STATUTORY PROVISIONS

This case involves the following statutory provisions: Marshall Revised Code § 439(A); Marshall Revised Code § 562(B); Marshall Revised Code § 1492; and Marshall Revised Code§ 1947.

STATEMENT OF THE CASE

I. PROCEDURAL HISTORY

Eddie Cafka and his company ECC Enterprises, Inc. (together, "Appellee") filed a lawsuit in the Potter County Circuit Court against Appellant Bess Marion ("Marion") alleging (1) intrusion upon seclusion by unauthorized scanning through his body to read his implanted chip, (2) public disclosure of private facts by publication of the Bash Abortion Now membership list, (3) illegal circumvention of a technological measure that controls access to data, and (4) misappropriation of trade secrets. (R. at 1, 3.)

Marion filed a motion for summary judgment. (R. at 1.) The Potter County Circuit Court granted Marion's motion as to all four counts. (R. at 1.) The Third District Court of Appeals for the State of Marshall then reversed on all counts. (R. at 1.)

On July 15, 2005, this Court granted Marion leave to appeal the decision of the Court of Appeals reversing the Potter County Circuit Court's award of summary judgment in her favor. (R. at 9.)

II. STATEMENT OF THE FACTS

Marion is a computer programmer and researcher. (R. at 2.) Appellee hired Marion to work at ECC Enterprises, Inc. ("ECC") on a project called "Music Man." (R. at 2.) The "Music Man" project involved designing and building computers using a technology where the image created by the computer is displayed via brainwaves, eliminating the need for a computer screen. (R. at 1-2.) Marion's office was adjacent to Appellee's. (R. at 2.) Not all of Appellee's employees were housed in the same location as Appellee and Marion; no more than three worked in any one loca-

tion. (R. at 2.) Employees were not given each other's telephone numbers or e-mail addresses. (R. at 2.) Only Appellee knew all of the employees and locations. (R. at 2.) At the time of hire, each employee was required to sign an employment agreement and a non-disclosure agreement. (R. at 2.) However, Appellee did not have Marion sign the non-disclosure agreement until she had been employed at ECC for six months and offered no additional compensation for signing the agreement. (R. at 2.)

Appellee implanted himself and every employee of ECC with radio frequency identification ("RFID") chips. (R. at 2.) RFID chips are activated when they receive signals from a transponder. (R. at 2.) Appellee's RFID chips used a simple cryptographic algorithm to generate and broadcast a 64-bit serial number based upon a 16-bit code number received from the transponder. (R. at 2.) The chips and transponders controlled access to the computers and doors at ECC's offices. (R. at 2.) Computers at ECC cannot be accessed until the computer's transponder receives the appropriate serial number from the RFID chip of the assigned employee. (R. at 2.) Appellee's implanted chip contained an encryption system similar to that of his employees, but it gave him complete access to all computers and files on ECC computers. (R. at 2.)

Marion experimented with her implanted RFID chip, using a homemade transponder, and was able to reverse engineer the cryptographic algorithm that the chip used to generate serial numbers. (R. at 3.) Marion, after using her transponder to send various signals to Appellee's chip, was able to reverse engineer the algorithm in Appellee's chip and build a clone of the chip. (R. at 3.) With this cloned chip Marion was able to access computers at ECC and download onto a thumb drive data from Appellee's computer, including a file that contained a membership list for Bash Abortion Now. (R. at 3.) The media previously linked Bash Abortion Now to anti-abortion activities including finding, following and threatening doctors who performed abortions. (R. at 3.) The computer file listed Appellee as "Grand Nowest" of Bash Abortion Now. (R. at 3.)

Shortly after Marion downloaded the data from Appellee's computer, Appellee's membership in Bash Abortion Now was posted on a number of web blogs. (R. at 3.) Marion conceded that these postings were done by her or under her direction. (R. at 5.) As a result of the postings of his membership in Bash Abortion Now, Appellee lost funding for "Music Man." (R. at 3.)

Two weeks after the Bash Abortion Now information appeared on the Internet, Marion quit working for ECC and went to work for Softer Microns. (R. at 3.) Three months after Marion started working for Softer Microns, the company announced it was developing a new product that used brain waves as a control mechanism displaying images directly in the brain of the users. (R. at 3.)

SUMMARY OF THE ARGUMENT

The trial court properly granted summary judgment on all four counts because Appellee failed to show any genuine issue of material fact, even when the evidence is construed in the light most favorable to him. There is no actionable claim for intrusion upon seclusion because there was no unauthorized or highly offensive intrusion, the alleged intrusion was not private in nature, and the scanning of the chip itself did not cause anguish or suffering. The disclosure of the facts concerning Appellee's membership in Bash Abortion Now is not offensive to a reasonable person and is of legitimate public concern as it is a newsworthy political event, therefore barring tort liability for public disclosure of private facts. Marion did not violate the Anti-Circumvention Act because there was no underlying data to protect, RFID chips are not effective technological measures, and even if the Act applies, Marion is protected from liability by the interoperability exception. Further, Appellee does not have a protectable trade secret as he did not use reasonable measures to maintain the information's secrecy, because RFID chips do not adequately protect information.

I.

Appellee cannot prove an intrusion upon seclusion claim. Appellee required all employees be implanted with a RFID chip and all employees knew that radio frequency signals could be used at any time, without their awareness, to scan their implanted chip. The scanning was a condition of employment, and all implanted employees, including Appellee, authorized this activity by maintaining employment at ECC. Appellee's calculated engagement and active involvement in the project are enough to infer his consent to his RFID chip scanning. Because Appellee and his employees consented to the scanning and Marion used Appellee's technology in an authorized manner, the scanning does not reach the level of egregious or highly offensive conduct. The degree of the alleged intrusion is so minimal Appellee did not even notice. The context and conduct prove that RFID scanning is not highly offensive.

Radio frequency signals are not private; any expectation of seclusion therein is not objectively reasonable. The harm must flow from the intrusion itself for an actionable claim. In this case, Appellee's alleged anguish was a result of publication, not the scanning of his RFID chip itself. Accordingly, Appellee fails to establish an actionable intrusion upon seclusion claim.

II.

Marion cannot be liable for public disclosure of private facts, as postings Appellee's membership in Bash Abortion Now is protected by the

First Amendment publisher's privilege. Even if such posting was not protected, Appellee cannot prove public disclosure of private facts because there is no evidence to support publicity, the membership of Bash Abortion Now is not a private fact, the disclosure of a membership list is not highly offensive to a reasonable person, and it was a newsworthy matter and of legitimate public concern. There is no evidence that the web blogs reached a large public audience. Appellee has placed himself in the public eye and his membership is not a private fact. It is impossible for Appellee to prove the disclosure of his membership is highly offensive because he voluntarily acceded into a position of authority in Bash Abortion Now, thereby engaging in newsworthy events. Losing funding is commonplace in technological endeavors and does not reach the level of highly offensive. Marion is also protected by the First Amendment because the recent political actions of Bash Abortion Now make their membership a newsworthy matter and of legitimate concern to public safety. Therefore, there is no genuine issue of material fact and the trial court was correct in granting summary judgment for Marion.

III.

Marion did not violate the Anti-Circumvention Act because the Act does not apply to RFID chips as there is no underlying data to protect, the RFID chips are not effective technological measures, and even if the Act applies, Marion is protected under the interoperability exception. The only information contained on the RFID chip is the encryption program, which does not amount to "underlying data" for purposes of the Act. RFID chips are not effective at controlling access to data, as data can be accessed without decryption. Appellee's computer files were open to anyone as soon as he activated the computer with his own RFID chip, demonstrating the RFID chip's ineffectiveness. Even if reverse engineering the RFID chip encryption program falls under the Anti-Circumvention Act, Marion did not violate the Act because the decryption was necessary to achieve interoperability.

IV.

Appellee also fails in his fourth cause of action. Information is only a trade secret if the subject took reasonable measures to protect its secrecy. Because Appellee did not require Marion to sign a non-disclosure agreement or inform his employees that the project they were working on was confidential, he did not take reasonable measures to protect the secrecy of the project. RFID chips are also not adequate to protect information. Because Appellee failed to institute other security precautions or take affirmative steps to defend this information, he does not qualify

for trade secret protection. Thus, Appellee cannot establish misappropriation of a trade secret.

For these reasons, this Court should reverse the holding of the Court of Appeals and grant summary judgment for Marion because no genuine issues of material fact exist as to any of the four causes of action.

ARGUMENT

The right to privacy has been simplistically defined as the "right to be let alone." *Leopold v. Levin*, 259 N.E.2d 250, 254 (Ill. 1970). The right to privacy is not absolute and can be waived. *Melvin v. Burling*, 490 N.E.2d 1011, 1012 (Ill. App. Ct. 1986) (citing Russell D. Workman, *Balancing the Right to Privacy and the First Amendment*, 29 Hous. L. Rev. 1059, 1061-62 (1992)).

Summary judgment is proper where the evidence in the record demonstrates the absence of any genuine issue of material fact and the moving party is entitled to judgment as a matter of law. Marshall R. Civ. P. 56(c); *see Celotex v. Catrett*, 477 U.S. 317, 322 (1986). This Court reviews *de novo* the decision of the court of appeals. *See Elder v. Holloway*, 510 U.S. 510, 516 (1994). A mere scintilla of evidence in support of Appellee's position is insufficient to withstand summary judgment. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986). A grant of summary judgment is proper in this case because there are no genuine issues of material fact in any of Appellee's claims.

I. APPELLEE'S PRIVACY RIGHTS HAVE NOT BEEN VIOLATED BECAUSE PASSIVE SCANNING OF A RFID CHIP CANNOT CONSTITUTE INTRUSION UPON SECLUSION

The State of Marshall statute governing the tort of intrusion upon seclusion mirrors the Restatement (Second) of Torts. (R. at 4.) The statute provides that one who intentionally intrudes upon the seclusion of another or his private affairs is subject to liability for invasion of privacy, if the intrusion would be offensive to a reasonable person. Marshall Revised Code § 439(A); *see also* Restatement (Second) of Torts § 652B (1977). Although the Marshall statute was enacted many years ago, there is no case law on point. (R. at 4.) Accordingly, it is necessary to use the standards of other jurisdictions as guidance. (R. at 4.)

Illinois has established a four prong test for intrusion upon seclusion that incorporates the Restatement analysis. *Melvin*, 490 N.E.2d at 1013-14. A violation occurs only if (1) there was an unauthorized intrusion or prying into the plaintiff's seclusion, (2) the intrusion was offensive or objectionable to a reasonable person, (3) the manner in which the intrusion occurs is private, and (4) the intrusion caused anguish and suffering. *Id.*

All four elements must be satisfied for an actionable claim. *Id.* Although not explicitly articulated in the Restatement, most courts employ the anguish element of *Melvin* in their analysis. *See, e.g., Strutner v. Dispatch Printing Co.*, 442 N.E.2d 129, 134-35 (Ohio Ct. App. 1982) (explaining an invasion privacy occurred when plaintiff suffered humiliation, shame, and anguish); *Froelick v. Adair*, 516 P.2d 993, 998 (Kan. 1973) (stating an actionable invasion of privacy arises when the conduct of the intrusion is so outrageous it causes mental harm or anguish in a person of ordinary sensibilities); *Pulla v. Amoco Oil, Co.*, 882 F. Supp. 836, 848 (S.D. Iowa 1994) (explaining an invasion of privacy claim failed because it did not establish the intrusion caused anguish or suffering); *Ellenberg v. Pinkerton's, Inc.*, 202 S.E.2d 701, 703 (Ga. Ct. App. 1973) (denying an invasion of privacy claim for lack of mental anguish).

This Court should analyze the present cause of action using the *Melvin* standard because it is the most practical and straightforward way to articulate and define the requirements of intrusion upon seclusion. For this reason, state courts and federal courts, including the 7th Circuit, prestigious law review articles, American Jurisprudence, and the Practising Law Institute ("PLI") have endorsed this standard. *See, e.g.*, Michael J. Leech, *Federal, State and Common Law Privacy Issues for the Computer Age*, 696 PLI/Lit 231, 246 (2003).

Under the *Melvin* standard, Appellee fails to establish an intrusion claim because he authorized and consented to the implantation and scanning of all RFID chips. Additionally, a reasonable person would not find the scanning of Appellee's chip highly offensive as Appellee consented to scanning and made it a condition of employment at ECC. Moreover, RFID chips use radio frequency signals, which are not private. Finally, the intrusion did not cause anguish or suffering. To meet the statutory requirements, the anguish must flow from the intrusion itself, not any subsequent action. Appellee's alleged distress came only after publication on web blogs. Appellee cannot show a genuine issue of material fact on any theory of intrusion upon seclusion. Therefore, the trial court's grant of summary judgment was proper.

A. Appellee's Active Involvement, Knowledge, and Engagement Manifest Consent to the Scanning of His RFID Chip

Appellee's first cause of action fails because he consented to the scanning of his RFID chip. Intrusion upon seclusion is not actionable if the plaintiff consented to the defendant's intrusion. *Lewis v. Legrow*, 670 N.W.2d 675, 688 (Mich. Ct. App. 2003); *see Smith v. Calvary Christian Church*, 614 N.W.2d 590, 594 (Mich. 2000). Determining whether consent exists requires a factual inquiry into the circumstances of each

case. *Lewis*, 670 N.W.2d at 688. The right to privacy may be waived by express consent of the individual or anyone authorized by that individual. *Id.* (citing *Doe v. Mills*, 536 N.W.2d 824, 831 (Mich. Ct. App. 1995)). The right of privacy may also be waived by implied consent, which requires "a clear, unequivocal, and decisive act of the party showing such a purpose." *Id.*

In *Lewis*, three ex-girlfriends brought suit due to the existence of non-consensual videotapes of their sexual relations with the defendant in his bedroom. *Id.* at 680. Plaintiffs testified that the sexual relations were consensual; however, the taping was not and all three were unaware of the existence of rolling recording equipment. *Id.* at 681. The court held that the plaintiffs' consent to sexual activity did not include express or implied consent to be videotaped. *Lewis*, 670 N.W.2d at 682, 689, 697.

This case is distinguishable from *Lewis* because Appellee and other chip bearers were not involved in private intimate relations or in a bedroom, which deserves the utmost protection of privacy. *See Griswold v. Conn.*, 381 U.S. 479, 485-86 (1965); *see also Lawrence v. Tex.*, 539 U.S. 558, 565 (2003). There is a considerable difference in the degree of privacy that the courts will recognize in intimate associations and that which the courts will recognize in technological matters. Appellee fully consented to frequent scanning of his chip; in fact, Appellee could not have access to his own computer or building without permitting his chip to be scanned. While the plaintiffs in *Lewis* had no knowledge, Appellee had absolute knowledge and control in his project because he ordered the implantation of the RFID chips, knew of their existence, and made use of his and his employee's chips. (R. at 2.) The plaintiffs in *Lewis*, on the other hand, did not consent to the films and were unaware that the films could be released. *Lewis*, 670 N.W.2d at 681.

In *Smith*, a former church member brought suit alleging an invasion of privacy when the church disclosed confidential information about him. 614 N.W.2d at 591-92. The Supreme Court of Michigan denied the plaintiff's intrusion claim, deciding that knowledge and active involvement can make a person so engaged that they indicate and manifest consent. *Id.* at 593-94. Explicit assent is then unnecessary. *Id.* According to the Michigan Supreme Court, "[u]nder tort law principles a person who consents to another's conduct cannot bring a tort claim for the harm that follows from that conduct. This is because no wrong is done to one who consents." *Id.*

Appellee is engaged enough in the "Music Man" project to indicate manifest consent to all practices the project encompasses, including scanning his RFID chip. Appellee implanted the RFID chip in himself and in all of his employees for the purpose of scanning the chips. (R. at 2.) Appellee's chip was scanned every time he approached a transpon-

der, including when using any of the computers or doors at ECC locations. (R. at 2.) Marion did no more by scanning Appellee's RFID chip than Appellee had previously authorized and expected of his employees as a condition of employment. Appellee's thorough engagement and activity in the project render his explicit assent unnecessary. By maintaining their employment with ECC, all employees, including Appellee, authorized and consented to frequent scanning of their RFID chips. This case is analogous to *Smith* and thus warrants a similar finding that Appellee has no actionable claim for intrusion upon seclusion because no unauthorized intrusion occurred.

B. Imperceptible Scanning of a RFID Chip Is Too Minimal an Intrusion to Be Highly Offensive to a Reasonable Person

The Court of Appeals of the State of Marshall erred in concluding that the scanning of Appellee's implanted chip would be highly offensive to a reasonable person. (R. at 4.) To determine whether a cause of action for intrusion exists, a judge should make a preliminary determination of offensiveness by considering the degree of the intrusion; the context, conduct, and circumstances surrounding the intrusion; the setting of the intrusion; the expectations of those whose privacy was allegedly invaded; and the intruder's motives and objectives. *Wilkins v. Nat'l Broad. Co.*, 84 Cal. Rptr. 2d 329, 334 (Cal. Ct. App. 1999). Other jurisdictions typically find offensive intrusions when the defendant has intruded on the privacy of the plaintiff in the most direct and egregious ways. *Broughton v. McClatchy Newspapers, Inc.*, 588 S.E.2d 20, 28 (N.C. Ct. App. 2003). Examples include when patients are exposed during medical procedures or when fiduciary relationships are disregarded. *See, e.g., Sanchez-Scott v. Alza Pharm.*, 103 Cal. Rptr. 2d 410, 412-13, 420 (Cal. Ct. App. 2001) (finding intrusion upon seclusion when oncologist brought a non-professional to a breast exam and while plaintiff was naked the two men laughed); *see also DeMay v. Roberts*, 9 N.W. 146, 147-49 (Mich. 1881) (recognizing invasion of privacy when physician took an non-professional male to a patients home for a childbirth when no assistance was necessary). The California Supreme Court found no intrusion upon seclusion when human bodily functions were at issue, even though excretory functions are usually done in private and observation could cause embarrassment. *Hill v. Nat'l Collegiate Athletic Ass'n*, 26 Cal. Rptr. 2d 834, 859-60 (Cal. Ct. App. 1994). The court held that observation of urination for the purposes of drug testing and athletic safety in collegiate athletics was not an intrusion upon seclusion. *Id.* The *Hill* court reasoned that a unique set of demands and voluntary consent effectively diminished the expectation of privacy. *Id.* at 849, 860. When voluntary consent is present it is rare for a court to find highly offensive conduct. *Id.*

Marion's conduct is not highly offensive under these standards. Unlike the significant intrusion effected by the presence of unlicensed strangers at extremely private medical procedures in *Sanchez-Scott* and *DeMay*, the degree of intrusion alleged by Appellee is very minimal; so minimal in fact that Appellee was unaware of the intrusion for approximately four months. (R. at 3.) In addition, voluntary consent to the RFID chip implantation and scanning generates a unique set of demands. The "scanning" of Appellee's chip occurred in precisely the same way as Appellee authorized for regular use of his RFID chip. Therefore, no reasonable person would consider the scanning of Appellee's RFID chip intrusive, much less egregiously offensive. Significantly, permitting a person who voluntarily installed a RFID chip to make such unreasonable claims of intrusion upon seclusion based on the type of interaction for which the chip was designed would have considerable negative implications for future technological developments.

C. There Is No Reasonable Expectation of Privacy in RFID Chips Because There Is No Limit to Access By Radio Waves

Not every expectation of privacy and seclusion is protected by the law. In order to have a privacy interest the law will protect, there must be an actual and objectively reasonable expectation of solitude. *PETA v. Bobby Berosini, Ltd.*, 895 P.2d 1269, 1279 (Nev. 1995); *Shulman v. Group W Prods., Inc.*, 74 Cal. Rptr. 2d 843, 864 (Cal. Ct. App. 1998). An intrusion must be into a sphere from which an ordinary man in plaintiff's position would reasonably expect that the particular defendant would be excluded. *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir. 1969). For instance, a New Jersey court held that an expectation of privacy in a storage room to which others have keys and access is unreasonable and that a defendant's subjective belief of privacy therein is irrelevant. *White v. White*, 781 A.2d 85, 92 (N.J. Super. Ct. App. Div. 2001) (citing *State v. Brown*, 660 A.2d 1221, 1225 (N.J. Super. Ct. App. Div. 1995)). In *White*, the court determined Mr. White did not have an actionable intrusion claim when his wife accessed his personal e-mails because, although the computer was his, it was reasonably accessible to her. *Id.* The court concluded, "whatever plaintiff's subjective beliefs were as to his privacy, objectively, any expectation of privacy under these conditions is not reasonable." *Id.*

Regardless of Appellee's subjective beliefs as to his privacy, expecting privacy under these conditions is not objectively reasonable. Appellee's chip implantation and project design are novel and untested and therefore gave Appellee no established reason to expect privacy. More importantly, radio signals such as those used by Appellee's RFID chip, are by their nature not private, but rather are beamed indiscriminately

outward, where they can be received by anyone. The level of privacy expected in technological matters is less than in other arenas, partially because of the difficulty of ensuring privacy. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 1611 (1999) (noting that no successful standards exist for limiting the collection and utilization of personal data in cyberspace). Thus, Appellee would more reasonably have expected the signal to be intercepted than to remain private.

The facts of the present case are in line with *White* because though the chips, like the private e-mails, ideally were to remain private, they were accessible to persons other than the person asserting privacy. Just as the wife's ability to access the "private" e-mails in *White* precluded that plaintiff's intrusion claim, the public accessibility of the RFID radio signal precludes Appellee's intrusion claim. Appellee did not have a reasonable expectation of privacy in the RFID signals and therefore can have no claim for intrusion upon seclusion in this case.

D. The Passive Scanning of the RFID Chip Itself Did Not Cause Anguish or Suffering

Appellee cannot prove a violation because the intrusion itself did not cause anguish or suffering. The tort of intrusion upon seclusion is aimed at the discomfort caused by the intrusion itself. *Thomas v. Pearl*, 998 F.2d 447, 452 (7th Cir. 1993) (emphasis added). In *Thomas*, a basketball coach recorded phone conversations of a recruit to reveal illegal recruiting. *Id.* at 449. However, the court did not accept the invaded seclusion claim, reasoning that neither the conversations nor the recording caused the suffering, but rather the later publication of the conversations. *Id.* The *Thomas* court held that the claim was not actionable because *Lovgren v. Citizens First Nat'l Bank of Princeton* established that a "plaintiff fails to state a claim for invaded seclusion if the harm flows from the publication rather than the intrusion." *Id.* (citing *Lovgren*, 534 N.E.2d 987, 989 (Ill. 1989)).

Appellee did not suffer any anguish as a result of the intrusion, itself. In fact, he was unaware of such intrusion until months later. (R. at 3.) The suffering and embarrassment resulted from the publication of the Bash Abortion Now list on web blogs and the loss of funding, which were subsequent to the allegedly intrusive scanning. (R. at 3.) Just as the *Thomas* plaintiff was a willing party to the recorded conversations, Appellee was a willing party to the chip implantation and RFID scanning. Like the allegations in *Thomas*, the alleged violation stems not from the alleged intrusion itself, but rather from later publication and conduct. Therefore, as in *Thomas*, Appellee's intrusion upon seclusion claim is not cognizable.

Appellee fails to establish any prong of the principal standard set forth in *Melvin*, much less all four elements required for an actionable intrusion upon seclusion claim. There was no unauthorized intrusion as Appellee consented to the RFID scanning. The alleged intrusion does not reach the standard of highly offensive to a reasonable person. Not every expectation of privacy is protected, because subjective desires for privacy are irrelevant. In addition, the alleged intrusion, itself, did not cause anguish and suffering. There is no genuine issue of material fact in this claim and this Court should reverse the Court of Appeals and hold that no cause of action maintains for intrusion upon seclusion.

II. NO PRIVATE FACT RELATING TO APPELLEE WAS DISCLOSED; ALTERNATIVELY, DISCLOSURE OF APPELLEE'S HIGH IN BASH ABORTION NOW WAS OF LEGITIMATE PUBLIC CONCERN

Appellee has no cognizable claim for disclosure of a private fact. The State of Marshall has enacted a statute that follows the Restatement (Second) of Torts governing claims for invasion of privacy, public disclosure of private fact. (R. at 5.) The statute states that liability for invasion of privacy exists if someone gives publicity to a matter concerning the private life of another and the matter publicized would be highly offensive to a reasonable person and not of legitimate concern to the public. Marshall Revised Code § 562(B); Restatement (Second) of Torts § 652D (1977). Following the Restatement, many jurisdictions require the following elements of the tort: (1) publicity, given to (2) private facts, (3) which would be highly offensive to a reasonable person and (4) is not of legitimate concern to the public. *Harris v. Easton Publ'g Co.*, 483 A.2d 1377, 1384 (Pa. Super. Ct. 1984); *see also Brown v. Mullarkey*, 632 S.W.2d 507 (Mo. Ct. App. 1982).

Appellee alleges an invasion of privacy by the public disclosure of the fact that he is the Grand Nowest of Bash Abortion Now. However, Marion cannot be liable because she is protected by the First Amendment publisher's privilege. Even if Marion is not protected, Appellee's claim does not meet any of the necessary criterion. Appellee does not have an actionable claim for invasion of privacy by public disclosure of private fact because there is no evidence of publicity, the membership list is not a private fact, the disclosure of the membership list is not highly offensive to a reasonable person, and the disclosure is a newsworthy fact of legitimate concern to the public. Appellee holds a position of public notoriety because the scrutinized actions of Appellee and the Bash Abortion Now group make the disclosure of social value and bring

Appellee into a position of public notoriety. Marion is not liable for this alleged invasion of privacy.

A. The First Amendment Publisher's Privilege Protects Marion's Disclosures

As a preliminary matter, a communication is absolutely privileged when its promulgation is of such major concern to the public interest that the publisher should be able to speak fully and without fear of liability. *Muck v. Van Bibber*, 621 N.E.2d 1043, 1045 (Ill. App. Ct. 1993). This privilege, extended to publishers as a defense in torts issues such as defamation, is based on the idea that conduct which otherwise would be actionable should be free from liability because the defendant's acts further social interest and are entitled to protection, even at the expense of harm to the plaintiff's reputation. *Muck*, 621 N.E.2d at 1045. The scope of the absolute privilege is narrow, but the Restatement (Second) of Torts also grants immunity when there is reasonable belief as to the existence of privilege. Restatement (Second) of Torts § 595 cmt. c (1977).

In the case at hand, Marion acted in furtherance of an interest of social importance: public safety. Marion's actions can be likened to a publisher because of the media attention and news accounts that were already circulated linking Bash Abortion Now to anti-abortion activities. (R. at 3.) Marion contributed to the circulation of important political and safety discussions and therefore deserves immunity under the publisher's privilege. Editorials that are published in the news or in online newspapers, or heard on television or the radio, are analogous to postings on web blogs, and web blogs deserve the same First Amendment protection, especially in matters of public safety and important social and political importance. The Court of Appeals found that a web blog was a publication, but inexplicably and without elucidating its reasoning determined such publication did not qualify for First Amendment protection. (R. at 5.) This rigid application constitutes a violation of free speech and freedom of the press, and if upheld will stifle future dissemination of news in this emerging and important medium.

Even if Marion does not qualify directly for the publisher's privilege, Marion reasonably believed she was qualified under the privilege and acting in the public's interest, which extends the scope of the absolute privilege to protect her publication under the reasoning of the Restatement. Marion is therefore protected by the First Amendment privilege and cannot be liable for publication of the Bash Abortion Now membership list.

B. No Evidence Supports the Allegation that Appellee's Membership in Bash Abortion Now Was Publicized

Even if Marion is not protected by the publisher's privilege, she is not liable for disclosing a private fact because the requirement of publicity cannot be proven. To state an actionable claim under the statute, it is essential that the private fact must actually be given publicity. "The elements of 'publicity' require that the matter is made public, by communicating it to the public at large, or to so many persons that the matter . . . become[s] one of public knowledge." *Harris*, 483 A.2d at 1384; *see also* Restatement (Second) of Torts § 652D cmt. a (1977). Therefore, in order to be actionable, the communication involving private facts must reach, or be sure to reach, the public. *Harris*, 483 A.2d at 1384. No action lies if the fact was communicated to "a single person or even to a small group of persons." Restatement (Second) of Torts § 652D cmt. a (1977).

The posting of Appellee's position in Bash Abortion Now on web blogs does not amount to publicity. In this case, Appellee relies on these postings to satisfy the publicity criteria but offers no evidence of how many people accessed the web blogs. Appellee thus fails to make any showing of publicity at all. The Court of Appeals also failed to offer any estimation of how many people accessed the blogs or whether Appellee's position in Bash Abortion Now became a matter of public knowledge. (R. at 5.) In order for the publicity prong to be satisfied, these web blogs must have been accessed or viewed by more than a small group of people. *See Harris*, 483 A.2d at 1384.

Under the Restatement, Appellee's claim has no merit if the fact was communicated to only a small group. Restatement (Second) of Torts § 652D cmt. a (1977). There is no showing in the record of whether some threshold number of people actually accessed the web blogs and were therefore apprised of the alleged private fact. Although Appellee need only prove a genuine issue of material fact, Appellee has failed to make even the most basic showing that a large number of people accessed the web blogs. Absent such showing that a sufficient number of persons accessed the web blogs to constitute "publicity," Appellee fails to produce even a scintilla of evidence that his membership was publicized. The grant of summary judgment for Marion was therefore proper.

C. Appellee's Membership in Bash Abortion Now Is Not a Private Fact Because It Is Open to the Public Eye

Appellee's membership in Bash Abortion Now is not a private fact because his high rank, coupled with the media coverage of the organization, leaves him open to the public eye. In order to state a valid claim for relief, publicity must be given to a private fact. *Harris*, 483 A.2d at 1384. It also follows that the recipient of the information must not have had

prior knowledge of that fact. *Id.* Similarly, the California Court of Appeals stated that "[t]here is no liability when the defendant merely gives further publicity to information about [the] plaintiff which is already public or when the further publicity relates to matters which the plaintiff leaves open to the public eye." *Sipple v. Chronicle Publ'g Co.*, 201 Cal. Rptr. 665, 669 (Cal. Ct. App. 1984). Another court looked to the fact that the plaintiff was in "public and in plain view" when she kissed the defendant to show that it was not a private fact. *Daly v. Viacom*, 238 F. Supp. 2d 1118, 1124 (N.D. Cal. 2002). In *Daly*, anyone on the public street or in viewing distance of the plaintiff could clearly see them kiss so it was no longer private. *Id.*

Here, Appellee's membership in Bash Abortion Now does not qualify as a private fact. The public media has linked Bash Abortion Now to the tracking down and threatening of doctors who perform abortions. (R. at 5.) Appellee has achieved the rank of Grand Nowest of the organization. (R. at 3.) Although the Court of Appeals stated that Appellee "kept his membership in Bash Abortion Now secret," his membership was still open to the public eye. (R. at 5.) There is no showing that, during Appellee's involvement with Bash Abortion Now, he was at any time shielded from other members, or that the organization employed any provisions to keep their membership secret. Even though Appellee may have wanted to keep his membership secret, there is no showing that made any effort to prevent exposure of his affiliation with the group. In fact, he possessed a file that contained his name, along with the names of other members. (R. at 3.) Because Marion merely published information that Appellee left open to the public eye, this Court should find that Appellee's membership in Bash Abortion Now is not a private fact.

Appellee's role in Bash Abortion Now makes him a public figure and his membership is, therefore, not a private fact. Based on his high ranking position in Bash Abortion Now, Appellee has placed himself at the forefront of a public controversy. Although dealing with a defamation claim, the United States Supreme Court in *Gertz v. Robert Welch, Inc.* held that people can be classified as public figures when they "have thrust themselves to the forefront of particular public controversies in order to influence the resolution of the issues involved." 418 U.S. 323, 345 (1974). Appellee's high rank in Bash Abortion Now invites attention and comment and certainly thrusts him to the forefront of the abortion controversy. Although *Gertz* involved a defamation claim, it is analogous to the case at bar because once it has been established that Appellee is a public figure with respect to his membership in Bash Abortion Now, it naturally follows that his membership is not a private fact.

Privacy is also not invaded when the defendant gives publicity to a business or activity in which the plaintiff is engaged in dealing with the public. Restatement (Second) of Torts § 652D cmt. b (1977). The Mary-

land Court of Special Appeals stated in *Furman v. Sheppard* that "while appellants did belong to a 'private' yacht club, their yacht was in navigable water in open view to the public." *Furman v. Sheppard*, 744 A.2d 583, 588 (Md. Ct. Spec. App. 2000). In that case, the defendant entered the yacht club after a member opened the gate, and videotaped the plaintiffs without their consent. *Id.* The *Furman* plaintiffs argued that the club was "private" because it was surrounded by an electronic security fence, had posted signs warning against trespassing and required a magnetic gate card to enter. *Id.* at 585. The court disagreed, holding that since the yacht was in navigable waters when videotaped, it did not matter that the club itself was private. *Id.* at 588.

Daly and *Furman* are analogous to the case at bar because there is no showing that those interested in Bash Abortion Now, presumably due to the media attention, could not just come in off the streets and observe Appellee in plain view as a member or in his position as Grand Nowest. Much like the yacht club at issue in *Furman*, Bash Abortion Now should be considered a private club that nevertheless operates in open view to the public. Moreover, unlike in *Furman*, there was no evidence that Bash Abortion Now had any security measures to exclude outsiders. In this context, Marion only gave publicity to an activity in which Appellee deals with the public. Therefore, Appellee does not satisfy the requisite private fact element of this tort and his claim must fail.

D. Publicity Given to a Voluntarily Accepted High Rank in a Controversial Organization Cannot Be Highly Offensive

Even if there was publicity given to a private fact, such publicity was not highly offensive to a reasonable person. The third element of a disclosure of private fact claim requires that a reasonable person of ordinary sensibilities would find the publicity highly offensive. *Harris*, 483 A.2d at 1384. In *Harris*, the court determined that, in assessing whether the publicity would be highly offensive, the "customs of the time and place, occupation of the plaintiff and habits of . . . fellow citizens are material." *Id.*; *see also* Restatement (Second) of Torts § 652D cmt. c (1977). In *Doe v. Mills*, the Court of Appeals of Michigan dealt with a case involving plaintiff's whose real names were placed on signs in public view indicating that they were about to undergo abortions. 536 N.W.2d 824, 827 (Mich. Ct. App. 1995). The court stated that it "cannot say that a reasonable person would not be justified in feeling seriously aggrieved by such publicity" and found that the plaintiff's allegations were sufficient to constitute a question for the jury. *Id.* at 829.

Unlike *Doe*, the case at hand does not present allegations sufficient to constitute a question for the jury; membership in a group of national

concern is significantly different than the very private and very intimate decision to terminate a pregnancy. In *Doe*, the plaintiff's personal choice to have an abortion had nothing to do with the public interest in the subject of abortions in general. There was no showing that the plaintiffs in *Doe* were high-ranking members in any pro-choice group. There was also no showing that the plaintiffs had any interest in influencing public policy by joining such a group. In contrast, Appellee did choose to join a prominent anti-abortion group and attained a high rank in that group, both of which indicate that he was interested in influencing public policy through the group. A reasonable person of ordinary sensibilities would not find highly offensive the exposure of Appellee's involvement in a group through which he intended to participate in the public debate about abortion, because Appellee chose to put himself in that position. Appellee also makes no showing that he, personally, was highly offended by the actual publicity of his membership in Bash Abortion Now. Therefore, this Court should reverse the Court of Appeals and find the disclosure of Appellee's association with Bash Abortion Now not actionable.

E. Legitimate Public Concern Justifies Disclosure of Appellee's Status in Bash Abortion Now

Under the final prong of public disclosure liability, no liability exists if the revealed information is of legitimate public concern. *Harris*, 483 A.2d at 1384. The right of privacy, the right of the public to be informed, and freedom of the press are all relative and limited, and none are absolute. *Blount v. T.D. Publ'g Corp.*, 423 P.2d 421, 424 (N.M. 1966). "Further, the right of privacy is generally inferior and subordinate to the dissemination of news." *Id.* When a matter of publicity is of legitimate public concern, there is no invasion of privacy under the common law and Constitution. *Sipple*, 201 Cal. Rptr. at 668. The right of privacy must ultimately be balanced against the competing constitutional right to publish newsworthy matters and accordingly the right to privacy must give way when necessary to ensure uninhibited discussion of legitimate public issues. *Goodrich v. Waterbury Republican-Am., Inc.*, 448 A.2d 1317, 1324 (Conn. 1982). "Freedom of discussion must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period." *Briscoe v. Reader's Digest Ass'n*, 93 Cal. Rptr. 866, 870 (Cal. Ct. App. 1971) (quoting *Thornhill v. Ala.*, 310 U.S. 88, 102 (1940)). The scope of the privilege of publicity extends to almost all reporting of recent events; and almost any truthful commentary on public affairs, no matter how serious the invasion of privacy, will be privileged. *Id.* at 870.

A balance between personal privacy and freedom of the press is necessary; thus the critical issue is the presence or absence of legitimate

public concern and newsworthiness in the matter. *Shulman v. Group W. Prods., Inc.*, 74 Cal. Rptr. 2d 843, 852 (Cal. Ct. App. 1998). To determine what constitutes "newsworthy," courts consider the following factors: (1) the social value of the facts published; (2) the depth of the articles intrusion into ostensibly private affairs; and (3) the extent to which the party voluntarily acceded into a position of public notoriety. *Kapellas v. Kofman*, 81 Cal. Rptr. 360, 370 (Cal. Ct. App. 1969). As a result, "when the legitimate public interest in the published information is substantial, a much greater intrusion into an individual's private life will be sanctioned, especially if the plaintiff willingly entered the public sphere." *Id.* In analyzing the elements of the newsworthy standard, courts have found social value of the facts published to involve the customs of society, community mores, and the focus of public attention at the time. *Virgil v. Time, Inc.*, 527 F.2d 1122, 1129 (9th Cir. 1975); *Sipple*, 201 Cal. Rptr. at 669-70; *Briscoe*, 93 Cal. Rptr. at 874-75. New York has also explicitly held information about "political happenings" is newsworthy. *Messenger v. Gruner Jahr Printing and Publ'g*, 727 N.E.2d 549, 552 (N.Y. 2000). Finally, a summary judgment motion in such cases is an approved and encouraged procedure because unnecessary and prolonged litigation would have a chilling effect on the exercise of First Amendment rights. *Sipple*, 201 Cal. Rptr. at 668.

The trial court correctly granted summary judgment for Marion as it is particularly appropriate in First Amendment cases, and the publicized matter in this case is newsworthy and incorporates constitutional protection. The Court of Appeals' reasoning is flawed because the court admits membership in Bash Abortion Now is not inherently offensive, but then declares the disclosure of such inoffensive membership is offensive. (R. at 5.) The court also cites *NAACP v. Alabama*, which is inapposite. *See NAACP v. Ala.*, 357 U.S. 449, 460 (1958). Unlike the members of the NAACP, not known for menacing acts, members of Bash Abortion Now have followed and threatened doctors and intentionally engaged themselves in the abortion debate.

This First Amendment privilege should extend to Marion's disclosure of Bash Abortion Now's membership because it is a "hot news" item of immediate public concern and a truthful commentary on public affairs. A number of news media accounts linked Bash Abortion Now to anti-abortion events, including the following and threatening of doctors who performed abortions, which made the group known to the public. (R. at 3.) The disclosure and publication of the Bash Abortion Now membership list is not a revelation of a fact so offensive as to shock the community's notions of decency because it is just a list of names and it is newsworthy. The publication of the Bash Abortion Now membership list is, however, newsworthy and of legitimate public concern because it was a dissemination of a political happening and is of social value. Abortion

is one of most controversial political issues in society today. It is a prominent focus of public attention and involves deeply-rooted societal beliefs.

The second element of newsworthiness is also met, as the publication did not reach the requisite depth into ostensibly private affairs. Appellee was very active in Bash Abortion Now, as he reached the Grand Nowest position. As a result, many people likely know him in this capacity and know the extent of his involvement. Appellee did not successfully keep the information about his membership a secret and private as he left the membership list in a work file which he could not be completely sure was private. Marion gained easy access to the information without even seeking this type of information about Appellee. Further, the prior media coverage of Bash Abortion Now's activities exemplifies that the matter was not deeply private. Because others had knowledge of Appellee's role in Bash Abortion Now, the list was kept in a non-secure and non-private place, and given the media interest in this political issue, the membership list was clearly not deep in private affairs.

The third component of newsworthiness is also met because, through his actions and associations with Bash Abortion Now, Appellee became a public figure, therefore thrusting himself into public notoriety. As *Shulman* explained, the broadcast is of legitimate public concern if a logical relationship to a newsworthy subject exists, even if the otherwise private person is involuntarily caught up in events of public interest. *Shulman*, 74 Cal. Rptr. 2d at 852. Even if Appellee desired privacy, by participating in Bash Abortion Now he put himself within the reach of newsworthy events and public affairs, thus becoming a public figure and barring his cause of action for this tort. In *Kapellas*, the court explained that those who assume public positions must realize they are subjecting themselves to "a searching beam of public interest and attention." 81 Cal. Rptr. at 371. The case here is analogous, because although it is unclear whether Bash Abortion Now elected Appellee to this position, he nonetheless acceded into a position of power and notoriety within the group by becoming the Grand Nowest. Appellee therefore subjected himself to public interest and attention through his involvement with the group. Additionally, Appellee's status as a well-known entrepreneur working on revolutionary technology makes his affiliations of public concern. Both facets of Appellee's actions and affiliations make him a public figure in newsworthy events and of legitimate public concern, sanctioning Marion's disclosure of the membership list and barring Appellee's tort claim.

In *Duran v. Detroit News, Inc.*, the Michigan Court of Appeals held that the publication of the location of a former Columbian judge was not an invasion of privacy because death threats against the judge placed neighbors in danger and thus the location was of legitimate concern to the public. *Duran v. Detroit News, Inc.*, 504 N.W.2d 715, 720 (Mich. Ct.

App. 1993). This case is analogous to *Duran*, because those in the vicinity of potential targets could benefit from the information. This Court should follow the reasoning of the *Duran* court, that public safety is a legitimate concern and worthy of news publication; citizens deserve to have full information about incendiary groups like Bash Abortion Now and their leader. In *American Knights of the Ku Klux Klan v. Kerik*, the Second Circuit Court of Appeals rejected the view that the First Amendment is implicated every time a law makes someone less willing to exercise their free speech rights. *Am. Knights of the Ku Klux Klan v. Kerik*, 356 F.3d 197, 209 (2d Cir. 2004). The court reasoned that "the individual's right to speech must always be balanced against the state's interest in safety . . . ." *Id.* Here, the First Amendment protection of freedom of publicity and discussion is essential for public safety, and the right of association is less compelling. Therefore, Marion's revelation of Appellee's membership in Bash Abortion Now is protected by the First Amendment.

The disclosure of the Bash Abortion Now membership list did not satisfy the requisite need for publicity, the membership was not a private fact, and the disclosure would not be highly offensive to a reasonable person. In addition, the First Amendment protects the publication of this information since it was newsworthy and constitutes a legitimate concern to public safety. A balance is always weighed in favor of free expression, and Marion respectfully requests this Court adhere to this precedent and affirm the trial court's holding that no actionable invasion of privacy or genuine issue of material fact exists, warranting summary judgment for Marion.

III. REVERSE ENGINEERING APPELLEE'S RFID CHIP CANNOT VIOLATE THE ANTI-CIRCUMVENTION ACT BECAUSE APPELLEE'S DESIGN DOES NOT PROTECT ANY INFORMATION

A claim under the Anti-Circumvention Act (the "Act") must prove three necessary elements: the alleged violator (1) circumvented a technological measure (2) effectively controlling access to (3) underlying data. Marshall Revised Code § 1492. The Act contains two exceptions precluding liability where the circumvention occurred to facilitate device interoperability or encryption research. *Id.* Even viewing the facts in the light most favorable to Appellee, Marion did not violate the Anti-Circumvention Act for three reasons. First, the Act does not apply to the RFID chips because there is no underlying data to protect. Second, the RFID chips were not effective technological measures. Third, even if the Act applies, Marion is protected by the interoperability exception.

Although there is no case law construing the Anti-Circumvention Act, case law in other jurisdictions construing the federal Digital Millennium Copyright Act ("DMCA") is instructive.[1] Sections 1201(a)(1)(A), 1201(a)(3), and 1201(f)(1) of the DMCA contain substantially similar language to that in the Anti-Circumvention Act. *See* 17 U.S.C. § 1201 (2005); Marshall Revised Code § 1492. Though the DMCA refers specifically to copyrighted information, as opposed to underlying data, the relevant portions of the statute, dealing with circumvention, effective technological measures, and interoperability, are nearly indistinguishable from the Anti-Circumvention Act provisions.

A. Appellee's RFID Chip Contains No Underlying Data to Trigger the Protection of the Anti-Circumvention Act

At its very heart, the Anti-Circumvention Act requires that the circumvented measure "prevent access to data." Marshall Revised Code § 1492. The Anti-Circumvention Act also makes multiple references to the "owner of the underlying data." *Id.* In other words, the circumvented measure must control access to underlying data.

The Anti-Circumvention Act cannot apply to Marion's reverse engineering of the RFID chip encryption program because there is no underlying data on the RFID chip. The only data on the chip is the encryption program. (R. at 2.) An encryption program cannot be both a technological measure and the underlying data the technological measure protects. Rationally, a technological measure cannot "guard" itself. More importantly, there is no data "underlying" the encryption program for purposes of the statute, as there is no data on the chip accessible only by use of the encryption program. For example, video data on DVDs is protected by the CSS encryption program. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 309-310 (S.D.N.Y. 2000), *aff'd* 273 F.3d 429 (2d Cir. 2001). One must circumvent the CSS program to access the video content. *Id.* The video data "underlies" the CSS encryption because it can only be accessed by circumventing or bypassing the encryption. In contrast, as access to the actual data of the RFID encryption program is not protected by the encryption, the data cannot be "underlying." Therefore, because there is no "underlying data," the Anti-Circumvention Act does not apply to circumventing the RFID encryption program.

Appellee may argue that the "underlying data" required to make the Anti-Circumvention Act applicable is the data on his computer, rather than data on the RFID chip. However, such a construction of the statute defies not only the plain language of the statute but also any reasonable construction of the Act. The first step in any statutory interpretation is

1. Although the DMCA protects copyrighted materials specifically, the goal of both acts is to protect property rights in the underlying material.

to examine the plain language of the statute. *See Gwaltney of Smithfield, Ltd. v. Chesapeake Bay Found.*, 484 U.S. 49, 56 (1987). According to the language of the Anti-Circumvention Act, the Act is violated only if the circumvention is performed without the "authority of the owner of the *underlying data*." Marshall Revised Code § 1492(a) (emphasis added). Similarly, a technological measure only effectively controls access to data if the ordinary course of its operation requires application of information or a process "with the authority of the owner of the underlying data." Marshall Revised Code § 1492(b). It is noteworthy that the statute does not use the phrase "owner of the *data*," but rather specifies that the targeted data must be underlying. The Act can therefore only be reasonably construed to mean that relevant data cannot be any tangentially-related data, but rather must be directly underlying the circumvented technological measure.

Here, the Anti-Circumvention Act does not apply to circumvention of the RFID encryption because the computer data was not directly protected by the encryption. The data on Marion's computer was a number of steps away from the encryption on the RFID chip; the encryption program did not interact with or even coexist in a machine with the data. The encryptions program's only action was to translate the 16-bit code into a 64-bit serial number. Various transponders then received the code and ran their own processes to determine whether to grant access. Marion then had to interact with the machine and identify, locate and remove the files. Given the remote relationship between the encryption program and the data on Appellee's computer, the computer data could not satisfy the definition of underlying needed to trigger application of the Anti-Circumvention Act.

B. RFID Chips Do Not Effectively Control Access to Data for Purposes of the Anti-Circumvention Act

Even if the encryption program on the RFID chip did protect underlying data, it did not effectively control access to that data. Section B of the Act provides that "a technological measure 'effectively controls access to data' if the measure, in an ordinary course of its operation, requires the application of information, or a process, or a treatment, with the authority of the owner of the underlying data, to gain access to the data." Marshall Revised Code § 1492(b).

The DMCA contains a substantially similar definition, requiring the application of information, a process or a treatment, with the authority of the owner to gain access. 17 U.S.C. § 1201(a)(3)(b). In *Reimerdes*, the court held that a 40-bit encryption system was an effective measure of control because access required use of three "keys" available only by licensing from the owners. 111 F. Supp. 2d at 317-318. The encryption

program prevented access to the underlying material, except after applying the keys or the decryption program at issue. *Id.* In contrast, the Sixth Circuit held that, where files were otherwise accessible, circumvention of a technological measure intended to prevent a printer from starting up did not effectively control access to those files. *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 548-549 (6th Cir. 2004). Notably, the Court of Appeals for the Federal Circuit determined that effective control requires protection of the underlying program, not just literal control of access. *The Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1201 (D.C. Cir. 2004) (holding that the DMCA could not intend to include disabling a burglar alarm on a building containing material under the definition of circumvention of an effective technological measure).

Here, as in *Lexmark*, the RFID chip encryption program did not effectively control access to the data because the data could be accessed without decrypting the program. Gaining entry into a computer at Appellee's office only required one interaction with the permitted RFID chip, not continuing interaction. (R. at 2.) The data on Appellee's computer was therefore accessible without any circumvention of the RFID encryption program; any person could access the computer by simply waiting for Appellee to activate the computer by means of his own RFID chip. The contents of the computer, including the files in question, were then completely open to that person. In contrast, the protected data in *Reimerdes* could only physically be accessed through the encryption program. No other method, much less such a straightforward, non-technological method, could be used. The current case more closely resembles *Lexmark*: in both, the files themselves were not protected by the alleged technological measure, but rather only the ability to start up the machine. Therefore, a measure that protects only the ability to start up the machine does not "effectively control access" to files contained thereon for purposes of the Anti-Circumvention Act. Unless some concept of protection is understood in the access requirement, the Anti-Circumvention Act could be grossly distorted to create liability for picking a lock on a building in which a single piece of data could be found. The *Chamberlain* court correctly found such an expansive reading of the DMCA untenable; such an irrational and overreaching reading of the Anti-Circumvention Act should also be disregarded. Therefore, the Anti-Circumvention Act should not be read to create liability for circumvention of a measure that neither directly controls access to nor is closely-related to protecting the underlying data.

C. Reverse Engineering the RFID Chip Encryption Program Was Necessary to Achieve Interoperability

Even if the RFID chip encryption program effectively controlled access to underlying data, Marion's conduct did not violate the Anti-Circumvention Act because the reverse engineering she performed was necessary to achieve interoperability with the transponders' programs. The Anti-Circumvention Act includes a safe harbor provision for reverse engineering in order to achieve interoperability. Marshall Revised Code § 1492. The Act provides that it shall not be a violation of the Act to reverse engineer a technological measure "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs." *Id.* However, the Act also requires that the person reverse engineering the program have lawfully obtained the right to use the program. *Id.* The DMCA contains a similar provision, allowing for reverse engineering to achieve interoperability. 17 U.S.C. § 1201(f). Like the Anti-Circumvention Act, the DMCA provides that reverse engineering may only be performed by a person who has lawfully obtained access to the computer program. *Id.*; *see* Marshall Revised Code § 1492. In *Lexmark*, the Sixth Circuit held that any purchaser of a Lexmark printer automatically gained lawful access to any programs contained within that computer, for purposes of the DMCA. 387 F.3d at 546.

Here, Marion's conduct is protected by the safe-harbor provisions because she reverse engineered the encryption algorithm for purposes of creating an algorithm interoperable with an external transponder. Without reverse engineering the existing algorithm, Marion could not have achieved interoperability with the transponders. Similar to the legal interoperability between a replacement garage door remote and another company's garage door opener in *Skylink*, interoperability was the sole purpose Marion's reverse engineering. Marion did not attempt to sell or distribute the reverse engineered algorithm or use the information for any purpose other than interacting with the transponders. The Anti-Circumvention Act does not specify that interoperability need be for any particular or even any lawful reason. So long as Marion sought to achieve interoperability, what she did with the interoperable device is irrelevant.

Appellee may argue that Marion did not meet the requirement of lawful procurement of the right to use the encryption program. However, Appellee is mistaken on two counts. First, Marion obtained the lawful right to use the encryption program located on the RFID chip implanted in her own arm; otherwise, she would not have been able to or allowed to use the chip to access the site, her office, or her computers. Just as any person lawfully obtaining a Lexmark printer obtained lawful

access to any software on that printer for their use, Marion obtained access to any software implanted in her arm for her use. It is not clear whether the encryption program on Appellee's chip was any different than the program on Marion's chip. If not, Marion had already lawfully received access to a copy of the program, by means of her chip.

Even if the programs were different, however, Marion could still lawfully obtain the right to use Appellee's encryption program because Appellee's chip necessarily broadcast the encrypted signals to any nearby transponder. A RFID chip signal can be picked up with any available transponder, whether installed by Appellee or not. In addition, any transponder can send an activation signal to Appellee's or Marion's RFID chips and thus receive back a 64-bit serial number generated by the encryption program, as Marion did with her own transponder and RFID chip. (R. at 3.) By using a measure that could be activated, utilized, and intercepted by any transponder from any source, Appellee effectively placed the encryption program on his RFID chip in the public domain. In fact, Appellee could not by any means prevent any member of the public from using the encryption program. Any person with a transponder had legal access to Appellee's encryption program. Because Marion obtained legal access to the encryption program – either through its presence in her own chip or its public accessibility – she was entitled to reverse engineer the program to achieve interoperability with the transponders.

The Anti-Circumvention Act is not applicable to Marion's decryption of the RFID encryption program because the program did not protect any underlying data, as required by the Act. In addition, even if the program controlled access to any data, it did not effectively control that access. Finally, regardless of whether the conduct otherwise might violate the Anti-Circumvention Act, Marion's conduct was specifically exempted from liability by the reverse engineering safe harbor provision.

IV. APPELLEE'S FAILURE TO EMPLOY REASONABLE MEASURES TO MAINTAIN SECRECY PRECLUDES TRADE SECRET PROTECTION

For Appellee to have a protectable trade secret, it must fall under Marshall's Trade Secrets Act, codified at Marshall Revised Code § 1947. (R. at 7.) In order to be a trade secret, "technical data" must be: (1) sufficiently secret to derive economic value from not being generally known and (2) subject to efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality. Marshall Revised Code § 1947. Other jurisdictions have similarly held that a trade secret must derive economic value from its secrecy and it must be the subject of measures that are reasonable under the circumstances to protect it. *See, e.g.*,

Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) (explaining that the subject of a trade secret must be secret and not of general knowledge in the public or in the trade or business). In *People v. Chung-Ta Hsieh*, the California Court of Appeal stated, "there is no trade secret protection for information known . . . to those skilled in the particular field." 103 Cal. Rptr. 2d 51, 56 (Cal. Ct. App. 2000). Finally, the possessor of a trade secret is not required to take "heroic measures to preserve its secrecy" but must "not fail to take all proper and reasonable steps to keep it secret." *USM v. Marson Fastener*, 393 N.E.2d 895, 902 (Mass. 1979).

Although Appellee's "Music Man" project does fall under the "technical data" portion of Marshall's Trade Secrets Act, it ultimately fails because it does not satisfy the two-part test of the statute. The very short time – a mere three months – between the alleged misappropriation and the announcement of a competitor's product indicates likelihood that the technology was generally known in the industry. *See, e.g., Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 899 (Minn. 1983) (reasoning "reverse engineering time is certainly a factor in determining whether information is readily ascertainable"). Further, Appellee's attempts to keep "Music Man" secret were not reasonable under the circumstances. Because Appellee can meet neither prong of the test, Appellee did not have a trade secret to misappropriate and Marion cannot be liable.

A. Appellee Did Not Sufficiently Notify Marion of a Protectable Trade Secret Because He Failed to Timely Procure a Non-disclosure Agreement

Appellee cannot possess a protectable trade secret unless he took reasonable measures to protect its secrecy. A lack of reasonable measures to protect secrecy ultimately led to a denial of protection in *J.T. Healy & Sons, Inc. v. James A. Murphy & Sons, Inc.*. 260 N.E.2d 723, 729-31 (Mass. 1970). The *J.T. Healy* court held that there was no protectable trade secret because the plaintiff failed to implement any affirmative procedures alerting employees of a trade secret. *Id.* The plaintiff's employees were not informed that any of the manufacturing processes were considered secret, were not required to sign non-disclosure agreements, were not partitioned into sections, and could plainly see operation of the processes the plaintiffs were seeking to protect. *J.T. Healey*, 260 N.E.2d at 730. Similarly, in *Alagold v. Freeman*, the court denied Alagold trade secret protection because there was no evidence that their proprietary information was marked "confidential" or that Alagold communicated the confidential nature of the information to its employees. 20 F. Supp. 2d 1305, 1315-16 (M.D. Ala. 1998). The court held that "it

cannot be said that Alagold undertook reasonable efforts under the circumstances to maintain the secrecy of its information." *Id.*

Lack of a confidentiality agreement, specifically, can render information ineligible for trade secret protection. In *Pressure Science, Inc. v. Kramer*, the district court denied trade secret protection where the plaintiff only required some of his employees to sign non-disclosure agreements and failed to set forth a written policy advising employees that the company considered its information confidential. 413 F. Supp. 618, 627 (D. Conn. 1976). An Indiana court also found that a plaintiff did not have a protectable trade secret where the plaintiff "did not ever tell [the defendant] that it considered the information confidential, let alone obtain a confidentiality agreement . . . ." *Zemco Mfg., Inc. v. Navistar Int'l Transp. Corp.*, 759 N.E.2d 239, 247, 253 (Ind. Ct. App. 2001). The *Alagold* court also cited the lack of a confidentiality agreement as a factor in its decision to deny trade secret protection. 20 F. Supp. 2d at 1315-16.

The fact that Appellee did not require Marion to sign a non-disclosure agreement for six months shows that his measures of protection were not reasonable under the circumstances. This case is similar to *J.T. Healy & Sons* because Appellee gave no notice that Marion was working on a project considered a protectable secret until six months after she started working. Until that point, Appellee failed to instruct Marion that the program she was working on was considered confidential and also failed to procure a non-disclosure agreement, which would have alerted Marion that "Music Man" was a trade secret. Even though Appellee did attempt to separate his employees so no more than three of them were at the same physical location, unlike in *J.T. Healy & Sons*, there is no evidence that the employees could not share information once their RFID chips allowed them access to their separate work stations. (R. at 2.)

Although Marion did eventually sign the non-disclosure agreement, after Appellee realized his mistake, Appellee offered no additional compensation for the agreement. Therefore, Marion is not bound to the agreement. A legally unenforceable confidentiality agreement is as useless a protection as none at all. Regardless, Marion worked for Appellee and ECC for six months without an agreement. As in *Alagold*, *Zemco*, and *Pressure Science*, this lack of a non-disclosure agreement is dispositive. Appellee utterly failed to apprise Marion that the information she was working on was confidential or obtain a non-disclosure agreement, rendering the information not "secret" and thus ineligible for trade secret protection.

B. Appellee's RFID Chips Were Not Reasonable Measures Under the Circumstances Because They Did Not Adequately Protect Information

Appellee's RFID chips were not a reasonable measure of protection to guarantee trade secret status for his "Music Man" project. Information is only a trade secret if reasonable measures are implemented to protect its secrecy. *Gillis Associated Indus., Inc. v. Cari-All, Inc.*, 564 N.E.2d 881, 884 (Ill. App. Ct. 1990). The *Gillis* court held that maintaining files on a computer to which only three key employees had access did not suffice as affirmative measures to keep the information secret because there was no evidence of internal or external physical security, of confidentiality agreements with employees, or of protection of hard copies of the files. *Id.* at 884-86. However, in *Surgidev Corp. v. Eye Tech., Inc.*, the court stated "[o]nly reasonable efforts, not all conceivable efforts, are required to protect the confidentiality of putative trade secrets." *Surgidev Corp. v. Eye Tech., Inc.*, 828 F.2d 452, 455 (8th Cir. 1987). What is adequate under the facts of one case may be considered inadequate under the facts of another. *Elm City Cheese Co., Inc. v. Federico*, 752 A.2d 1037, 1050 (Conn. 1999). In *Com-Share, Inc. v. Computer Complex, Inc.*, for instance, a Michigan district court held that the plaintiff utilized utmost care in protecting the secrecy of its software by utilizing built-in passwords and marking each page with the word "confidential." 338 F. Supp. 1229, 1234-35 (E.D. Mich. 1971).

In order to qualify for protection, Appellee must have undertaken more affirmative steps to protect his trade secret. Unlike the plaintiff in *Com-Share*, Appellee in this case failed to mark any of the pages of information "confidential" and also failed to build passwords into the system themselves, despite his anxiety that a competitor would learn of his project and beat him to the market. Instead of limited access to information, Appellee utilized RFID chips which sent out their access codes to anyone nearby and did not limit access to confidential information; the chips constantly broadcast the necessary serial numbers into the public sphere. In addition, no other security measures prohibited someone from accessing the information on computers previously activated by an authorized employee.

Although Appellee segregated the physical locations of his employees, segregation alone is not a reasonable measure under these circumstances. While *Surgidev* suggests that not "all conceivable efforts" must be undertaken, measures which are easily defeated and incomplete cannot possibly suffice for trade secret protection. *Com-Share* and *Gillis* both provide that multiple levels of effective protection should be used. Appellee's RFID measures break down to exactly those found insufficient in *Gillis* – keeping the files on a computer to which access is supposedly

restricted. Like the plaintiff in *Gillis*, Appellee failed to place the information under "lock and key" or even ensure that the computers were truly limited to those persons with authorized access. Therefore, the use of RFID chips is not a reasonable measure of protection and the "Music Man" files are not protectable trade secrets.

As a whole, Appellee has not taken the requisite steps necessary to protect "Music Man" and qualify for trade secret protection. Appellee did not alert employees of the confidential nature of his project, he did not have Marion sign a timely non-disclosure agreement with adequate consideration, he did not segregate the information adequately, and he did not keep the secret documents under lock or encode them in a way only he could decipher. By transmitting serial numbers into the public domain and not otherwise limiting access to the project, Appellee failed to take reasonable efforts under the circumstances to ensure trade secret protection. For these reasons, Marion respectfully requests this Court reverse the Court of Appeals and hold that Appellee possessed no trade secret to misappropriate.

CONCLUSION

Marion did not intrude upon Appellee's seclusion because there was no unauthorized, offensive intrusion, or resulting anguish and suffering. Marion also did not unlawfully disclose private facts by revealing Appellee's Bash Abortion Now membership. The Anti-Circumvention Act does not apply to Marion's reverse engineering of the RFID encryption program. Finally, Appellee did not have a protectable trade secret because he failed to use reasonable measures to maintain the information's secrecy. For the foregoing reasons, Marion respectfully requests that this Court reverse the decision of the Court of Appeals.

Respectfully Submitted,

ATTORNEYS FOR PETIONER

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the above and foregoing Brief for Appellant was mailed by first class certified mail, return receipt requested, to all counsel of record on this 30th day of September, 2005.

BRIEF FOR THE RESPONDENT

No. 2005-CV-0237

IN THE
SUPREME COURT OF MARSHALL
FALL TERM 2005

BESS MARION,
PETITIONER,

V.

EDDIE CAFKA AND ECC ENTERPRISES, INC.,
RESPONDENT.

ON GRANT OF LEAVE OF APPEAL
TO THE DISTRICT COURT OF APPEALS OF
THE STATE OF MARSHALL

BRIEF FOR RESPONDENT

CHERISH M. KELLER
ELAINE WYDER-HARSHMAN
ATTORNEYS FOR RESPONDENTS

QUESTIONS PRESENTED

I. Whether the Defendant intruded upon Mr. Cafka's seclusion when she scanned Mr. Cafka's body to access data on the RFID chip he had implanted in his arm.

II. Whether the Defendant publicly disclosed private facts about Mr. Cafka when she posted on the Internet facts which Mr. Cafka had taken steps to keep private that concerned his involvement in an anti-abortion group.

III. Whether Mr. Cafka's efforts to protect the Music Man data were sufficient to preserve his rights under Marshall's trade secrets statute, where his measures included requiring employees to enter into confidentiality agreements, limiting employees' contact with one another, physically separating employee work areas, allowing only limited access to information, and implementing an RFID-based security system.

IV. Whether Defendant, in the course of discovering data related to Mr. Cafka's Music Man project, violated Marshall's Anti-Circumvention Statute by breaking the cryptographic algorithm used to generate serial numbers integral to Mr. Cafka's RFID-based security system.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES

UNITED STATES COURT OF APPEALS CASES

UNITED STATES DISTRICT COURTS

STATE CASES

STATUTES

STATE RULES

OTHER AUTHORITIES

ARTICLES

OPINIONS BELOW

The Order of the Marshall Circuit Court is unpublished. The Opinion and Order of the Third District Court of Appeals of the State of Marshall (June 30, 2005) is also unpublished; it can be found in the Record on pages 1-8.

STATUTES INVOLVED

Four statutes are involved in this case, the pertinent parts of which may be found in the Appendix. The Marshall statute governing intrusion upon seclusion is Marshall Revised Code § 439(A) and is set out on A-1. The Marshall statute governing public disclosure of private facts is Marshall Revised Code § 562(B) and is on A-1. The Marshall Anti-Circumvention Act is Marshall Revised Code § 1492 and is on A-1. Finally, the Marshall Uniform Trade Secrets Act is Marshall Revised Code § 1947 and is on A-2.

STATEMENT OF THE CASE

FACTS

Mr. Eddie Cafka started his own business in Marshall, ECC Enterprises, Inc., to design and build the next generation of computer technology. (R. at 1.) An inventor as well as a businessperson, Mr. Cafka aimed to design computer technology that could project images into users' brains instead of onto computer screens. (R. at 1-2.) He code-named his project "Music Man." (R. at 2.)

Fearing a competitor would steal his project, Mr. Cafka took extensive measures to keep the Music Man project a secret. (R. at 2.) He divided his employees into groups of three or fewer. (R. at 2.) He had those groups of employees work in different facilities. (R. at 2.) He had his employees work on different parts of the Music Man project so no employee knew all of the details. (R. at 2.) He did not even allow his employees to know where other employees were or how to contact them. (R. at 2.) Further, he visited the facilities personally to gather his employees' research because he did not trust the security of Internet transmission. (R. at 2.) Moreover, he required his employees to sign non-disclosure agreements when they were hired. (R. at 2.) The agreements were intended to protect confidential and trade secret information, including "concepts, source code, computer programs, business plans, formulas and all other proprietary and secret materials." (R. at 2; Exh. A.)

To further protect his work, Mr. Cafka implemented a Radio Frequency Identification (RFID) based security system. (R. at 2.) The system consists of scanners (described as "transponders" by the court below) linked to security mechanisms and microchips. (R. at 2.) Mr. Cafka im-

planted a chip in his right arm, and he required his employees to do the same. (R. at 2.) The scanner transmits a 16-bit code by radio signal, which activates any chip within a few meters of the scanner. (R. at 2.) In response, the chips use an encrypted algorithm to generate a custom 64-bit serial number and transmit it back to the scanner. (R. at 2.) The RFID-based security system was designed to allow only designated employees to access certain office doors and certain company computers. (R. at 2.) Only Mr. Cafka's chip allowed access to all offices and computers. (R. at 2.)

The Defendant, Bess Marion (Marion), began working for Mr. Cafka in January of 2002. (R. at 2; Exh. A.) She did not sign the non-disclosure agreement when she started, but when Mr. Cafka realized that in July, 2002, he had her sign it immediately. (R. at 2.) Professionally, Marion was an excellent programmer, and she worked in the River City facility in an office adjacent to Mr. Cafka's office. (R. at 2.)

However, Marion harbored negative memories of Mr. Cafka from high school, resented his success, and believed she knew more about technology than he did. (R. at 2.) She took the job with ulterior motives: she wanted to learn about the Music Man project so she could release a similar product before Mr. Cafka could. (R. at 2.)

To that end, she experimented with the RFID-based security system technology in the ECC offices. (R. at 3.) Using a scanner she built and the RFID chip in her arm, she reverse engineered the cryptographic algorithm in the chip. (R. at 3.) She then brought her scanner to work and repeatedly scanned Mr. Cafka's chip as he passed by or entered her office. (R. at 3.)

With this data, she reverse engineered Mr. Cafka's chip and built a clone. (R. at 3.) Using this cloned chip one evening, she returned to the office complex, entered Mr. Cafka's office, accessed his computer, and downloaded all of his data files. (R. at 3.) These files contained data on all of the Music Man research. (R. at 3.)

In addition, the data contained a file concerning Mr. Cafka's personal life. (R. at 3.) Among Mr. Cafka's other files, Marion found a file that contained the membership list for the anti-abortion group Bash Abortion Now (BAN). (R. at 3.) The list identified Mr. Cafka as the "Grand Nowest" of the group. (R. at 3.) BAN had been linked in the news to anti-abortion activities including finding, following, and threatening doctors who performed abortions. (R. at 3.) Marion has conceded for the purposes of this litigation that soon after she obtained this information, she posted or caused it to be posted on various Internet web logs. (R. at 3, 5.) These postings caused Mr. Cafka to lose funding for the Music Man project. (R. at 3.) They also caused Mr. Cafka great embarrassment. (R. at 3.)

Two weeks after the information appeared on the Internet, Marion quit. (R. at 3.) Shortly thereafter, she began working at a competing company, Softer Microns. (R. at 3.) Three months later, Softer Microns announced that it was developing a product that did exactly what Music Man aimed to do: project images onto users' brains via brainwaves. (R. at 3.)

Trial Proceedings

Mr. Cafka filed suit against Marion on four counts: intrusion upon seclusion for the unauthorized scanning of his RFID chip, public disclosure of private facts for posting his association with BAN on the Internet, misappropriation of trade secrets, and a violation of Marshall's anti-circumvention act. (R. at 3.) In response, Marion filed a motion for summary judgment which the Potter County Circuit Court granted. (R. at 3-4.)

Appellate Proceedings

The District Court of Appeals of Marshall reversed the trial court's grant of summary judgment to Marion. (R. at 4.) It found that scanning a person's body to access an implanted chip was an intentional intrusion and that such an intrusion would be highly offensive to a reasonable person. (R. at 4.) While Mr. Cafka consented to be scanned in some settings, the court acknowledged, he did not consent to be scanned by Marion. (R. at 4.) It found the trial court erred in granting summary judgment on this count. (R. at 4.)

The appellate court also found that the trial court erred in granting summary judgment against Mr. Cafka on his claim for public disclosure of private facts. (R. at 6.) The court acknowledged that Mr. Cafka kept his association with BAN secret and that it was made public only by the Internet blog postings. (R. at 5.) It concluded that while the posting was a publication, it was not protected by the First Amendment. (R. at 5.) Noting that disclosure of a membership list violates the constitutionally-protected freedom of association, the court concluded that "there can be no dispute" that the disclosure would be offensive to a reasonable person and is not of legitimate public concern. (R. at 5.)

Addressing the anti-circumvention claim, the court found that the trial court erred in granting Marion summary judgment on this count as well. (R. at 7.) The court noted that the Marshall statute required that where data is protected by a form of technology and that technology is decrypted or otherwise avoided, there is a violation. (R. at 7.) Because the RFID chip was protected by an encryption program, and Marion gained access to it by copying the encryption, decrypting it, and accessing the data, Mr. Cafka stated a claim. (R. at 7.)

Finally, the appellate court found that the trial court erred in granting summary judgment and dismissing Mr. Cafka's complaint as to misappropriation of trade secrets. (R. at 7.) The court noted that because Marion received no compensation for signing the non-disclosure agreement, the agreement could not be enforced. (R. at 7.) However, the court also noted that the agreements were evidence that Mr. Cafka took reasonable measures to protect his trade secrets. (R. at 8.) Acknowledging that he took other steps to keep his trade secrets confidential, including separating his workers and their assignments, segregating the computers, and requiring his employees to implant RFID chips in their bodies, the court concluded that he took "reasonable measures" to keep his trade secrets confidential and is thus protected by the Marshall trade secret statute. (R. at 8.)

This Court issued its Order granting leave to appeal on July 15, 2005, and the order can be found on page nine of the Record.

SUMMARY OF ARGUMENT

I. INTRUSION UPON SECLUSION

The Defendant, Bess Marion, intruded upon Mr. Cafka's seclusion when she scanned his RFID chip without authorization. To prove intrusion upon seclusion, there must be an unauthorized intrusion or prying that would be highly offensive to a reasonable person into a matter in which the person had a legitimate expectation of privacy.

Marion's intrusion was unauthorized, because while Mr. Cafka consented to be scanned by his own transponders in certain locations, he did not consent to be scanned by Marion or any other employee in any other location. Marion's intrusion would be highly offensive to a reasonable person as well, in light of her ill motives and the type of sensitive information she gained. She did not have a newsworthy purpose, and she gained personal information that provided her access to data and space to which she was not otherwise entitled. Further, Mr. Cafka had a legitimate expectation of privacy in his RFID chip: the generally recognized, reasonable expectation of privacy in a person's own body. The extensive steps he took to keep the data on his chip private reflect his subjective expectation of privacy and demonstrate that his expectation was reasonable.

Lastly, although the Marshall statute does not identify anguish and suffering as a separate element, Mr. Cafka suffered from Marion's actions. He suffered a loss of autonomy when Marion took away from him the decision to share personal information with her. The ramifications of her action also demonstrate that Mr. Cafka suffered—he felt great embarrassment and lost funding for the Music Man project.

II. PUBLIC DISCLOSURE OF PRIVATE FACTS

When Marion posted facts about Mr. Cafka's association with BAN, she publicly disclosed a private, non-newsworthy fact. The three elements of public disclosure of private facts are that a private fact about the plaintiff was publicized, the matter publicized would be highly offensive to a reasonable person, and the matter is not of legitimate public concern. As today's bloggers are publishers—indeed, modern-day pamphleteers—the blog postings about Mr. Cafka's association in BAN thus constitute publication. First, his association was a private fact because it was not part of the public record and Mr. Cafka took multiple steps to keep it private, including keeping the fact hidden in a file that only he could legitimately access.

Second, Mr. Cafka's involvement with BAN would be highly offensive to a reasonable person. It was not an ordinary activity and was more than a nuisance, causing him great embarrassment and loss of funding. And if it cannot be found offensive as a matter of law, it is an inquiry for a jury.

Third, Mr. Cafka's personal association with BAN is not a matter of legitimate public concern, or "newsworthy." While BAN's activities may be newsworthy, Mr. Cafka's personal association with BAN is not. There is no social value in Mr. Cafka's personal involvement with BAN, as it does not relate to or negatively affect his professional life. He kept his association very private, and thus the publication was deeply intrusive. Further, although Mr. Cafka is a well-known inventor and businessperson, he is not automatically a public figure. He did not run for public office, and he did not make any related facts public. The question of how much he opened his life to public scrutiny is one for a jury.

III. MISAPPROPRIATION OF TRADE SECRETS

Because Mr. Cafka took reasonable measures to preserve his trade secrets, he is entitled to bring a cause of action against Marion for misappropriation of trade secrets under Marshall's Trade Secret Act. To qualify for protection, the information must be the subject of reasonable efforts, under the circumstances, to maintain its secrecy and confidentiality. Mr. Cafka took measures to protect his information which exceeded this standard.

Simple measures can suffice to protect a trade secret. For example, securing the work area, restricting the disclosure of information, and entering into confidentiality agreements may be sufficient, depending on the circumstances. Mr. Cafka took relatively elaborate measures, including installing an RFID-based security system, securing work areas and computers, segregating work areas and employees, and requiring all his

employees to sign confidentiality agreements. These efforts meet and exceed the standard.

Given the confidential nature of the relationship between Marion and her employer, the security measures taken by Mr. Cafka were reasonable. Even if Marion's confidentiality agreement is invalid due to lack of consideration, Marion and other employees are bound by the duty of confidentiality which may be implied in the employer-employee relationship.

Marion's breach of confidentiality and her successful theft of Mr. Cafka's secrets do not undermine the objective reasonableness of his efforts. Trade secret law is designed to reward innovators and punish those who acquire a competitive advantage by improper means. Accordingly, a trade secret holder is not required to take extraordinary measures. Rather, reasonableness should be judged under the circumstances of a normal business environment.

Mr. Cafka took extraordinary measures to protect the Music Man project. If there are any outstanding issues of material fact pertaining to the implementation of those measures, those issues should be settled at trial. For these reasons, summary judgment is inappropriate.

IV. Violation of the Anti-Circumvention Act

Marion also violated the Anti-Circumvention Act by reverse engineering a cryptographic algorithm used to generate serial numbers as part of the RFID-based security system. The Anti-Circumvention Act creates a cause of action for circumventing a technological measure that effectively controls access to data. Marshall Rev. Code § 1492. The Act defines "circumvention of a technological measure" as "to decrypt an encrypted work, or otherwise to avoid, bypass[,] remove, deactivate a technological measure[,] without the authority of the owner of the underlying data." *Id.* Marion violated this provision when she reverse engineered the cryptographic algorithm and used that information build an unauthorized clone of Mr. Cafka's chip. She effectively broke the security system by replacing one part with an unauthorized component.

Marion could be liable under the Anti-Circumvention Act regardless of whether Mr. Cafka protected his interest in the underlying information. Unlike the Digital Millennium Copyright Act, the Anti-Circumvention Act creates a cause of action for circumvention alone. Because Marion could be subject to liability for circumvention of a technological measure, summary judgment is not appropriate.

ARGUMENT

In 1890, Warren and Brandeis worried that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in

the closet shall be proclaimed from the house-tops.'" Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890). These fears are still pertinent today. Here, Mr. Cafka suffered an intrusion upon his seclusion when Marion scanned the microchip that he had implanted in his arm as part of his security system. *See* Marshall Rev. Code §439(A). He suffered public disclosure of private facts when she posted facts about his association with an anti-abortion group on the latest form of publication, Internet web logs. *See* Marshall Rev. Code § 562(B). Despite the multiple precautions that Mr. Cafka took to safeguard his right "to be let alone," *see The Right to Privacy*, 4 Harv. L. Rev. at 195, Marion violated it.

The same actions that violated Mr. Cafka's right to privacy also violated two other Marshall statutes, the Trade Secret Act, *see* Marshall Rev. Code § 1947, and the Anti-Circumvention Act, *see* Marshall Rev. Code § 1492. The Trade Secret Act protects the trade secret holder against disclosure or unauthorized use, *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475-76 (1974), provided that the protected information is "the subject of efforts that are reasonable under the circumstances to maintain its secrecy and confidentiality." Marshall Rev. Code § 1947. Because Mr. Cafka took extraordinary measures to ensure the secrecy and confidentiality of his Music Man project, he is entitled to protections of the Trade Secret Act. The Anti-Circumvention Act provides that "no person shall circumvent a technological measure that effectively controls access to data." Marshall Rev. Code § 1492. Yet Marion did exactly that when she broke a cryptographic algorithm and used that information to circumvent the RFID-based security system.

This Court reviews grants of summary judgment de novo and uses the same legal standard as the trial court to determine whether summary judgment was proper. *See Celotex v. Catrett*, 477 U.S. 317, 322 (1986). Summary judgment is proper only if evidence in the record demonstrates that there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law. Marshall R. Civ. P. 56(c)[1]. An issue is material only where the presence or absence of a legal element of the claim, identified by the applicable substantive law, might affect the outcome of the suit. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986). In determining that there are no genuine issues of material fact, a court must construe all facts in the light most favorable to the party opposing the motion and draw all justifiable inferences in favor of that party. *See id.* at 248. Because Marion moved for summary judgment below, this Court must construe all facts in the light most favorable to Mr. Cafka.

1. Marshall Rule of Civil Procedure 56(c) is identical to Federal Rule of Civil Procedure 56(c).

I. THE UNAUTHORIZED SCANNING OF MR. CAFKA'S RFID CHIP WAS AN INTRUSION UPON SECLUSION BECAUSE IT WAS HIGHLY OFFENSIVE, PARTICULARLY IN LIGHT OF DEFENDANT'S METHOD AND MOTIVE; IT WAS DONE IN SPITE OF MR. CAFKA'S LEGITIMATE AND REASONABLE EXPECTATION OF PRIVACY; AND IT CAUSED HIM SUFFERING AND ANGUISH

Defendant Bess Marion (Marion) intruded upon Mr. Eddie Cafka's seclusion when she scanned his RFID chip without authorization. Following the *Restatement (Second) of Torts*, the Marshall statute for intrusion upon seclusion states:

> 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.

Marshall Rev. Code § 439(A); *see Restatement (Second) of Torts* § 652B (1977)

There is no case law directly on point in Marshall that identifies the required elements. (R. at 4.) However, courts that have adopted the *Restatement* definition typically identify that there must be (1) an unauthorized intrusion or prying (2) that would be offensive to a reasonable person (3) into a matter in which the person has a legitimate expectation of privacy or that is a private matter. *See, e.g., Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 876 (8th Cir. 2000); *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1067 (Colo. App. Ct. 1998). Further, some courts have articulated a fourth requirement that the intrusion must cause anguish and suffering. *See, e.g., Melvin v. Burling*, 490 N.E.2d 1011, 1013-14 (Ill. App. Ct. 1986).

Invasions need not be physical trespasses and can be perpetrated with a variety of media, from taking photographs to viewing with one's own eyes to videotaping. *See, e.g., Daily Times Democrat v. Graham*, 162 So.2d 474, 476-78 (Ala. 1964) (photographing woman whose dress blew upwards from a jet of wind); *Benitez v. KFC Nat'l Mgmt. Co.*, 714 N.E.2d 1002, 1033 (Ill. App. Ct. 1999) (viewing through peephole in women's bathroom); *Lewis v. LeGrow*, 670 N.W.2d 675, 688-89 (Mich. App. Ct. 2003) (videotaping sexual encounters without consent). Even in *Tomblin v. Treviño*, where the court noted that intrusions are often physical, the court recognized a cause of action for an invasion of privacy over the forced disclosure of a driver's social security number to a police officer. No. SA01CA1160-OG, 2002 WL 32857194, at *1, 4 (W.D. Tex. June 17, 2002). The focus must not be the medium, but the intrusion—as one court pointed out, "[i]s rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cab-

inet . . . ? Not really." *White v. White*, 781 A.2d 85, 92 (N.J. Super. Ct. 2001).

Here, Mr. Cafka did not consent to Marion scanning the RFID chip he had implanted in his arm. That unauthorized scanning would be highly offensive to a reasonable person, and Mr. Cafka had a reasonable expectation of privacy in the information stored on the chip. In addition, he experienced anguish and suffering as a result of Marion's intrusion.

A. Because Mr. Cafka did not consent to be scanned by his employees or in a location where he had not installed a scanner, the scanning was an unauthorized intrusion

Marion intruded when she repeatedly scanned Mr. Cafka's RFID chip without his consent. An intrusion takes place when the actor "believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *Fletcher*, 220 F.3d at 876. In *Fletcher*, an employer called an employee's doctor to verify the employee's health condition after hearing that she had told others that she had a staph infection. *Id.* at 874. In lieu of a general medical authorization form, the employer gave the doctor's office the employee's worker's compensation form. *Id.* The court concluded that the use of that form was inapt and that the facts left "little doubt" that the employer intruded. *Id.* at 876.

Any purported consent must be given freely and voluntarily. *Wal-Mart Stores, Inc. v. Lee*, 74 S.W.3d 634, 647 (Ark. 2002). In cases where consent is contested, the degree of consent given can determine whether there was an intrusion. *See id.* at 645-46. In *Wal-Mart Stores*, Wal-Mart management suspected one of its employees of stealing. *Id.* at 640. The jury accepted the employee's testimony that he had only given limited consent to search for the fishing equipment his supervisors had mentioned and not broad consent to search his entire residence. *Id.* at 645-46. The court noted that substantial evidence supported the jury's conclusions that the employee did not freely or tacitly consent, and thus his consent was not valid. *Id.* at 647-48.

Further, consent must be given for the activity at issue, particularly if it exceeds the scope of previously-given consent. In *High-Tech Institute, Inc.*, the plaintiff consented to his school testing a blood sample for rubella. 972 P.2d at 1064. Without his knowledge, the school also had his blood tested for human immunodeficiency virus (HIV). *Id.* Commenting that a general privacy interest in a person's own body has been recognized along with an interest in a person's own health, *id.* at 1068, the court concluded that the unauthorized HIV test was an invasion of the plaintiff's privacy, *id.* at 1071. In a similar vein, the court in *Lewis* recog-

nized that while a person allows a sexual partner access to his or her body during an intimate encounter, it is a question of fact whether such consent includes the consent to be videotaped during the encounter. 670 N.W.2d at 688-89.

Marion's actions went far beyond the activities to which Mr. Cafka consented. While he implicitly consented to having his RFID chip scanned by the scanners he installed at the locations he installed them, it is a distinctly separate question whether he consented to having his RFID chip scanned by any other device, in any other location, or by any other person. Like the accused employee in *Wal-Mart Stores*, Mr. Cafka consented to one form of intrusion—being scanned by his own equipment. But just as in *Wal-Mart Stores*, here it is also a question of fact for a jury whether he consented implicitly or at all to repeatedly being scanned by Marion. Like the aggrieved parties in *Lewis* and *High-Tech Institute*, Mr. Cafka implicitly authorized being scanned for one purpose only—to gain access to his company facilities and computers. Marion has not alleged that she believed or was substantially certain that she had permission to scan his chip. She has not presented any evidence that Mr. Cafka consented to being scanned by her.

B. The scanning would be highly offensive or objectionable to a reasonable person in light of Marion's motive and the type of information she acquired

Marion's intrusion would be highly offensive to a reasonable person. To determine whether an intrusion would be highly offensive, courts often consider the setting into which the intruder intrudes; the context, conduct, and circumstances surrounding the intrusion; the degree of the intrusion; the intruder's motives and objectives; and the expectations of those whose privacy is intruded upon. *Wolfson v. Lewis*, 924 F. Supp. 1413, 1421 (E.D. Pa. 1996) (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 648 (Cal. 1994)).

Activities may be highly offensive due to the surrounding circumstances. *Wolfson*, 924 F. Supp. at 1432. In *Wolfson*, two reporters from *Inside Edition* repeatedly followed and videotaped a family in spite of their knowledge of the family's concerns about security and threats. *Id.* at 1415, 1431. Calling the defendants' activities "a course of conduct apparently designed to hound, harass, intimidate and frighten" and concluding that a reasonable jury would likely think that the defendants' actions advanced no newsworthy goal, the court concluded that the family stated a cause of action. *Id.* at 1432-33.

Even an acceptable motive can lead to an intrusion upon seclusion. *See Shulman v. Group W. Prod., Inc.*, 955 P.2d 469, 494 (Cal. 1998). In *Shulman*, a television news cameraman rode with two seriously injured

patients in an air ambulance and recorded communications between one of the patients and the flight nurse. *Id.* Though the purpose was not malicious and the story was potentially newsworthy, the court concluded that the conduct intercepted what would normally have been a private conversation between a patient and a nurse and constituted a highly offensive disregard for the patient's privacy. *Id.*

Moreover, the type of information gained is important. In *High-Tech Institute*, the court noted that while unauthorized testing of the plaintiff's blood for HIV may not have been offensive alone, because the information gained was highly personal, medical information, it was more likely highly offensive. 972 P.2d at 1069-70. Recognizing the serious consequences of a diagnosis of HIV, a highly sensitive diagnosis which may bring a strong social stigma, the court concluded that the HIV test was an unreasonable, offensive intrusion. *Id.* at 1070-71.

Being scanned was not offensive to Mr. Cafka when done by his own scanners and with his consent. However, the manner of the scanning performed by Marion is akin to the videotaping done by the reporters in *Wolfson*—with ill intentions, Marion repeatedly scanned Mr. Cafka without his consent for a non-newsworthy purpose. Marion's motive is also suspect. She was not gathering news. She was not in any way aiding Mr. Cafka. Ultimately, she used the information she gained by scanning him to enter his office and access his data files. (R. at 3.) If the news-gathering motive in *Shulman* failed to keep the reporters' behavior from being judged offensive, then Marion's illicit purpose is likely be found highly offensive as well.

The information Marion gained was highly personal. The data on Mr. Cafka's RFID chip provided access to Mr. Cafka's personal office and computer files, space and information to which Marion was not otherwise entitled access. (R. at 2-3.) This was highly personal space and information, like the *High-Tech Institute* plaintiff's HIV status was highly personal information. While access to Mr. Cafka's office and files would not directly cause a similar social stigma, it was a similar intrusion into highly personal matters.

C. Mr. Cafka had a legitimate expectation of privacy in the data in his RFID chip that was both reflected in the steps he took to protect the data and objectively reasonable

Mr. Cafka had a legitimate expectation of privacy in his RFID chip. A legitimate expectation of privacy is the "touchstone" of intrusion into seclusion, *Wal-Mart Stores*, 74 S.W.3d at 644, and that expectation must be subjectively held and objectively reasonable, *Med. Lab. Mgmt. Consultants v. Am. Broad. Co.*, 306 F.3d 806, 812-13 (9th Cir. 2002).

A subjective expectation of privacy can be demonstrated by behavior consistent with having an actual expectation of privacy. *See id.* at 813. The court in *Medical Laboratory Management Consultants* found that the plaintiff's conduct, allowing allowed several reporters who were posing as potential corporate customers to tour the premises of his lab and meet with him in a private conference room, was not consistent with an expectation of privacy in those areas. *Id.* at 810, 813-14. On the other hand, stopping one of the reporters from entering his office reflected an expectation of privacy in that space. *Id.* at 813-14.

The expectation of privacy must have been objectively reasonable. *Id.* at 812-13. In *Y.G. v. Jewish Hospital of St. Louis*, the court noted that the plaintiffs had been assured that there would be no publicity surrounding an event for couples who used *in vitro* fertilization, twice refused interviews or requests to be filmed, and made "every reasonable effort" to avoid being filmed. 795 S.W.2d 488, 501 (Mo. App. Ct. 1990). The court concluded the plaintiffs stated a claim after a news broadcast concerning the event pictured them. *Id.* In contrast, when a neighbor aimed a surveillance camera at the plaintiffs' garage, driveway, side-door area, and backyard, the plaintiffs could not state a claim because those were areas that a passerby could readily observe. *Schiller v. Mitchell*, 828 N.E.2d 323, 329 (Ill. App. Ct. 2005). The plaintiffs could have no reasonable expectation of privacy in these areas. *See id.*

Certain matters are generally recognized as private, such as the privacy interest in one's own body. *High-Tech Institute*, 972 P.2d at 1068. In addition, after sharing access to certain matters with others, a plaintiff has no reasonable expectation of privacy from those individuals. *See White*, 781 A.2d at 92. As the court noted in *White*, a plaintiff who stores his email on a family computer had no reasonable expectation of privacy in that email. *Id.* Further, there is generally less of a reasonable expectation of in the workplace than at home, as employers often need to enter an employee's work area for "legitimate work-related reasons wholly unrelated to illegal conduct." *O'Connor v. Ortega*, 480 U.S. 709, 720-22, 724 (1987).

Mr. Cafka had a reasonable expectation of privacy in the data stored in the RFID chip that he implanted in his arm, consistent with the expectation or privacy that all individuals have in their bodies. He did not allow access to the data on his RFID chip to others and then complain, like the lab owner in *Medical Laboratory Management Consultants* did. Instead, just as the plaintiffs in *Y.G.* took multiple steps to remain free from publicity about their use of *in vitro* fertilization, Mr. Cafka took extensive measures to keep his RFID data secret. His RFID-based security system utilized a cryptographic algorithm. (R. at 2.) He implanted a RFID chip in his body and required that his employees do the same, instead of simply carrying cards with RFID chips. (R. at 2.) He did not

share access to the data with anyone, unlike the plaintiff in *White* who kept his email on the family's shared computer; instead, his RFID chip was the only one that allowed access to all areas and computers. (R. at 2.) No employee, let alone casual passerby, had access to the data on Mr. Cafka's chip.

Further, Mr. Cafka was not an employee at ECC Enterprises—he was the employer, and his employees had no legitimate work purpose in accessing the data contained in his RFID chip. Even if Mr. Cafka had been an employee, Marion did not access his chip for any legitimate work-related reason that was unrelated to illegal conduct. Instead, she scanned his chip to acquire his personal data with no legitimate, work-related reason.

D. Mr. Cafka experienced anguish and suffering from the privacy intrusion alone, and, in addition, from the resulting financial loss

Mr. Cafka experienced anguish and suffering as the result of Marion's intrusion. Neither the *Restatement (Second) of Torts* § 652B nor Marshall Revised Code § 439(A) mentions that anguish and suffering is an element of intrusion upon seclusion, but a few courts have read into it such a requirement, *see, e.g.*, *Melvin*, 490 N.E.2d at 1014. Yet regardless of whether it is a distinct element, victims of a tortuous intrusion have been harmed by the violation of their privacy. *See High-Tech Institute*, 972 P.2d at 1070.

The loss of autonomy was a harm to Mr. Cafka. Privacy has been defined as "an autonomy or control over the intimacies of personal identity," and for this tort, the intrusion at issue is an interference with that autonomy. *Id.* In *High-Tech Institute*, the court noted that damages for intrusion upon seclusion may include general damages for harm to the person's privacy interest. *Id.* There, the plaintiff's right to personally decide whether and when to have a HIV test was violated when his school ordered a HIV test on blood he had submitted for a rubella test. *Id.* at 1071. Here, Marion made a decision for Mr. Cafka about whether to share with her the private data he carried on his RFID chip. Just as the school in *High-Tech Institute* caused harm when it violated its student's autonomy, Marion caused harm when she violated Mr. Cafka's autonomy.

Further, Mr. Cafka experienced anguish and suffering as a result of Marion's actions. Proof of suffering and anguish may be found in the effects of an intrusion. *See Melvin*, 490 N.E.2d at 1014. In *Melvin*, the plaintiffs stated a cause of action where the defendant ordered items by mail order to be delivered and billed to the plaintiffs without their authorization. *Id.* at 1012. The court concluded that the plaintiffs exper-

ienced anguish and suffering based on the difficulty they had returning the items and resolving the issue with creditors. *Id.* at 1014. Here, Marion repeatedly scanned Mr. Cafka, subsequently gained access to his personal files, later went to work for a company that soon-after announced the development of a product similar to Mr. Cafka's, and also published the fact of his association with an anti-abortion group, which resulted in a loss of funding. (R. at 3.) While the plaintiffs in *Melvin* were hassled by returning merchandise and dealing with creditors, Mr. Cafka's career was profoundly, negatively affected as the result of Marion's actions.

II. THE DEFENDANT COMMITTED THE TORT OF PUBLIC DISCLOSURE OF A PRIVATE FACT WHEN SHE POSTED ON THE INTERNET NON-NEWSWORTHY FACTS ABOUT MR. CAFKA'S ASSOCIATION WITH BAN THAT HE HAD TAKEN REASONABLE STEPS TO KEEP PRIVATE

Marion publicly disclosed private, non-newsworthy facts about Mr. Cafka when she posted facts about his association with BAN on web logs on the Internet. Publication of private facts is "concerned with the propriety of stripping away the veil of privacy with which we cover the embarrassing, the shameful, the tabooed, truths about us." *Haynes v. Alfred A. Knopf, Inc.*, 8 F.3d 1222, 1230 (7th Cir. 1993). However, these facts do not need to be shameful, as "[e]ven people who have nothing rationally to be ashamed of can be mortified by the publication of intimate details of their li[ves]." *Id.* at 1229.

The Marshall statute regarding public disclosure of private facts follows the Restatement (Second) of Torts § 652D. The statute states:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his/her privacy, if the matter publicized is of a kind that
>
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public.

Marshall Rev. Code § 562(B). While there is some variation, courts in jurisdictions that follow the *Restatement (Second) of Torts* require that (1) publicity be given (2) to private facts about the plaintiff, (3) that the matter publicized would be highly offensive to a reasonable person, and (4) that the matter was not of legitimate public concern. *See, e.g.*, *Shulman*, 955 P.2d at 478; *Doe v. TCF Bank Ill., FSB*, 707 N.E.2d 220, 221 (Ill. App. Ct. 1999).

A. Because the evolving view of publication encompasses postings on Internet web sites, Marion gave publicity to Mr. Cafka's association with BAN by posting it on web logs

Because bloggers are modern-day pamphleteers, postings on web logs are publications. Internet web logs, or "blogs," are open forums for communication where users, or "bloggers," can post their thoughts. *In re Stevens*, 15 Cal. Rptr. 3d 168, 173 n.3 (App. Ct. 2004). Blogs are a popular tool of communication—seven percent of the 120 million United States adult internet users have created a blog, and by the end of 2004, *thirty-two million Americans* were blog readers. Lee Rainie, Director of Pew Internet & American Life Project, *The state of blogging* (Jan. 2005), at http://www.pewinternet.org/PPF/r/144/report_display.asp.

The historic conception of the press included all types of publications that served as outlets for information and opinion; freedom of the press has "not [been] confined to newspapers and periodicals." *Branzburg v. Hayes*, 408 U.S. 665, 704 (1972). The United States Supreme Court has noted that today, "[a]ny person or organization with a computer connected to the Internet can 'publish' information." *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 853 (1997). In a similar vein, courts have noted that "[w]ith the Internet, the average computer blogger has, in effect, his or her own printing press to reach the world." *In re Stevens*, 15 Cal. Rptr. 3d at 172-73 (quoting *Vo v. City of Garden Grove*, 9 Cal. Rptr. 3d 257, 281 (App. Ct. 2004) (Sills, J., concurring & dissenting)).

In cases involving the publication of private facts on internet websites, courts have repeatedly understood that posting material online is publishing. Where an individual threatened to post sensitive employee information on his personal website, the court stated that the defendant was "threatening to publish" those facts. *Purdy v. Burlington N. & Santa Fe Ry. Co.*, No. 0:98-CV-00833-DWF, 2000 WL 34251818, at * 1, 3 (D. Minn. Mar. 28, 2000). Similarly, in *Carafano v. Metrosplash.com, Inc.*, without analyzing publication, the court addressed the posting of the plaintiff's personal information on a website as publication. 207 F. Supp. 2d 1055, 1068-69 (C.D. Cal. 2002).

The publicity requirement must be flexible. While the *Restatement (Second) of Torts* requires communication to be to the public at large or to enough people so that the matter is "substantially certain" to become public knowledge, section 652D cmt. a, disclosure to a limited number of people who have a special relationship to a plaintiff, such as family, neighbors, church members, club members, or fellow employees, can be equally as harmful as disclosure to the public at large and can satisfy the publicity requirement, *Miller v. Motorola, Inc.*, 560 N.E.2d 900, 903 (Ill. App. Ct. 1990). In a similar vein, the court in *Chisholm v. Foothill Capi-*

tal Corp. concluded that the plaintiff could have a special relationship with her office's potential clients and that information disclosed to them could satisfy the publicity requirement. 3 F. Supp. 2d 925, 940 (N.D. Ill. 1998). Conversely, disclosure to individuals with a "natural and proper" interest does not qualify as publicity. *See, e.g.*, *TCF Bank*, 707 N.E.2d at 222 (spouse had "natural and proper" interest in plaintiff's credit card debt); *Roehrborn v. Lambert*, 660 N.E.2d 180, 183 (Ill. App. Ct. 1995) (Police Training Institute administrator had "natural and proper" interest in potential officer's test results).

Marion published facts concerning Mr. Cafka's membership in BAN, since facts about his association were posted on blogs by Marion or under her direction. (R. at 5.) The fact that Mr. Cafka lost funding for the Music Man project as a result of the postings is evidence that the postings reached their audience on the Internet. (*See* R. at 3.) Just as the Internet postings in *Purdy* and *Carafano* qualified as publication, Marion's postings about Mr. Cafka's membership in BAN qualify as publication.

Alternatively, even if blogs readers are not considered the general public, they are a group of people who have a special relationship to Mr. Cafka. Mr. Cafka is on the cutting edge of computer technology, having established a business to design computers to project images into users' brains. (R. at 1-2.) Individuals who helped fund Music Man likely had a strong interest in computer technology, as did Mr. Cafka's competitors, including Marion's current employer. Like the plaintiff in *Chisholm*, Mr. Cafka has a special relationship with the individuals in his professional world, and his interactions with them can potentially propel or destroy his career. Unlike the individuals with whom facts were shared in *Roehrborn* and *TCF Bank*, Mr. Cafka's competitors and patrons have no "natural and proper" interest in knowing with whom Mr. Cafka associates in his private life.

B. Mr. Cafka's association with BAN was part of his private, not public, life because it was not part of the public record and he took multiple steps to maintain his privacy

Mr. Cafka kept his association with BAN firmly part of his private life. Facts that are part of the public record, such as court records or police reports, are not private. *Florida Star v. B.J.F.*, 491 U.S. 524, 532 n.7 (1989); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 494-95 (1975). Consequently, a state may not impose liability on a newspaper for publishing lawfully-obtained public facts about a publicly significant matter. *Florida Star*, 491 U.S. at 533, 536. Further, the more steps an individual takes to keep information private, the more likely it is to be found private. *See Chisholm*, 3 F. Supp. 2d at 929-30. In *Chisholm*, the plaintiff sued her former employer for invasion of privacy, alleging that a co-

worker told potential clients of the firm about her private romantic relationship with another person. *Id.* However, the court noted that the two appeared in public as a couple, lived together, and were open about their relationship; because the relationship was public, it was not a private fact. *Id.* at 940-41. In contrast, the plaintiff in *Diaz v. Oakland Tribune, Inc.*, took extensive steps to keep her original gender a private fact, having changed her driver's license, legal name, social security records, and high school records. 188 Cal. Rptr. 762, 771 (App. Ct. 1983). Her original gender was not in the public record, and the court concluded that before a local newspaper revealed she had been born male, it was a private fact. *Id.*

Like the plaintiff in *Diaz*, Mr. Cafka took multiple steps to keep his association with BAN a private matter. There is no evidence on the record that it was available to the public before Marion published it or that either BAN or Mr. Cafka had been charged with any crime. (R. at 5.) Unlike the situation in *Florida Star*, the facts here were not lawfully obtained but instead acquired through dishonest conduct. Further, unlike the plaintiff in *Chisholm* who was open in public about her relationship, Mr. "Cafka kept his membership in BAN a secret and apparently took steps to keep it a secret." (R. at 5.) To get the information, Marion had to scan Mr. Cafka's RFID chip, reverse engineer the algorithm in the chip, build a clone of the chip, and use the chip to access Mr. Cafka's computer files. (R. at 3.) The fact that she had to take multiple unauthorized steps to gain the information is evidence of the pains that Mr. Cafka took to keep his involvement with BAN a private matter.

C. To a reasonable person, Mr. Cafka's association with BAN would be highly offensive because of the ramifications of its disclosure; alternatively, if this court finds it is not offensive as a matter of law, it presents a question for a jury

Mr. Cafka's involvement with BAN would be highly offensive to a reasonable person, as demonstrated by his loss of funding after the fact was published. The publication itself as well as the context, conduct, and circumstances surrounding a publication are relevant to determine offensiveness. *Green v. Chi. Tribune Co.*, 675 N.E.2d 249, 254 (Ill. App. Ct. 1996). Further, if it is not clear as a matter of law whether a publication was offensive, then offensiveness is a question of fact for a jury. *See, e.g.*, *Miller*, 560 N.E.2d at 903 (whether fact that plaintiff had mastectomy surgery would be highly offensive was jury question).

In *Green*, the defendant newspaper published the words that the plaintiff said to her son after he died of a gang-related gunshot wound, along with a picture of his body. 675 N.E.2d at 251. The *Green* court

stated that reasonable people could differ and find that the publication was not about an ordinary daily activity and not a minor or moderate annoyance. *Id.* at 255 (citing *Restatement (Second) of Torts* § 652D cmt. c). Instead, it was about an extraordinarily painful event in the plaintiff's life, the plaintiff's published statements were made after she told reporters she did not want to make a statement, and the picture was taken while the reporters kept her out of her son's room. *Id.* Because reasonable people could make those findings, the court held that the plaintiff sufficiently alleged offensiveness. *Id.* In addition, where offensiveness is not clear as a matter of law, it is a question for the jury. *See Miller*, 560 N.E.2d at 903. As the court acknowledged in *Miller*, because it could not determine as a matter of law whether the defendant's disclosure of the plaintiff's mastectomy to co-workers would be highly offensive to a reasonable person, offensiveness was a question of fact for a jury to decide. *Id.*

Because Mr. Cafka suffered great embarrassment and lost funding for the Music Man project as a result of the publication of his involvement with BAN, reasonable people could differ and conclude that the publication was offensive. Although the matter here does not involve the death of a loved one as in *Green*, the same factors lean towards offensiveness. Sharing the fact that he was involved in an anti-abortion group was not an ordinary experience for Mr. Cafka, considering the steps he took to keep his involvement with BAN secret and the covert actions that Marion took. (*See* R. at 2-3.) It was more than an annoyance as well, considering his great embarrassment and loss of funding. (*See* R. at 3.) Alternatively, if this court cannot be certain that it the publication is offensive as a matter of law, then offensiveness is a matter for a jury, like the offensiveness of publicizing the plaintiff's mastectomy was a question for the jury in *Miller*.

D. While BAN's activities may be newsworthy, Mr. Cafka's personal involvement with them is not; community mores, which are properly considered by a jury, may also reflect that his personal involvement is not newsworthy

Mr. Cafka's personal association with BAN is not a legitimate public concern. Matters of legitimate public concern are frequently discussed as "newsworthy," *Y.G.*, 795 S.W.2d at 499, and certain subjects, such as criminal activity, are considered generally newsworthy, *see Cox Broad. Corp.*, 420 U.S. at 492. For other matters, courts look to a variety of factors to determine newsworthiness, including the social value of the facts, the depth of the publication's intrusion into private matters, and the extent to which the person voluntarily assumed a position of public notoriety. *Diaz*, 188 Cal. Rptr. at 772. However, as the *Restatement (Second) of*

Torts notes, "what is proper [in this analysis] becomes a matter of the community mores." Section 652D cmt. h. If there is room for differing views, the question is one properly before a jury, not a court. *Times Mirror Co. v. Superior Court*, 244 Cal. Rptr. 556, 562 (App. Ct. 1988).

1. *There is little if any social value in Mr. Cafka's specific connection with BAN*

Not every aspect of a person's life is a matter of public interest—even when the general issue is newsworthy, the particular individual's involvement in it may not be. *See Gilbert v. Med. Econ. Co.*, 665 F.2d 305, 308 (10th Cir. 1981). As the Tenth Circuit recognized:

> Because each member of our society at some time engages in an activity that fairly could be characterized as a matter of legitimate public concern, to permit that activity to open the door to the exposure of any truthful secret about that person would render meaningless the tort of public disclosure of private fact.

Id. Instead, the line must be drawn when the facts constitute "a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he has no concern." *Restatement (Second) of Torts* § 652D cmt. h.

In *Times Mirror*, upon returning to her apartment, the real party in interest found her roommate dead; after a reporter discovered her identity, her name was published in a newspaper. 244 Cal. Rptr. at 558. The court recognized that while the story was about criminal activity, the proper focus was whether the witness's *name* was newsworthy, and that inquiry was one properly for a jury. *Id.* at 562. In contrast, some facts are newsworthy *because* they are connected to particular individuals. In *Gilbert*, the defendants published an article that suggested that a plaintiff's personal problems caused her to commit malpractice on her job as an anesthesiologist and that consequently she harmed two patients. 665 F.2d at 306. The court noted that publishing the plaintiff's name and personal problems was newsworthy because the problems were the alleged cause of her malpractice and the publication warned potential patients and employers about the risks of working with her. *Id.* at 309.

In analyzing the social value of personal association, the right to freedom of association is relevant. Freedom of association "does not extend to joining with others for the purpose of depriving third parties of their lawful rights." *Madsen v. Women's Health Ctr.*, 512 U.S. 753, 776 (1994). But the Supreme Court has also proclaimed that "[i]t is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech." *NAACP v. Alabama*, 357 U.S. 449, 460 (1958). In *NAACP*, the court explicitly acknowledged that especially when a group holds dissi-

dent beliefs, preserving privacy in that group association may be necessary to preserve the freedom of association. *Id.* at 462. Because disclosure of other NAACP membership lists had resulted in economic consequences, physical threats, and loss of employment, the Court concluded that disclosure of the membership lists in question would likely violate the members' right to associate. *Id.* at 462-63.

There is no social value in the fact that Mr. Cafka is a member in and "Grand Nowest" of the anti-abortion group BAN. The group is opposed to abortion, and news stories have connected it with finding, following, and threatening doctors who performed abortions. (R. at 3.) Thus the group's general activities and existence are likely newsworthy, as abortion is a divisive, lively topic of debate in our country.

However, the fact that Mr. Cafka in particular belongs to the group is not newsworthy. While Mr. Cafka's involvement could be newsworthy if he was connected to criminal activity, as suggested by *Madsen*, the record does not reflect that BAN or its members have been convicted of criminal activity (R. at 1-9). Just as the court in *Times Mirror* focused on the witness's name, the issue here is Mr. Cafka's *personal involvement* in BAN. And unlike the plaintiff in *Gilbert*, Mr. Cafka's name and specific involvement in an anti-abortion group do not relate to or negatively impact his professional work. He has the liberty right recognized in *NAACP* to associate with like-minded individuals in his private life. Like publication of the NAACP membership lists, publication of the BAN membership list negatively affected Mr. Cafka's employment and adversely affected his freedom to associate.

2. *The publication was deeply intrusive in light of how private Mr. Cafka kept his involvement in BAN*

The second factor in evaluating newsworthiness is the depth of intrusion. *Michaels v. Internet Entm't Group, Inc.*, 5 F. Supp. 2d 823, 841 (C.D. Cal. 1998). In *Michaels*, the plaintiffs sued over the disclosure of videotape of their sexual relations. *Id.* at 840. The court noted that this factor must be determined in light of community mores, and it concluded that the plaintiffs were likely to convince a trier of fact that disclosure of the footage was deeply intrusive because it concerned very private matter. *Id.* at 841. Whether publication of Mr. Cafka's association with BAN was deeply intrusive must also be determined in light of community mores. Mr. Cafka's involvement with BAN was a very private matter for him, as demonstrated by the measures he took to keep it private, and a jury may likely find its disclosure was highly offensive. However, if this Court concludes that this factor is uncertain, the question must go to a jury.

3. *Mr. Cafka did not voluntarily assume a position of public notoriety, but is simply a businessman and entrepreneur*

Mr. Cafka did not voluntarily assume a public position. While individuals who seek public office or voluntarily become involved in public affairs do not have the right to keep issues private that are connected with their public conduct, not all individuals involved in public affairs lose their privacy rights. *See Diaz*, 188 Cal. Rptr. at 772. In *Diaz*, the plaintiff was the first female student body president of her college; however, the court concluded that there was little or no connection between her fitness for office and the published fact of her original gender. *Id.* at 772-73. The extent to which she assumed a position of public notoriety and opened up her private life were questions of fact for a jury. *Id.* at 773. On the other hand, in *Kapellas v. Kofman*, an editorial pointed out past offenses, already in the public record, of the minor children of a candidate for city counsel. 459 P.2d 912, 923-24 (Cal. 1969). Noting that the public is normally allowed to determine whether facts about government officials and candidates for those offices are relevant to their qualifications for office, the court found the publication newsworthy. *Id.* at 923. In a related vein, the court in *Carafano* concluded that publication of the plaintiff's home address was newsworthy because she became an entertainment celebrity, publicly discussed her home life, and entertained fans at her home. 207 F. Supp. 2d at 1069.

In contrast, although Mr. Cafka is a well-known inventor and a successful businessperson, (R. at 6, 1), he is not automatically a public figure. Like the plaintiff in *Diaz*, exactly whether and how much Mr. Cafka opened his life to public scrutiny is a question for the jury. Unlike the plaintiff in *Kapellas*, Mr. Cafka did not run for a public office, and so the public is not automatically entitled to scrutinize his private life. Because his leadership position in BAN is a private post, the public was not entitled to evaluate his qualifications for that office. Further, unlike the plaintiff in *Carafano*, Mr. Cafka did not make public any facts that would make the publication of his personal associations appropriate. To the contrary, he took steps to keep his membership in BAN a secret, (R. at 5), and revealing his status in BAN is not in any manner connected to the information he shared in his public doings as an inventor and businessperson.

III. BECAUSE MR. CAFKA'S EFFORTS WERE REASONABLE UNDER THE CIRCUMSTANCES, HIS RFID-BASED SECURITY SYSTEM AND OTHER MEASURES WERE SUFFICIENT TO PROTECT HIS INTERESTS UNDER MARSHALL'S TRADE SECRET ACT

Trade secret law protects the trade secret holder from disclosure or unauthorized use of the secret by those who have received the secret in confidence and by those who have gained the secret through improper means, such as theft or espionage. *Kewanee Oil Co.*, 416 U.S. at 475-76. In short, trade secret law protects trade secret holders such as Mr. Cafka from the actions of persons like Marion.

The Court of Appeals was correct in reversing the District Court's grant of summary judgment to Marion on the claim for misappropriation of trade secrets. Information protected under Marshall's Trade Secret Act must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality." (R. at 7.) Because the measures Mr. Cafka took to protect his trade secrets were reasonable as a matter of law and of fact, he is entitled to continue his case against his former employee, the defendant.

A. TAKEN IN THEIR ENTIRETY, MR. CAFKA'S EFFORTS TO PROTECT HIS TRADE SECRETS WERE REASONABLE UNDER THE CIRCUMSTANCES BECAUSE HE TOOK STEPS BOTH TO CONTROL ACCESS AND TO ENSURE CONFIDENTIALITY

Because Mr. Cafka made reasonable efforts to protect data relating to Music Man, that data is entitled to protection under the Trade Secret Act. To qualify for protection under Marshall's Trade Secret Act, the information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality." Marshall Rev. Code § 1947. Under Marshall's Trade secret act, as under trade secret law in general,[2] the reasonableness of the measures taken depends on the circumstances. *Id.*

Mr. Cafka took extraordinary measures to address key aspects of security. Although holders of trade secrets use a variety of methods to protect their trade secrets, those methods can be placed into one of two categories. A holder can preserve secrecy either by imposing a duty of

2. Marshall's statute is tracks the language of the *Uniform Trade Secrets Act* (1985) (UTSA). (R. at 7.) Other sources of trade secret law include the Restatement (Third) of Unfair Competition §§ 39-45 (1994), the *Restatement (First) of Torts* § 757 (1939), and the common law. These sources of law share common conceptions of reasonableness. *Accord Lyn-Flex West, Inc. v. Dieckhaus*, 24 S.W.3d 693, 698 (Mo.App. 1999). Because of this commonality, the basis for any particular jurisdiction's trade secret jurisprudence is irrelevant to the persuasive value of decisions from that jurisdiction.

confidentiality on those persons who have access to the secrets, or by limiting actual access to the secret. Mr. Cafka implemented an RFID-based security system, going so far as to implant chips in himself and his employees. (R. at 2.) He segregated employees and their computers at multiple work sites, and limited access to information on a need-to-know basis. (R. at 2.) He also executed confidentiality agreements with his employees. (R. at 2.) Due to Cafka's efforts to limit access and ensure confidentiality, his secrets are protected under the Trade Secret Act. *See* Marshall Rev. Code § 1947.

Methods need not be extreme to protect a trade secret. *Religious Tech. Center v. Netcom On-Line Comm. Serv., Inc.*, 923 F. Supp. 1231, 1254 (N.D. Cal. 1995). In *Netcom*, the court found that reasonable efforts could include "advising employees of the existence of a trade secret, limiting access to the information on a 'need to know basis,' requiring employees to sign confidentiality agreements, and keeping secret documents under lock." *Id.* at 1253-54 (citations omitted). In *Netcom*, the plaintiff had gone even further, logging documents, keeping materials at a limited number of sites, using alarms, issuing photo identification, and employing security personnel. *Id.* at 1254. The court determined the plaintiff's measures to be more than adequate. *Id.*

Like the plaintiff in *Netcom*, Mr. Cafka restricted access to his trade secrets and imposed duties on his employees. He kept his work at a limited number of sites, required employees to sign confidentiality agreements, and established an elaborate security system. (R. at 2.) Unlike the Center, the record does not indicate that he hired security personnel. However, given the small number of workers Mr. Cafka kept at each site, such a decision would be quite reasonable.

The means of protection need not be as elaborate as Mr. Cafka's measures. As long as a workplace is reasonably secure from burglary, it can be sufficient for an employer to require confidentiality agreements and to remind employees periodically of their agreements. *Vermont Microsystems, Inc. v. Autodesk, Inc.*, 88 F.3d 142, 150 (2d Cir. 1996). Simply storing a compilation of customer information on a computer with restricted access can be a reasonable means of maintaining secrecy if buttressed by a confidentiality agreement. *Morlife, Inc., v. Perry*, 56 Cal. App. 4th 1514, 1523 (App. Ct. 1997). Accordingly, reasonable efforts may consist of measures as simple as a password that restricts access in conjunction with notification to employees that the employer expects confidentiality.

B. MR. CAFKA USED EXTRAORDINARY METHODS TO CONTROL ACCESS TO THE MUSIC MAN PROJECT, INCLUDING AN RFID-BASED SECURITY SYSTEM THAT EMPLOYED IMPLANTED MICROCHIPS

Mr. Cafka used extraordinary methods to control access to the Music Man project. Among other measures, Mr. Cafka employed a Radio Frequency Identification (RFID) based security system to control access to work areas and to employee computers. (R. at 2.)

An RFID system consists of a scanner, a microchip containing information, and accompanying software which interprets the scan. *See* Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, 2004 UCLA J. of L. & Tech. 5, 4-7 *available at* http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf. The system works much like a bar code system, except that RFID technology doesn't require a direct line of sight. *Id.* at 3. Instead, the scanner sends out a radio signal to activate (and in some cases to power) the chip. *Id.* at 4-5. When the chip encounters the scanner's signal, it responds by transmitting identifying information back to the scanner. *Id.* at 4. The software in the scanner processes the information it receives and returns the results to the system. *Id.* at 6-7. Depending on the software, the result could be matching a lost pet with its owner, tracking goods in transit, or allowing an employee access to a secure area. *See id.* at 2.[3] In Mr. Cafka's case, he required each employee to be implanted with an electronic chip to control each employee's access to particular work areas and computers. (R. at 2.)

Mr. Cafka's RFID-based security system provided even greater security than other conventional systems. In concept, Mr. Cafka's RFID-based security system is the equivalent of a sophisticated password or keycard system. However, integral characteristics of this particular RFID-based system provide greater security than a password or keycard based system. Unlike conventional passwords, the RFID serial number, the "password," could not be communicated without reverse engineering. In contrast to keycards, implanted chips cannot be misplaced or stolen. Thus, Mr. Cafka's system was much more secure than other reasonable methods of protection.

Further, Mr. Cafka did not rely upon the security system alone. The reasonableness of Mr. Cafka's use of the RFID-based security system must be considered in the light of other steps Mr. Cafka took. *See* Mar-

3. While the record refers to the scanner as a transponder (*e.g.* R. at 2), RFID literature refers to the scanner as a transceiver and the chip as a transponder. *C.f. id.* at 4 ("Transponders are the data-carrying device in an RFID system and are usually referred to as RFID tags. . . The reader is a radio transceiver that communicates with the transponder via radio waves.") (citations omitted). To avoid confusion, this brief will use the terms "scanner" and "chip."

shall Rev. Code § 1947. To limit access, Mr. Cafka segregated the work among multiple sites, and provided secure computers, and avoided transferring data over the Internet. (R. at 2.) To ensure confidentiality, he not only required his employees to sign confidentiality agreements, but he minimized employees' contact with each other. (R. at 2.) Given these extensive security procedures, this Court must conclude that as a matter of law, that Mr. Cafka's RFID-based security system was part of reasonable efforts to protect the Music Man data. If any question of material fact concerning the implementation of these procedures remains, that question should be directed to the trial court. *See* Marshall R. Civ. P. 56(c)

C. MR. CAFKA'S CONFIDENTIALITY AGREEMENTS WITH HIS EMPLOYEES WERE REASONABLY CALCULATED TO PROTECT HIS SECRETS FROM DISCLOSURE, EVEN IF MARION'S AGREEMENT IS UNENFORCEABLE FOR LACK OF CONSIDERATION

Requiring employees to sign confidentiality agreements was a reasonable measure to protect the Music Man data. Marion's failure to sign the confidentiality agreement at the beginning of her employment is irrelevant to the question of whether Mr. Cafka took reasonable measures for several reasons.

First, the record shows that the company's standard practice was to enter into a confidentiality agreement with new employees. (R. at 2.) Because this Court is reviewing the grant of a summary judgment motion, facts must be construed in the light most favorable to the party opposing summary judgment. *Anderson,* 477 U.S. at 248. That favorable light directs that Mr. Cafka's policy be regarded as uniform. Given Marion's lack of good faith, her failure to sign the agreement should be construed as an evasion of that requirement, rather than a lack of diligence on Mr. Cafka's part. Further, Mr. Cafka showed diligence in safeguarding his rights by obtaining her signature when he discovered that she had not signed the agreement. (R. at 2.)

Second, it does not matter whether Marion was contractually bound by the confidentiality agreement because employees may be bound to confidentiality without such an agreement. *See Kewanee Oil Co.,* 416 U.S. at 475. When an employer discloses trade secrets to an employee so that employee can do her job, a confidential relationship is implied. *Id.*; *Futurecraft Corp. v. Clary Corp.*, 205 Cal. App. 2d 279, 285 (App. Ct. 1962); Thus, Marion would be bound by an implied confidential relationship not to disclose her employer's secrets.

Mr. Cafka reasonably relied on his employees being bound by a duty of confidence. Under the *Restatement (Third) of Unfair Competition* § 41, a duty of confidence is owed by a person if at time of disclosure "(1) the

person knew or had reason to know that the disclosure was intended to be kept in confidence, and (2) the other party to the disclosure was reasonable in inferring that the person consented to an obligation of confidentiality." If Marion or any other employee had any doubt as to whether Mr. Cafka considered their relationship confidential, his insistence on the confidentiality agreement should have been sufficient to communicate that expectation. Further, Marion represented that she agreed to keep her employer's confidence by signing that contract. Thus, Mr. Cafka successfully imposed a duty of confidence on Marion and his other employees.

Despite the generality of the confidentiality agreement, Marion could easily identify determine that the Music Man information was protected under Marshall's Trade Secret Act. She sought that information with the knowledge that it would confer a significant business advantage (R. at 2), a key aspect of trade secrets, *see Morlife*, 56 Cal. App. 4th at 1522. Specific notice of which secrets are protected is not required, particularly where itemization would jeopardize the secrecy of that information. *Autodesk*, 88 F.3d at 150. All that matters is that Marion had reason to know the information was confidential, and her employer had reason to believe that she had consented to an obligation of confidentiality. *See Restatement (Third) of Unfair Competition* § 41.

Mr. Cafka is entitled to protection from Marion's bad faith. The law of trade secrets is highly concerned with protecting trade secret holders against breaches of faith. *Pachmayr Gun Works, Inc. v. Olin Mathieson Chem. Corp., Winchester W. Div.*, 502 F.2d 802, 807 (9th Cir. 1974). Confidentiality agreements are primary examples of reasonable measures taken to protect secrecy. *Id.* This is not a case where the employer has taken no steps to limit the distribution of protected information, *see e.g. Equifax Servs., Inc. v. Examination Mgmt. Servs.*, 453 S.E.2d 488, 492 (Ga. App. Ct. 1994); failed to follow policies meant to ensure confidentiality, *see e.g. DB Riley, Inc. v. AB Engineering Corp.*, 977 F. Supp. 84, 91 (D. Mass. 1997); or encouraged the sharing of information among employees, *see e.g. Omega Optical, Inc. v. Chroma Tech. Corp.*, 800 A.2d 1064, 1067-68 (Vt. 2002). Rather, Mr. Cafka took measures that would certainly have protected him, had Marion not breached her duty of confidentiality.

Because a valid confidentiality agreement can only enhance Mr. Cafka's ability to impose a duty of confidence that is at least implied, this Court must conclude that Mr. Cafka used reasonable means to ensure confidentiality under Marshall's Trade Secret Act. If any doubt remains concerning whether Mr. Cafka consistently or correctly executed these confidentiality agreements, those issues of material fact must be reserved for the trial court. *See* Marshall R. Civ. P. 56(c).

D. THE REASONABLENESS OF MR. CAFKA'S MEASURES SHOULD BE JUDGED WITHOUT REFERENCE TO MARION'S SUCCESSFUL DISCOVERY OF HIS SECRETS THROUGH IMPROPER MEANS; TO FIND OTHERWISE WOULD BE TO THWART THE PURPOSES OF TRADE SECRET LAW BY UNJUSTLY REWARDING ESPIONAGE

To find Mr. Cafka's means of protection unreasonable in light of Marion's success in discovering his secrets would thwart the purposes of trade secret law. Trade secret law is designed to encourage both ethics and innovation. *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 749 (E.D. Mich. 1999) (citing *Kewanee Oil Co.*, 416 U.S. at 481-82). These laws enable businesses to enter into good faith relationships, and to share information within confidential relationships, in order to assist in product development. *See id.* Accordingly, trade secret laws punish industrial espionage and deny competitors any advantage that they have obtained by unfair means. *Id.* In the present case, the Marion's lack of good faith and use of improper means are undisputed. She sought employment with Mr. Cafka with the intention of stealing his Music Man technology and beating him to market with a finished product. (R. at 2.) Marion cannot escape liability through her success: her successful espionage should have no bearing on whether the measures used to protect the Music Man project were reasonable.

In *E. I. DuPont DeNemours & Co. v. Christopher*, the Fifth Circuit Court of Appeals found reasonable DuPont's efforts to protect its trade secrets, despite the relative ease with which those secrets could be stolen. 431 F.2d 1012, 1015-16 (5th Cir. 1970). In *DuPont*, undisclosed third parties hired two photographers to take aerial photographs of a methanol plant under construction. *Id.* at 1017. When DuPont employees noticed the airplane overhead, they began an investigation to discover why the craft was circling over the plant. *Id.* at 1013. The investigation revealed the mission and the identity of the two photographers. *Id.* These photographs had the potential to reveal aspects of DuPont's superior process for producing methanol. *Id.* at 1013-14. DuPont sued the photographers for damages due to disclosure of trade secrets and sought to enjoin both the continuing circulation of the information and any additional photography. *Id.* at 1014. The photographers argued that they were not liable because they had no confidential relationship with DuPont, they conducted their activities from public airspace (ostensibly breaking no aviation standards),[4] and they engaged in no fraudulent or illegal conduct in obtaining the photographs. *Id.* Yet the court decided that their method of acquiring the information was improper, and that DuPont had

4. The court concluded that it need not reach a question concerning the legality of the pilot's flight pattern. *DuPont*, 431 F.2d at 1017.

acted reasonably to protect its trade secrets, thus preserving its cause of action. *Id.* at 1015-16.

The court in *DuPont* reasoned that to find otherwise would unjustly reward improper means of discovery and would punish the persons trade secret law was intended to protect. *See id.* Although the court could require reasonable precautions against prying eyes, it would not be reasonable to require the DuPont to erect an impenetrable fortress. *Id.* at 1016-17. To require such security would place too great a burden on inventors. *Id.* at 1016. Rather, the law is designed to penalize spies and pirates for obtaining protected information through devious means. *Id.* Thus, security measures are not per se unreasonable just because a clever person is able to breach those measures in the course of espionage. To find those measure unreasonable merely because somebody was able to acquire the secret through trickery would be to give moral sanction to piracy. *Id.*

In the present case, Mr. Cafka's reasonable security measures were breached by a talented employee bent on espionage, and this employee should not be rewarded for her efforts. Further, Mr. Cafka himself took extraordinary measures to protect his information, including requiring his employees to sign confidentiality agreements. Unfortunately for Mr. Cafka Marion used extreme and unexpected measures to gain access to protected information, going as far as fabricating her own scanner and a duplicate RFID chip. (R. at 3.) Further, Marion had no intention of honoring her confidential employment relationship. Her conduct should not be rewarded.

Requiring Mr. Cafka to guard against these circumstances would place an unfairly heavy burden on Mr. Cafka. At best, it would force him to take extreme and costly measures. At worst, Marion would be unjustly enriched. To allow Marion's successful espionage to diminish the apparent reasonableness of Mr. Cafka's measures would be contrary to the purposes of trade secret law: trade secret law rewards innovation and effort, and punishes the unethical acquisition of secrets. *Kewanee Oil Co.,* 416 U.S. at 475-76. Accordingly, the reasonableness of Mr. Cafka's measures must be judged according to normal expectations of the business environment. Viewed in this context, Mr. Cafka took reasonable precautions to protect his trade secrets.

IV. MARION VIOLATED MARSHALL'S ANTI-CIRCUMVENTION ACT BY BREAKING A CRYPTOGRAPHIC ALGORITHM IN ORDER TO GENERATE SERIAL NUMBERS MIMICKING MR. CAFKA'S WITH THE GOAL OF CIRCUMVENTING THE RFID-BASED SECURITY SYSTEM

Marion violated Marshall's Anti-Circumvention Act (ACA) by decrypting the algorithm used to generate serial numbers in the RFID-

based security system. The ACA provides that "[n]o person shall circumvent a technological measure that effectively controls access to data." Marshall Rev. Code § 1492. The Act creates a cause of action for accessing information without authorization by circumventing those means.

Marion circumvented the RFID-based security system by breaking the cryptographic algorithm necessary to generate passwords compatible with the security system. The ACA defines "circumvention of a technological measure" as "[1] to decrypt an encrypted work, or otherwise to avoid, bypass[,] remove, deactivate a [2] technological measure[ ], [3] without the authority of the owner of the underlying data." *Id.*

The presence of the second and third elements is undisputed. The RFID-based security system is clearly a technological measure for purposes of the ACA because it requires the use of an algorithm and the application of a serial number to access information protected by this system. *See* Marshall Rev. Code § 1492. It is also clear that Marion had no authority to access the entire Music Man project—none of Mr. Cafka's employees were authorized to access to the entire body of data. The only question remaining is whether breaking the cryptographic algorithm in Mr. Cafka's chip constitutes circumvention. Because Marion broke the system as a whole, this court should hold that breaking the algorithm constitutes circumvention.

A. Marion violated the Anti-Circumvention Act when she circumvented the RFID-based security system by breaking and copying the cryptographic algorithm for Mr. Cafka's chip

A cryptographic algorithm is a mathematical formula used to transform a message from its original form ("plain text") to an unreadable form ("cipher text"). Kenneth P. Weinberg, Note, *Cryptography: "Key recovery" shaping cyberspace (pragmatism and theory)*, 5 J. Intell. Prop. L. 667, 673 (1998). To read the message, the message must be decrypted according to a multi-character "key," or by breaking the code. *Id.* at 674. Keys are commonly described by their bit length,: each bit is a digit or character in the key. H.R. Rep. No. 105-108, pt. 1, at 5 (1997). The longer the key, the more difficult to break the encryption scheme, because of the exponentially greater number of possible sequences of characters constituting the key. *Id.*

The chips for Mr. Cafka's RFID-based security system used cryptographic algorithms to generate 64-bit serial numbers based 16-bit codes transmitted by the scanners (R. at 2). Accordingly, the 64-bit serial numbers are encrypted versions of the original 16-bit codes. Upon receiving the correct serial number, a scanner would allow access to work areas or

computers.[5] (R. at 2.)

Marion's circumvention of the RFID-based security system with a cloned chip is strikingly similar to the circumvention at issue in *Universal City Studios, Inc. v. Reimerdes,* 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom., Universal City Studios, Inc., v. Corley*, 273 F.3d 429 (2d Cir. 2001). In *Reimerdes,* Universal City Studios and other seven other motion picture studios brought suit under the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA). 111 F. Supp. 2d at 303. The studios sought to enjoin the defendant from distributing a software program named DeCSS. *Id.* at 303. DeCSS allowed users to circumvent the Content Scrambling System (CSS), a technological measure the studios used to protect DVDs from illegal copying. *Id.* at 311. Content on DVDs with CSS technology is encrypted according to a cryptographic algorithm, and can be decrypted for playback only by licensed DVD players. *Id.* at 309-310.

DeCSS was created by reverse engineering a licensed DVD player to discover the cryptographic algorithm and keys protecting the movies. *Id.* at 311. DeCSS provided users with the cryptographic keys access the DVDs on unlicensed DVD players. *Id.* Although the defendants simply provided an alternate method of decryption, the court characterized this software as breaking the CSS copy protection system. *Id.* at 308. The court found that DeCSS circumvented CSS in violation of the DMCA. *Id.* at 319.

Similarly, Marion reverse engineered Mr. Cafka's RFID chip to discover his algorithm for the RFID-based security system. (R. at 3.) Using this information, she created a substitute chip. (R. at 3.) This chip allowed her access to Mr. Cafka's information without authorization. (R. at 3.) As in *Reimerdes*, the defendant broke the entire security system by (1) reverse engineering the protective technological measure, and (2) replacing an authorized component with the resulting unauthorized version. Accordingly, a reasonable jury could find Marion liable for circumvention under Marshall's Anti-Circumvention Act for breaking the cryptographic algorithm.

B. MARION'S ACTIONS DO NOT FALL UNDER THE STATUTORY EXCEPTIONS OF REVERSE ENGINEERING OR ENCRYPTION RESEARCH

Marion cannot claim that her reverse engineering falls under either statutory exception to liability for circumvention under the Anti-Circumvention Act. The ACA provides that:

---

5. Presumably the scanner could decrypt the serial number through application of a key specific to that algorithm, to determine whether the serial number corresponded with the original 16-bit code.

> It shall not be a violation of this provision (a) if the technology measure is "reverse engineered" by a person who has who has lawfully obtained the right to use the computer program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs.

Marshall Rev. Code § 1492.

Marion's actions are distinguishable from a similar reverse engineering exception applied by the Federal Circuit Court of Appeals in *Chamberlain Group, Inc., v. Skylink Technologies*, because the circumvention in *Chamberlain* did not infringe on Chamberlain's rights. *See* 381 F.3d 1178, 1204 (Fed. Cir. 2004). In *Chamberlain*, the defendant Skylink reverse engineered Chamberlain's encryption in order to create an aftermarket garage door opener that was compatible with Chamberlain products. *Id.* at 1183. Although Skylink reverse engineered the copyrighted code used to open the garage doors, access to the code was implicitly authorized by fair use: every customer who owned a Chamberlain garage door opener was entitled to the use of that code in order to open their garage doors. *Id.* at 1202. Through reverse engineering, Skylink merely provided owners of Chamberlain products with the means to achieve that lawful use. *Id.* at 1204.

In stark contrast to Skylink, Marion used reverse engineering to further an illegitimate purpose, her intended theft of the Music Man data. The record describes how Marion built her own scanner and tested her own chip in order to access work areas and computers protected by the RFID-based security system. (R. at 2). This court should not construe the ACA to allow reverse engineering for the purposes of acquiring trade secrets through improper means.

Neither can Marion claim that she is protected under the Act because she was merely developing another encryption product. The ACA provides that decryption shall not be a violation of the ACA "if the decryption is part of 'encryption research' . . . conducted to advance the state of encryption technology or to assist in the development of encryption products." Marshall Rev. Code § 1492. Marion's personal scanner and cloned chip were not encryption products: she fabricated a single version of each for her personal use. Neither can she argue that her development of Music Man would advance the state of encryption technology, because Music Man is not essentially an encryption product.

C. Even if the Music Man project is not protected by the Trade Secret Act, Marion could be found liable for violations of the Anti-Circumvention Act because the Anti-Circumvention Act creates an independent cause of action for mere circumvention

Even if Mr. Cafka's data is not protected under the Trade Secret Act, Marion could still be found liable for breaking the cryptographic algorithm used in the RFID-based security system. Unlike the DMCA, which protects only copyrighted materials, liability under the Anti-Circumvention Act is not linked to particular intellectual property rights in the underlying material. *Compare* Marshall Rev. Code § 1492 *with Chamberlain*, 381 F.3d at 1195. Rather, the statute imposes liability for digital trespass.

In *Chamberlain*, the court recognized a distinction between access rights and underlying copyright interests. 381 F.3d at 1193-94. It also recognized a statutory link between the two: the DMCA addresses access only where underlying copyright interests are implicated. *Id.* at 1197. The court refused to recognize a cause of action under the DMCA for circumvention alone, because such a broad reading would expand the rights of the copyright owner by allowing the owner to exclude public access entirely. *Id.* at 1200. However, no broad right of public access is at issue for data protected under the Anti-Circumvention Act.

In contrast to the DMCA, Marshall's Anti-Circumvention Act makes no reference to underlying property interests. It imposes liability for the simple act of circumvention, for bypassing a technological measure "without the authority of the owner of the underlying data." Marshall Rev. Code § 1492. Thus, where otherwise unprotected materials are concerned, liability under the Anti-Circumvention Act is analogous to liability for breaking and entering.[6] Accordingly, regardless of whether Mr. Cafka took reasonable steps to protect his secrets, Marion could be found liable for circumvention under the Anti-Circumvention Act.

CONCLUSION

There are genuine issues of material fact as well as questions of law that preclude summary judgment because, construed in the light most favorable to the non-movant below, Mr. Cafka, Marion's actions can be deemed an intrusion upon Mr. Cafka's seclusion, publication of private facts, a trade secret violation, and an anti-circumvention act violation. This Court should

6. Because Marion had no right to access the entire Music Man project, this court need not reach the question of whether the Anti-Circumvention Act would apply to someone who circumvented a technological measure which controlled access to her own data.

affirm the decision of the District Court of Appeals of Marshall and remand with instructions to proceed to trial.

Respectfully Submitted,

_____

COUNSEL FOR RESPONDENT

APPENDIX

Intrusion upon Seclusion, Marshall Revised Code §439(A):

> 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.

Public Disclosure of Private Facts, Marshall Revised Code § 562(B):

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his/her privacy, if the matter publicized is of a kind that:
>
> a. would be highly offensive to a reasonable person, and
> b. is not of legitimate concern to the public.

Anti-Circumvention Act, Marshall Revised Code § 1492:

> No person shall circumvent a technological measure that effectively controls access to data. As used in this section:
>
> a. To "circumvent a technology measure" shall mean to decrypt an encrypted work, or otherwise to avoid, bypass [,] remove, deactivate, or impair a technological measure[ ], without the authority of the owner of the underlying data.
> b. A technological measure "effectively controls access to data" if the measure, in an ordinary course of its operation, requires the application of information, or a process, or a treatment, with the authority of the owner of the underlying data, to gain access to the data.
>
> It shall not be a violation of this provision
>
> a. if the technology measure is "reverse engineered" by a person who has lawfully obtained the right to use the computer program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, or
> b. if the decryption is part of "encryption research" which means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies protecting data if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products. For purposes of this provision, "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

Applicable section of the Marshall Uniform Trade Secrets Act, Marshall Revised Code § 1947:

> "Trade Secret" shall mean information including but not limited to technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or a list of actual or potential customers or suppliers, that:
>
> a. is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
> b. is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.
>
> "Misappropriation" means:
>
> a. acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret was acquired by improper means
> b. disclosure or use [of] a trade secret of a person without express or implied consent by a person who
> i. used improper means to acquire knowledge of the trade secret. . .