

RAMP & PISANI, LLP
60 Westervelt Avenue
P.O. Box 249
Tenafly, New Jersey 07670
(201) 567-8877
Attorney for Plaintiffs,
Brian Pietrylo and Doreen Marino

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

BRIAN PIETRYLO, et al.

Plaintiffs,

Hon. Faith S. Hochberg, U.S.D.J.
Hon. Patty Schwartz, U.S.M.J.

Civil Action No. 06-5754 (FSH)

-v-

HILLSTONE RESTAURANT GROUP
d/b/a HOUSTON'S

Defendant.

Document filed electronically.

PLAINTIFFS' TRIAL BRIEF

RAMP & PISANI, LLP
60 Westervelt Avenue
P.O. Box 249
Tenafly, New Jersey 07670
201-567-8877
Attorneys for Plaintiffs

On the Brief:

Fred J. Pisani, Esq.

TABLE OF CONTENTS

PRELIMINARY STATEMENT 5

LEGAL ARGUMENT

POINT I

PLAINTIFFS WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT DEFENDANT DID NOT HAVE CONSENT OR AUTHORIZATION TO ACCESS “THE SPECTATOR”, IN VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT- 18 USC 2701 (a) (1) (SECOND COUNT OF AMENDED COMPLAINT) 9

POINT II

PLAINTIFFS WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT DEFENDANT EXCEEDED IT’S AUTHORIZATION, IF ANY, TO ACCESS “THE SPECTATOR”, IN VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT - 18 USC 2701 (a) (2) (SECOND COUNT OF AMENDED COMPLAINT) 13

POINT III

PLAINTIFFS’ WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT THE DEFENDANT WRONGFULLY TERMINATED THEM IN VIOLATION OF A CLEAR MANDATE OF PUBLIC POLICY (INVASION OF PRIVACY)- (SIXTH COUNT OF AMENDED COMPLAINT) 14

POINT IV

PLAINTIFFS’ WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT DEFENDANT VIOLATED THEIR COMMON LAW RIGHT TO PRIVACY 16

POINT V

PLAINTIFFS ARE ENTITLED TO PUNITIVE DAMAGES 21

POINT VI

THE FEDERAL STORED COMMUNICATIONS ACT: TO PREVAIL
PLAINTIFFS MUST PROVE THAT DEFENDANT EITHER
INTENTIONALLY OR KNOWINGLY ACCESSED THE
SPEC-TATOR WITHOUT AUTHORIZATION 24

POINT VII

THE NEW JERSEY WIRE TAPPING & ELECTRONIC SURVEILLANCE
CONTROL ACT: TO PREVAIL PLAINTIFFS MUST PROVE THAT
DEFENDANT EITHER KNOWINGLY OR PUPOSELY ACCESSED
THE SPEC-TATOR WITHOUT AUTHORIZATION 26

TABLE OF AUTHORITIES

Cases:

Alexander v Riga, 208 F3d 419 (2000) 21

Bisbee v. John C. Conover Agency Inc., 186 NJ Super 335, 340-41 (App. Div. 1982). 16

Borse v. Pierce Goods Shop Inc., 963 F 2d 611 (3d. Cir. 1992) 14,15

Entrot v. BASF Corp. 359 NJ Super 162 (App. Div. 2003). 11

Erickson v. Marsh and McLennan Company, 117 NJ 539 (1986) 11

Hennessey v. Coastal Eagle Point Oil Co., 129 NJ 81 (1992) 14

Kolstad v American Dental Ass’n, 527 US 526 (1999)..... 21

MacDougall v. Weichert, 144 NJ 380, 391 (1996). 14

Milwaukee & ST. Paul R. Co. v Arms, 92 US 489 (1875) 21

Pierce v. Ortho Pharmaceutical Corp., 84 NJ 58, 72 (1980). 14

Pure Power Boot Camp, et. al. v Warrior Fitness Boot Camp, et. al., 587 F. Supp. 2d 548 (S.D. N.Y. 2008)17, 18,25

Rumbauskas v. Canter, 138 NJ 173 (1994). 16

Smith v Wade 461 US 30 (1983) 21

Smyth v. Pillsbury Company, 914 F. Supp. 97 (E. D. Pa. 1996) 15

Wyatt Technology Corp. v. Smithson et al. (2006 WL 5668246(C.D. Cal.),

Statutes

18 USC 2701 et seq. 10,21,24

18USC §2701-11 9

18USC §2701(c)(2) 10, 13

18 USC 2707 (c). 24

NJSA 2A;156A-32 (a). 26

NJSA 2A:156A-27 (a)..... 10. 26

PRELIMINARY STATEMENT

Plaintiffs respectfully submit this trial brief to address certain legal issues that may arise during the course of trial.

In March 2004, defendant, Hillstone Restaurant Group, d/b/a Houston's ("Houston's" or "Defendant") hired plaintiffs, Brian Pietrylo ("Pietrylo") and Doreen Marino ("Marino"), to work as servers at Houston's Restaurant located at the Riverside Square Mall in Hackensack, New Jersey.

During their private off time from work, Pietrylo and Marino maintained accounts on MySpace.com. In March 2006, Pietrylo set-up a "private group" on his MySpace account. Pietrylo named the group "The Spectator". It was a private group not open to the public.

Pietrylo intended The Spectator to be private. The homepage of The Spectator included the following language:

The Spec-Tator

Category: Other

Type: Private Membership

Founded: March 2, 2006

Location: Hackensack, New Jersey

Members: 2

"A place for those of us at Riverside to talk about all the crap/drama/and gossip occurring in our workplace, without have to worry about outside eyes prying in...but because the group is oh so private, only participants will stay members. Past and present employees welcomed."

The initial posting from Pietrylo included the following:

“I just thought this would be a nice way to vent about any BS we deal with at work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation.”

Pietrylo sent email invitations to other employees inviting them to become members of The Spectator. The email invitation contained a link to The Spectator and once the invitee accepted the invitation, a link to the site would permanently appear on the invitee’s own homepage, also stored on the MySpace.com website. Among the invitees were plaintiff Marino, Pietrylo’s live-in girlfriend, and Karen St. Jean (“Karen”), a greeter at the restaurant. Pietrylo invited no managers working at the restaurant nor did he invite any upper corporate personnel.

In May 2006, Robert Anton (“Anton”), one of Houston’s on-site managers and Karen’s supervisor, approached Karen while she was working a shift at Houston’s Restaurant. He asked Karen for her personal email address and password so that he could access The Spectator from Karen’s personal MySpace.com homepage. Since Anton was her boss and her manager, Karen gave him her personal information. If he were not her manager, Karen would not have given him her personal information. Karen has repeatedly stated that if she did not give Anton her personal information she thought something would happen to her at work. She felt pressured. She didn’t want to lose her job, especially since Houston’s had recently fired her husband, who worked there as a manager.

Karen did not give Anton permission to share her password with upper management personnel of Houston’s, parent company, Hillstone Restaurant Group, including Robert Marano (“Marano”), the Regional Supervisor of Operations, Tino Ciambriello (“Ciambriello”), Vice-President of Operations, overseeing approximately 45 restaurants

nationwide, and Michael Lamb (“Lamb”), Director of Human Resources, responsible for approximately 6,000 employees.

Karen did not permit Anton to share her password with other managers working at the restaurant, although she did expect him to show the content of The Spectator to those managers, such as Tijeon Rodriguez and Jason Sokolow.

Anton accessed The Spectator on a number of occasions. He made copies of the postings on The Spectator, although he never gave a copy of them to Marano, Ciambriello or Lamb. Anton did not fire either plaintiff, nor was he involved in the decision to fire the plaintiffs.

There are various factual versions on how Marano secured Karen’s personal email address and password.

Marano admitted that he was not invited to The Spectator. He also admitted reading the words on the front page that the group was entirely private and it could only be joined by invitation. He understood what the word private meant yet he continued to read the postings on the site. He accessed The Spectator a number of times, although he knew that Pietrylo was the creator of The Spectator during his first visit to the site. In an email dated May 6, 2006, Marano shared Karen’s email address and password with Ciambriello and Lamb. Both Ciambriello and Lamb work out of offices in San Francisco, California. Ciambriello is the Vice President of Operations, overseeing approximately 45 restaurants nationwide. Lamb is the Director of Human Resources, responsible for approximately 6,000 employees.

In the email, Marano gave them step-by-step instructions on how to access The Spectator.

The body of that email is as follows:

“How to get into the site;

Go to www.myspace.com

Under Member Login:

karenjaochicho@yahoo.com

Under password:

Keepout1

On the far right of the main screen in a blue box you will see “my group”, click on that

Then click on the Houston’s Logo,

Scroll down just below the large photos and on the right of the screen click on “view all topic”

You will be able to read all of the posting listed since this site inception 8 weeks ago.

Please call me once you have had a moment to review.

Thank you,
Rob Marano”

Marano terminated Pietrylo because he created The Spectator and posted comments therein and terminated Marino because she was part of the group and posted comments on The Spectator about the restaurant and its management.

LEGAL ARGUMENT

POINT I

PLAINTIFFS WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT DEFENDANT DID NOT HAVE CONSENT OR AUTHORIZATION TO ACCESS “THE SPECTATOR”, IN VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT- 18 USC 2701 (a) (1) (SECOND COUNT OF AMENDED COMPLAINT)

In 1986, Congress amended the Federal Wire Tap Act by enacting the Electronic Communication Privacy Act of 1986 (ECPA), which includes the Federal Stored Communications Act, 18USC §2701-11. The purpose of the amendment was to update and clarify the federal privacy protection and standards in light of dramatic changes in new computer and telecommunication technologies. *Senate Report No. 99-541, Cong., 2d Sess. I (1986)*.

In enacting the ECPA, Congress recognized that “computers are used extensively today for the storage and processing of information” and that while a first-class letter was “afforded a high level of protection against unauthorized opening” there were “no comparable...statutory standards to protect the privacy and security of communications” transmitted by new forms of telecommunications and computer technology. *Id.* at 3 and 5. As such, Congress adopted the ECPA, which represents a fair balance between privacy expectations of American citizens and legitimate needs of law enforcement agencies. *Ibid.*

Title II of the ECPA creates civil liability for one who “(1) intentionally accesses without authorization a facility thru which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters

or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. 18 USC 2701 et seq.

New Jersey amended its wiretap act in 1993, P.L.1993, C.29. These amendments, regulating access of stored electronic communications, were identical to the ECPA (Title II) amendments. NJSA 2A: 156A-27(a). Plaintiffs contend that defendant has violated both of these statutes.

One of the exceptions to liability exists when prior consent is given by an authorized user to access the site. 18USC §2701(c)(2) accord NJSA 2A: 156-27(c) 2.

Defendant contends that plaintiffs' claims (Second Count and Fourth Count) should be dismissed because Karen St. Jean consented on several occasions to access by Houston's managers.

Contrary to defendant's claim, plaintiffs will prove, by a preponderance of the evidence, that Karen St. Jean did not voluntarily consent or authorize defendant to access "The Spectator."

First, she did not provide Tijean Rodriguez, a manager at Houston's Restaurant, with her email address and password to access The Spectator. Sine they were friends, she showed him the website at his home during a social evening. She did not show him the website in an employer-employee environment.

Second, she only provided Anton, another of Houston's on-site managers, with her email address and password because he asked for it as her manager. He asked for it while she working at the workplace. Karen testified that she gave it to him because he was the manager. Had he not been the manager, she would not have given it to him.

She repeatedly testified that if she did not give Anton her email address and password she thought something would happen to her at work. She felt pressured. She did not want to lose her job.

Based upon this evidence, it is clear that Karen St. Jean's consent was not freely given. Although there was no actual threat, Karen believed that there was an implied threat.

In addressing whether consent is freely given, the court would consider Karen's perception, whether accurate or not, in determining whether consent was freely given.

Erickson v. Marsh and McLennan Company, 117 NJ 539 (1986); *Entrot v. BASF Corp.* 359 NJ Super 162 (App. Div. 2003).

The court, however, does not have to decide whether or not Karen freely consented to providing Anton with her email address and password, since Anton did not terminate the plaintiffs and was not involved at all in the decision to fire the plaintiffs. Anton testified that he did not even provide Marano, the Regional Supervisor who fired the plaintiffs, with copies of the postings he made from The Spectator.

Even if the court were to find that Karen freely consented to providing Anton with her password, Karen's consent to one is not consent to all. Karen did not give Anton carte blanche to do whatever he wanted with her personal information, such as pass it along to others, extremely high up in Houston's corporate structure.

Karen testified that she only gave her email address and password to Anton. She did not consent or permit him to pass it along to Marano, Ciambriello or Lamb. In her declaration, she declared that she did not consent or give permission to Marano, Ciambriello or Lamb to use her email address and password to access The Spectator. Until recently, she did not even know that they had used her personal information to access The Spectator.

Defendant's claim that consent to one is consent to all borders on the absurd. As an example, please consider the following hypothetical: Karen gives her home key to Anton to go pick up some Houston paperwork that she left there. Not only does Anton use the key to go to her house to pick up the paperwork, he gives the key to Marano, and Marano gives the key to Ciambriello and Lamb. One could not reasonably argue that not only was she giving consent to Anton to go to her house, but that she was giving consent to anyone else who he gave the key to, to go to her house and rummage through her belongings. This makes no logical sense and would not be supported by law.

Plaintiffs will show that Karen St. Jean did not provide Marano with her email address and password. They will further show that Anton gave Marano St. Jean's email address and password and that he used it to access "The Spectator" on a number of occasions, and later, provided Ciambriello and Lamb with St. Jean's email address and password, following their request.

Based upon the foregoing, the plaintiffs will be able to prove that defendant accessed The Spectator in violation of this federal statute.

POINT II

PLAINTIFFS WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT DEFENDANT EXCEEDED IT'S AUTHORIZATION, IF ANY, TO ACCESS "THE SPECTATOR", IN VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT- 18 USC 2701 (a) (2) (SECOND COUNT OF AMENDED COMPLAINT)

For all of the reasons outlined in Point I above, plaintiffs will prove, by a preponderance of the evidence, that defendant exceeded it's authorization, if any, to access "The Spectator, in violation of 18 USC 2701 (a) (2).

POINT III

PLAINTIFFS' WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT THE DEFENDANT WRONGFULLY TERMINATED THEM IN VIOLATION OF A CLEAR MANDATE OF PUBLIC POLICY (INVASION OF PRIVACY)- (SIXTH COUNT OF AMENDED COMPLAINT)

It is well established that “an employee has a cause of action for wrongful discharge when the discharge is contrary to a clear mandate of public policy.” *Pierce v. Ortho Pharmaceutical Corp.*, 84 NJ 58, 72 (1980).

Sources of public policy include the United States and New Jersey Constitutions, federal and state laws, and administrative rules, the common law and specific judicial decisions. *MacDougall v. Weichert*, 144 NJ 380, 391 (1996).

INVASION OF PRIVACY: VIOLATION OF PUBLIC POLICY

The sixth count of the amended complaint alleges that plaintiffs were wrongfully terminated in violation of the public policy guaranteeing the right to privacy. According to the New Jersey Supreme Court in *Hennessey v. Coastal Eagle Point Oil Co.*, 129 NJ 81 (1992) “both logical and ample precedence support a finding of public policy and the language and jurisprudence of the New Jersey Constitution.” *Id.* at 90.

In *Hennessey*, the New Jersey Supreme Court did not find that the constitutional right to privacy governs the conduct of private actors, however, they did find that existing constitutional privacy protections form the basis for a clear mandate of public policy supporting the wrongful discharge claim. *Id.*

Additionally, in *Borse v. Pierce Goods Shop Inc.*, 963 F 2d 611 (3d. Cir. 1992), the Court of Appeals held that an invasion of privacy would give rise to a wrongful discharge action in violation of a clear mandate of public policy. *Id.* at 620.

In its holding, the *Borse* court observed that if the plaintiff could establish and sustain an action for invasion of privacy and show that the intrusion would be highly offensive to a reasonable person, then that would be sufficient to conclude that the discharge violated public policy. *Id.* at 620-626.

In *Smyth v. Pillsbury Company*, 914 F. Supp. 97 (E. D. Pa. 1996) an at will employee brought an action against its former employer alleging wrongful discharge in violation of public policy claiming an invasion of his right to privacy as a result of the interception of emails sent to and from the plaintiff to his supervisor over the employer's electronic email messaging system. The court affirmed plaintiff's termination finding that he had no expectation of privacy with regard to the matter in which the email communications were transmitted specifically over defendant-employer's electronic messaging system or were sent to work computers at the defendant's workplace. The court, however, acknowledged the cause of action for wrongful discharge in violation of a clear mandate of public policy relating to an invasion of privacy claim. *Id.* at 98-100.

Based upon these holdings and the facts which will be introduced during the trial, as more fully discussed below in Point IV, plaintiffs will prove, by a preponderance of the evidence, that the defendant wrongfully discharged them in violation of a clear mandate of public policy; specifically invasion of privacy.

POINT IV

PLAINTIFFS' WILL PROVE, BY A PREPONDERANCE OF THE EVIDENCE, THAT DEFENDANT VIOLATED THEIR COMMON LAW RIGHT TO PRIVACY

In today's workplace, one area of conflict is the proper balance between an employee's right to privacy and an employer's right to control and manage the workplace.

As such, New Jersey courts recognize common law tort claims for invasion of privacy. *Rumbauskas v. Canter*, 138 NJ 173 (1994). Of these, a cause of action for "unreasonable intrusion upon seclusion" is the most applicable for potential invasion of privacy in the workplace. *Id.*

In order to prevail based upon this claim, the plaintiffs must produce facts that show that (1) their solitude of seclusion or their private affairs of concerns were infringed; and (2) the infringement would be highly offensive to a reasonable person. *3 Restatement Torts 2d §652B* See also *Bisbee v. John C. Conover Agency Inc.*, 186 NJ Super 335, 340-41 (App. Div. 1982).

Based upon the evidence in this record, plaintiffs will prove that the defendant violated their common law right to privacy.

First, to be actionable, the intrusion must lack consent. There is no dispute that Pietrylo and Marino never consented to any of Houston's on-site managers or it's parent company's high-level executives accessing The Spectator. As previously discussed, Karen St. Jean did not consent or authorize access to "The Spectator", either.

Plaintiffs had a reasonable expectation of privacy with regard to The Spectator. The creation, maintenance and use of "The Spectator" took place outside of the workplace. An invitation was necessary to lawfully access "The Spectator". It was Pietrylo's intention that

The Spectator be private as indicated by the language on his homepage as well as his initial posting.

A recent court decision out of New York, although not binding on this court, shed further light on the issue of a reasonable expectation of privacy regarding electronic communications in an employer-employee setting.

In *Pure Power Boot Camp, et. al. v Warrior Fitness Boot Camp, et. al.*, 587 F. Supp. 2d 548 (S.D. N.Y. 2008), a former employer brought an action seeking an injunction and damages, accusing former employees of stealing employer's business model, customers and documents. In support of their claim, the employer submitted numerous personal emails of the employee, which it had accessed and copied off of the employer's computer. The former employee claimed that the employer had violated the Electronic Stored Communications Act, 18 USC 2701.

The employees were hired by the owner of Pure Power Boot Camp to work at her fitness center. While employed, the employees improperly accessed the owner's office, retrieved a signed restrictive covenant agreement and shredded it. The employees soon left their employ, and they opened a competing fitness center. Pure Power's owner, using one of her company's computers, accessed and printed emails from three of the former employee's personal accounts: Hotmail, Gmail and WFBC. She stated she was able to access the hotmail account because the employee had left his username and password on the company computer so that it would automatically load when the hotmail account was accessed. She accessed one of the other accounts because the employee had given his username and password to another Pure Power employee (although the former employee denied this).

The former employee admitted using the work computer to view some of hot mail emails, but claimed that he never drafted or received any emails on these accounts while he was at work.

In addressing the issues, the court noted that accessing and obtaining emails directly from an electronic communication service provider is a violation of the Stored Communications Act if done without authorization. The employer claimed that she was authorized to access the emails because (1) the employee had no expectation of privacy in his Hot Mail email account and (2) he had impliedly consented to access by leaving the user name and password in her work computer.

The court rejected both of the employer's claims and found that she had violated the Stored Communications Act. The court began its holding by stating that courts routinely find that employees have no reasonable expectation of privacy in their workplace computers where the employer has a policy, which clearly informs employees that company computers cannot be used for personal email activity. **However**, this was not a case where an employee was using his employer's computer or email system, and then claimed that the emails contained on the employer's computers are private. In Pure Power, as in our case at bar, the employee did not store any of the electronic communications on the employer's computers, servers or systems. The employee, as in our case at bar, did not send, receive or post communications on the employer's computers or email system. The communications, as in our case at bar, were located on and accessed from third party communication service providers, there, Hot mail, here, My Space.

Based upon the foregoing, the court found that the employee had a reasonable expectation of privacy based upon his subjective belief that his personal email accounts,

stored on third party computer systems, protected (albeit ineffectively) by passwords, and would be private.

The court also rejected the claim that the employee had implied consented to access to the email account.

In the case at bar, The Spectator postings were not posted or transmitted over Houston's electronic messaging system. Plaintiffs did not use defendant's computers to access The Spectator or participate on The Spectator. All of it was done outside of work on plaintiffs' private time.

Houston's admits that it accessed The Spectator by using a participant's password. A jury will have to decide if Houston was "authorized" to use that password. The unauthorized use of an individual's private password to access the website clearly establishes that there was a reasonable expectation of privacy.

From the facts adduced during discovery, a jury could also find that defendant's conduct was highly offensive to a reasonable person.

If you believe Karen St. Jean, Marano secured her email address and personal password without her consent, knowledge or permission. Not only did he use it to access The Spectator, on a number of occasions, he shared her personal information and password with a Vice President, who oversees 45 restaurants nationwide, and the Director of Human Resources, who handles 6,000 employees. He gave them the information and told them how to access the site so that they could access the site and monitor it, if they desired.

Marano admits that he accessed The Spectator on more than one occasion, even though he discovered during his first visit to the site that Pietrylo was its creator. Did he confront Pietrylo about The Spectator before he accessed it the second time? No. Did he

speak to him at all about it before he fired him? No. Why did he continue to access The Spectator? He certainly didn't do it to continue to read the postings since reading them before had upset him. A jury could conclude that he went back onto The Spectator to spy on and continue to monitor the plaintiffs, and the other participants of The Spectator, without their knowledge.

Defendant's callous and arrogant conduct evidences a complete disregard for the rights and feelings of the plaintiffs and the other employees who worked at the restaurant and participated in The Spectator. In this case, the jury must be the ultimate arbitrator to determine whether Houston's has gone to far.

Defendant claims that they found the language used in the postings to be "offensive", "troubling" and "disgusting". Under these facts, however, a jury could easily find that Houston's actions were "offensive", "troubling" and "disgusting", as well as highly offensive to a reasonable person, when their off-site high level executives improperly accessed The Spectator and spied on a small group of their non-management employees, who worked as servers, bar tenders, and greeters, at one of their many restaurants.

POINT V

**PLAINTIFFS ARE ENTITLED TO PUNITIVE DAMAGES UNDER THE STATUTE
AND FEDERAL LAW**

There is a specific damages provision in the plain language of the Electronic Stored Communications Act (18 USC 2707), which provides that in a civil action the court may assess punitive damages if the violation of the statute is willful or intentional. 18 USC 2707 (c). This is less of a standard to meet than in other federal statutes where punitive damages are available. In most of them, the violation must be malicious and willful. *Please see Alexander v Riga, 208 F3d 419 (2000); Kolstad v American Dental Ass'n, 527 US 526 (1999); Smith v Wade 461 US 30 (1983)*. Under this statute, however, punitive damages are available if the conduct, which results in a violation of the statute, is either willful or intentional.

As stated by the Supreme Court, many years ago, in *Milwaukee & ST. Paul R. Co. v Arms, 92 US 489 (1875)*: “Redress commensurate to such injuries should be afforded. In ascertaining its extent, the jury may consider all the facts which relate to the wrongful act of the defendant, and its consequences to the plaintiff, but they are not at liberty to go farther, unless it was done willfully or was the result of that reckless indifference to the rights of others which is equivalent to an intentional violation of them...” *Id.*

To assess punitive damages, there must have been some willful misconduct, or that entire want of care, which would raise the presumption of a conscious indifference to consequences. *Id. 91 US at 493.*

That conscious indifference and want of care is evident in this case. “The Spectator” was created and maintained completely outside the workplace. Participation, such as reading

and writing the postings present on “The Spectator”, was not done using the defendant’s computers or email system. It was done off work hours, not during work hours.

Neither plaintiff consented to or authorized Houston’s managers or Hillstone’s upper management personnel to access “The Spectator”.

Karen St. Jean did not voluntarily consent to or authorize Rob Marano to access “The Spectator” using her email address and password. She certainly did not consent or authorize Rob Marano to provide her email address and password to Tino Ciambriello and Michael Lamb, so that they could access “The Spectator.”

Rob Marano, Hillstone’s Regional VP of Operations and the individual who terminated plaintiffs, knew the first time he accessed “The Spectator” that Brian Pietrylo created “The Spectator”. With that knowledge in hand, what did Marano do? Did he immediately terminate the plaintiffs for creating and/or participating in “The Spectator”? No. Did he summon Pietrylo to his office and advise him that he had accessed “The Spectator”? No. Did he ask Pietrylo for his consent and authorization to continue to access “The Spectator”? No. Did he confront him with copies of the postings he made from “The Spectator”? No.

Instead, what he did was to send an email to Tino Ciambriello, Hillstone’s VP of Operations, an upper management executive responsible for overseeing 45 restaurants nationwide, and Michael Lamb, Hillstone’s Head of Human Resources, another upper management executive, responsible for overseeing approximately 6,000 employees nationwide, and provided them with Karen St Jean’s email address and password. In the email, he gave them explicit, step-by-step instructions on how to access “The Spectator” using Karen St. John’s password.

In addition, he accessed “The Spectator” on other occasions to monitor what was being posted on the site. Only later did he then terminate the plaintiffs because of “The Spectator.”

Marano’s conduct exhibited a conscious indifference to the rights and interests of Karen St. Jean, Doreen Marino and Brian Pietrylo.

POINT VI

**THE FEDERAL STORED COMMUNICATIONS ACT: TO PREVAIL PLAINTIFFS
MUST PROVE THAT DEFENDANT EITHER INTENTIONALLY OR KNOWINGLY
ACCESSED THE SPEC-TATOR WITHOUT AUTHORIZATION**

The Federal Stored Communications Act is a criminal statute with a civil action component. 18 USC §2707(a).

The elements necessary to establish criminal liability are intentional access without authorization. Defendant believes that in order to succeed on a civil claim under the act, not only do you have to prove these criminal elements, you also have to prove an additional element: that defendant knew the victim or user had not authorized them. This is inaccurate.

Under the statute, a criminal offense is committed if one ...**intentionally** accesses without authorization a facility through which an electronic communication service is provided... and ... obtains... electronic communications while it is in electronic storage in such system... 18 USC 2701 (a) (1).

Under the civil action section of the statute, ...any ...person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing **or** intentional state of mind, may, in a civil action, recover from the person or entity... 18 USC 2707 (a)

The key term in the civil action section is the disjunctive term “or”. The statute’s civil section states knowing **or** intentional. Defendant, however, uses the conjunctive term “and” in their proposed jury charge.

Knowing and intentional are synonymous terms. The Thesaurus lists knowing as a synonym for intentional, and intentional as a synonym for knowing.

The American Heritage Dictionary defines intentional as intended, done deliberately and defines knowingly as planned or deliberate.

There is no additional element necessary to establish civil liability. The claimant must prove a knowing or intentional access without authorization. In Wyatt Technology Corp. v. Smithson et al. (2006 WL 5668246(C.D. Cal.)), defendant, amongst other things, filed a counterclaim against the plaintiff alleging a violation of the Federal Stored Communications Act. In rendering its decision, the court articulated what the claimant had to prove to succeed under the act. The court stated that the claimant had to prove intentional access without authorization and referenced both §2701(a)(1) and §2707(a). There was no additional “knowledge” element. Id. at 8. See also Pure Power Boot Camp v. Warrior Fitness Boot Camp, 2008 WL 4866165(S.D.N.Y.).

In both of these cases, the court found a violation of the Federal Stored Communications Act where the alleged victim left their username and password on one of the work computers which was discovered by another and was used to access electronic communications of the alleged victim stored on a third party service provider. In each of these cases, the claimant was not required to prove both that the company knew that the victim had not authorized them when they left their user name and password on the computer and that with that knowledge they intentionally accessed the information. The proof required is an intentional or knowing access without authorization.

POINT VII

THE NEW JERSEY WIRE TAPPING & ELECTRONIC SURVEILLANCE CONTROL ACT: TO PREVAIL PLAINTIFFS MUST PROVE THAT DEFENDANT EITHER KNOWINGLY OR PUPOSELY ACCESSED THE SPEC-TATOR WITHOUT AUTHORIZATION

The New Jersey Wire Tapping & Electronic Surveillance Control Act is a criminal statute with a civil action component. NJSA 2A; 156A-32 (a).

The elements necessary to establish criminal liability are knowing access without authorization. Defendant believes that in order to succeed on a civil claim under the act, not only do you have to prove these criminal elements; you also have to prove an additional element. This is inaccurate.

Under the statute, a criminal offense is committed if one ...**knowingly** accesses without authorization a facility through which an electronic communication service is provided... and ... obtains... electronic communications while it is in electronic storage in such system... NJSA 2A: 156A-27 (a).

Under the civil action section of the statute, ...any ...person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing **or** purposeful state of mind, may, in a civil action, recover from the person or entity... NJSA 2A; 156A-32 (a)

The key term in the civil action section is the disjunctive term “or”. The statute’s civil section states knowing **or** purposely. Defendant, however, uses the conjunctive term “and” in their proposed jury charge.

Knowing and purposely are synonymous terms. The Thesaurus lists knowing as a synonym for purposely, and purposely as a synonym for knowing.

The American Heritage Dictionary defines purposely as intended, done deliberately and defines knowingly as planned or deliberate.

There is no additional element necessary to establish civil liability. The claimant must prove a knowing or purposeful access without authorization. The proof required is a knowing or purposeful access without authorization.

Respectfully submitted,

RAMP & PISANI, LLP
Attorneys for Plaintiffs

DATE: March 4, 2009

s/Fred J Pisani
FRED J. PISANI, ESQ.