IN THE COURT OF APPEALS
STATE OF ARIZONA
DIVISION ONE

MOBILISA, INC., a Washington corporation,

Plaintiff/Appellee,

vs.

JOHN DOE 1 and THE SUGGESTION BOX, INC.,

Defendant/Appellants.

Court of Appeals
Division One
No. 1 CA-CV 06-0521

Maricopa County
Superior Court
Cause No. CV2005-012619

APPELLANTS' OPENING BRIEF

Christopher T. Whitten, Esq. - #014296
WHITTEN BERRY, PLLC
101 North First Avenue, Suite 1800
Phoenix, Arizona 8503

Charles Lee Mudd, Jr.
LAW OFFICES OF CHARLES LEE MUDD, JR.
3344 North Albany Avenue
Chicago, Illinois 60618

Co-Counsel for **Defendants/Appellants**

IN THE COURT OF APPEALS
STATE OF ARIZONA
DIVISION ONE

MOBILISA, INC., a Washington corporation,

Plaintiff/Appellee,

vs.

JOHN DOE 1 and THE SUGGESTION BOX, INC.,

Defendant/Appellants.

Court of Appeals
Division One
No. 1 CA-CV 06-0521

Maricopa County
Superior Court
Cause No. CV2005-012619

APPELLANTS' OPENING BRIEF

Christopher T. Whitten, Esq. - #014296
WHITTEN BERRY, PLLC
101 North First Avenue, Suite 1800
Phoenix, Arizona 8503

Charles Lee Mudd, Jr.
LAW OFFICES OF CHARLES LEE MUDD, JR.
3344 North Albany Avenue
Chicago, Illinois 60618

Co-Counsel for **Defendants/Appellants**

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Statutes

Rules

JURISDICTIONAL STATEMENT

I. THE PARTIES

Appellee Mobilisa, Inc. ("Mobilisa") is a Washington corporation in the software development business, specializing in applications for mobile devices. Nelson Ludlow ("Ludlow") is the President of Mobilisa.

Appellant John Doe is an anonymous party that allegedly obtained unauthorized access to Mobilisa's computer system and obtained a copy of a personal e-mail from the system.

Appellant The Suggestion Box, Inc., ("TSB") is an Arizona Corporation that offers anonymous electronic mail services to individuals, corporations, and organizations. Appellant John Doe used TSB's services to send a copy of the personal e-mail to various third parties.

II. FACTUAL BACKGROUND

On June 21, 2005, Nelson Ludlow sent a personal email to his girlfriend Shara Smith from his corporate Mobilisa email address (referred to herein as the "Ludlow Email"). See Index on Appeal, item number 10 (hereinafter references to documents included in the Index on Appeal shall be referred to Index _____, with the item number following). October 11, 2005 Ludlow Declaration, attached thereto, at ¶ 2. He also sent copies of the Ludlow Email to two other places: an account which then forwarded the message to his own cellular phone and his own personal e-mail account.[1] *Id.* The contents of the Ludlow Email contained intimate, personal communications from Mr. Ludlow to Ms. Smith. *Id.* at ¶ 7.

[1] For the privacy of those concerned, the actual email addresses have not been included.

On June 27, 2005, John Doe, a subscriber of TSB's anonymous email service, sent an anonymous electronic communication to at least one individual at Mobilisa with the subject line "Is this a company you want to work for?" (referred to herein as "Anonymous Email"). The body of the Anonymous Email contained the contents of the Ludlow Email. *Id.* ¶ 2.

Upset that the Ludlow Email had been published to others at Mobilisa, Ludlow had an extensive review of Mobilisa's computer system conducted. This review found no evidence of an intrusion in, or that John Doe had obtained the Ludlow Email from, Mobilisa's computer systems. *Id.* at ¶ 6; and see, Transcript of December 2, 2005 Proceedings, attached as Index 21 at pp. 18-29 ("It is true that Mr. Ludlow said we can't find in our investigation any intrusion that we can pin this on.").

III. PROCEDURAL BACKGROUND

Without any evidence that anyone had obtained unauthorized access to its computer system, Mobilisa filed a Complaint for Damages and Injunctive Relief in the Superior Court of the State of Washington in July of 2005, naming John Does 1-10 as Plaintiffs (referred to herein as "the Washington case"). Index 1. The Washington case, in essence, alleged that an anonymous party trespassed and violated two Federal laws by obtaining unauthorized access to its computer system and wrongfully accessing information therein.

In August of 2005, still without any evidence of unauthorized access to its computer system, Mobilisa filed an Application for Subpoena in the Arizona Superior Court seeking to conduct discovery to determine the identity of the sender

of the Anonymous Email. Index 1. TSB objected. Index 4. The matter was briefed and Respondent Judge Davis issued an initial, three page minute entry on December 28, 2005 (referred to herein as "Under Advisement Ruling"). Recognizing that forcing TSB to reveal the identity of the person who sent the anonymous email might violate both the United States and Arizona Constitutions and that there was no controlling law in Arizona, the trial court adopted the standard employed by the Delaware Supreme Court in *Doe v. Cahill*, 884 A.2d 451 (Del. 2005) ("*Cahill* Standard), the only State Supreme Court case to have addressed the issue at the time. Index 15.

The *Cahill* Standard establishes two prerequisites to discovery intended to uncover the name of an anonymous speaker: (1) the plaintiff must make reasonable efforts to notify the anonymous speaker and (2) the plaintiff must establish that it would survive summary judgment.

In spite of its adoption of the *Cahill* Standard, the trial court ordered TSB to notify the sender of the Anonymous Email of the pending discovery request. The trial court also provided the sender an opportunity to object. Index 15. TSB notified John Doe of the pending discovery request, and John Doe objected to it. Index 26.

In its Under Advisement Ruling, the trial court also concluded that "there is not sufficient verified evidence provided to the Court at this point for the Court to find that the underlying claim would survive a motion for summary judgment." Index 15. Rather than deny Mobilisa's motion, the trial court invited the parties to further brief the issue in light of its adoption of the *Cahill* Standard.

As requested by the trial court, Mobilisa filed additional memoranda in support of its request to conduct discovery. Index 17, 20 and 23. TSB and John Doe also filed additional memoranda objecting to the requested discovery. Index 18, 19 and 26.

On February 27, 2006, despite Mobilisa producing no evidence that unauthorized access or intrusion had occurred in or to its computer system, the Court found that the Plaintiff "established enough material facts through its initial and supplemental affidavits that, given reasonable inferences that could be drawn from those facts, a finder of fact could conclude that the email information in question, was, more probably than not, wrongfully obtained," and therefore allowed Mobilisa to conduct discovery to ascertain the identity of the sender of the anonymous email. Index 25.

Appellants filed a Petition for Special Action on April 14, 2006. Without reaching the merits raised in the Petition for Special Action, this Court declined to accept special action jurisdiction. See this Court's Order dated May 10, 2006.

STATEMENT OF THE ISSUES

1. Whether the trial court abused its discretion by improperly applying the *Cahill* Standard to the claims in Mobilisa's complaint by disregarding essential elements in each of these claims - particularly, unauthorized access to Mobilisa's computer systems - for which Mobilisa failed to produce any evidence in the record warranting the trial court's conclusion that Mobilisa could survive summary judgment and order requiring TSB to disclose John Doe's identity?

2. Whether the trial court abused its discretion by imposing the burden to notify Petitioner John Doe of the proceedings under the *Cahill* Standard on TSB?

3. Whether the trial court abused its discretion by issuing its ruling prior to the deadline having passed for Petitioner John Doe to have filed a Memorandum in Opposition?

ARGUMENT

This appeal squarely focuses on whether the trial court erred in applying the *Cahill* Standard it adopted for determining when a court may compel disclosure of an anonymous speaker's identity. As the *Cahill* Standard requires a plaintiff to demonstrate it would survive summary judgment, a plaintiff seeking disclosure of an anonymous speaker's identity must therefore produce *some* evidence that supports each essential element of *at least one* of the claims alleged in its complaint. Although the trial court properly adopted a summary judgment standard, it failed to enforce the accompanying summary judgment burden against Mobilisa. In reviewing the record, the trial court erroneously focused on whether it appeared the Ludlow Email had been obtained wrongfully. This was misguided. For, in doing so, the trial court completely ignored the requisite essential element for all of Mobilisa's claims – unauthorized access to Mobilisa's computer system. The record simply does not contain any evidence supporting this element required of each of Mobilisa's claims. Consequently, the trial court erred in applying *Cahill* and concluding Mobilisa could satisfy a summary judgment standard. For this reason, this Court should reverse the trial court's February 27, 2006 Ruling granting Mobilisa's Motion for Leave to Conduct Discovery, order the lower court to deny Mobilisa's Motion for Leave to Conduct Discovery, and order the lower court to preclude discovery of John Doe's identifying information.

I. STANDARD OF REVIEW

Generally, a trial court's discovery rulings will not be disturbed absent an abuse of discretion. *Blazek v. Superior Court In and For the County of Maricopa*,

177 Ariz. 535, 537, 869 P.2d 509, 511 (App. 1994). It is always an abuse of discretion, however, when the trial court misapplies the law. *Brown v. Superior Ct.*, 137 Ariz. 327, 332, 670 P.2d 725, 730 (1983); *Grant v. Arizona Public Service Co.*, 133 Ariz. 434, 456, 652 P.2d 507, 529 (1982) (Abuse of discretion where a judge commits an "error of law ... in the process of reaching [a] discretionary conclusion").

The United States and Arizona Constitutions both create privileges that allow anonymous free speech. Whether an evidentiary privilege exists is a question of law, and this Court is not bound by the trial court's conclusions of law on such matters. *City of Tucson v. Superior Ct.*, 167 Ariz. 513, 809 P.2d 428 (1991).

II. THE LAW OF FORCING THE DISCLOSURE OF THE IDENTITY OF ANONYMOUS SPEAKER

The advent of electronic communications has required courts to apply long-standing constitutional principles to new technologies and communications media. In this case, courts have long recognized that the First Amendment of the United States Constitution protects anonymous speech. Courts have applied these same principles to electronic communications. Particularly, Courts have been required to apply these principles to situations where a Plaintiff seeks to discover information that would identify an anonymous speaker. Recently, the Supreme Court of Delaware issued the first opinion from a State Supreme Court to address this specific issue in *Doe v. Cahill*, 884 A.2d 451 (Del. 2005).[2]

[2] On July 13, 2006, the Supreme Court of Wisconsin issued the second opinion from a State Supreme Court to address this specific issue. *See,* Lassa v. Rongstad, 718 N.W.2d 673 (Wisc. 2006). In *Lassa*, the Wisconsin

A. PROTECTION OF ANONYMOUS SPEECH

The First Amendment protects the right to speak anonymously. *Buckley v. Am. Constitutional Law Found,* 525 U.S. 182, 200 (1999); *Talley v. California,* 362 U.S. 60, 65 (1960). The Supreme Court has stated that "[a]nonymity is a shield from the tyranny of the majority," that "exemplifies the purpose" of the First Amendment: "to protect unpopular individuals from retaliation . . . at the hand of an intolerant society." *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334, 357 (1995) (holding that an "author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment"). Consequently, courts must "be vigilant . . . [and] guard against undue hindrances to political conversations and the exchange of ideas." *Buckley,* 525 U.S. at 192. This vigilant review "must be undertaken and analyzed on a case-by-case basis," where the court's "guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue." *Dendrite Int'l, Inc. v. Doe No. 3,* 775 A.2d 756, 760-61 (N.J. Super. A.D. 2001).

B. PRIVILEGED SPEECH APPLIED TO ANONYMOUS ELECTRONIC COMMUNICATIONS

The principles protecting anonymous speech have been extended to the Internet and electronic communications. *Reno v. ACLU,* 521 U.S. 844, 870 (1997)

Supreme Court discussed and adopted the concerns raised by *Doe v. Cahill,* 884 A.2d 451 (Del. 2005). However, the *Lassa* court concluded that a motion to dismiss standard would satisfy these concerns in Wisconsin because, unlike Delaware, Wisconsin requires particularity in pleading the claims at issue. *Id.* at 687. Because Arizona is a notice pleading state (like Delaware), *see, Anserv Ins. Servs., Inc. v. Albrecht,* 192 Ariz. 48 (Ariz. 1998), *Lassa* is inapplicable to this appeal. In addition, it should be noted that a motion for reconsideration has been filed with the Wisconsin Supreme Court in *Lassa.*

(there is "no basis for qualifying the level of First Amendment protection that should be applied to" the Internet). As the First Amendment protects the right to speak anonymously and this right extends to electronic communications, any discovery device seeking anonymous speakers' names and addresses is subject to a qualified privilege. Consequently, courts must consider this qualified privilege before authorizing discovery in such cases. *See, Sony Music Entertainment v. Does,* 326 F.Supp.2d 556, 565 (S.D.N.Y. 2004) ("Against the backdrop of First Amendment protection for anonymous speech, courts have held that civil subpoenas seeking information regarding anonymous individuals raise First Amendment concerns."). In so doing, the courts addressing these issues have made efforts to balance the interests of the anonymous speakers against the plaintiff's need for the subpoenaed information. *See, e.g., Cahill*, 884 A.2d 451; *Doe v. 2theMart.com*, 140 F.Supp.2d 1088 (W.D. Wash. 2001); *Dendrite*, 775 A.2d at 771; *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal.1999).

As these courts have recognized, an inherent problem arises in such cases because, at the outset of litigation, plaintiffs typically rely upon mere allegations of wrongdoing. However, a privilege is generally not overcome by mere allegations. Indeed, a serious chilling effect on anonymous speech would result if Internet speakers knew they could be identified by persons who merely allege wrongdoing, without necessarily having any intention of carrying through with actual litigation. *See, e.g., Seescandy.com*, 185 F.R.D. at 578 ("People who have committed no wrong should be able to participate online without fear that someone who wishes

to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity."); *see also, 2theMart.com*, 140 F.Supp.2d at 1093 ("If Internet users could be stripped of . . . anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment Rights. Therefore, discovery requests seeking to identify anonymous Internet users must be subject to careful scrutiny by the courts.").

Consequently, courts have employed standards and imposed strict requirements upon plaintiffs that must be met prior to authorizing the discovery of information identifying anonymous speakers. *See, e.g.*, *Cahill*, 884 A.2d at 460-461; *2theMart.com*, 140 F.Supp.2d 1088; *Dendrite*, 775 A.2d at 771; *Seescandy.com*, 185 F.R.D. at 578.

C. EMERGENCE OF THE *CAHILL* STANDARD

In October 2005, the Delaware Supreme Court addressed the issue of what standard should be applied to determine when the disclosure of an anonymous speaker's identity could be obtained through discovery. In so doing, it thoroughly analyzed the various standards employed by other courts in similar circumstances. The *Cahill* court concluded that the most effective standard would be a synthesized version of the standard adopted in *Dendrite Int'l, Inc. v. Doe No. 3,* 775 A.2d 756, 760-61 (N.J. Super. A.D. 2001).

Essentially, the standard employed by *Cahill* requires the *Plaintiff* seeking discovery of an anonymous speaker's identity to (a) "undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for an order of

disclosure, and to withhold action to afford the anonymous defendant a reasonable opportunity to file and serve opposition to the application" and (b) demonstrate that it would survive a summary judgment motion. *Cahill*, 884 A.2d at 460-461. With respect to the notification requirement, the Court held that:

> The notification provision imposes very little burden on a [] plaintiff while at the same time giving an anonymous defendant the opportunity to respond. When *First Amendment* interests are at stake we disfavor *ex parte* discovery requests that afford the plaintiff the important form of relief that comes from unmasking an anonymous defendant.

Id. As to the summary judgment requirement, the Court concluded that requiring a plaintiff to demonstrate it would survive a summary judgment provides the most effective balance between a plaintiff's rights and those of the defendant anonymous speaker. *Id.* The *Cahill* opinion represents the first State Supreme Court opinion to address these issues. Recently, the United States District Court for the District of Arizona agreed with *Cahill* and concluded that "a summary judgment standard should be satisfied before [a party] can discover the identifies of [an anonymous defendant]." *Best Western International, Inc. v. Doe*, No. CV-06-1537-PHX-DGC, 2006 U.S. Dist. LEXIS 56014, *11 (D. Ariz. July 25, 2006).

III. TRIAL COURT ABUSED ITS DISCRETION

The trial court abused its discretion by (a) improperly applying the *Cahill* motion for summary judgment standard to the claims in Mobilisa's complaint by disregarding essential elements in each of these claims - particularly, unauthorized access to Mobilisa's computer systems - for which Mobilisa failed to produce any evidence in the record warranting the trial court's conclusion that Mobilisa could

survive summary judgment and order requiring TSB to disclose John Doe's identity, (b) improperly imposing the burden on TSB to notify Petitioner John Doe of the proceedings, and (c) improperly failing to consider John Doe's opposition by issuing its ruling prior to the deadline having passed for Petitioner John Doe to have filed an opposition memorandum.

A. JUDGE DAVIS IMPROPERLY APPLIED THE LAW IN DISREGARDING ESSENTIAL ELEMENTS OF MOBILISA'S CLAIMS – PARTICULARLY, UNAUTHORIZED ACCESS TO MOBILISA'S COMPUTERS – FOR WHICH MOBILISA FAILED TO PRODUCE ANY EVIDENCE.

Initially, the trial court correctly determined that a summary judgment standard, such as that in *Cahill*, should be used to determine whether Mobilisa was entitled to conduct discovery that would require TSB to identify John Doe.[3] Specifically, the *Cahill* Standard requires that a plaintiff produce evidence that it would withstand a summary judgment motion as a prerequisite to conducting such discovery. *Cahill*, 884 A.2d at 460-461. Although the Court correctly adopted such a standard, it misapplied the standard to the claims in the Plaintiff's Complaint.

In its February 27, 2006 Order granting the Plaintiff's Motion for Leave to Conduct Discovery, the Court merely found that "a finder of fact could conclude that the email information in question was, more probably than not, wrongfully obtained." Index 25 at p. 2. The trial court incorrectly limited the scope of

[3] For this reason, TSB does not appeal the Court's adoption of this standard and, because Appellee has not filed a separate appeal on this issue, this question is not squarely before the Court. It should be noted, however, that the *Cahill* Standard represents but a baseline for protecting the constitutional rights of anonymous speakers. For, *Cahill* does not impose an additional element requiring a balance of the harms. Appellants would not object to this Court adopting a more stringent standard than that established in *Cahill*.

Plaintiff's burden under the *Cahill* Standard to production of evidence that the email was wrongfully obtained. It completely failed to address an essential element in each of Mobilisa's claims - unauthorized access to Mobilisa's computers. In fact, Mobilisa should have been required to produce some evidence that John Doe wrongfully obtained the Ludlow Email *from its computers* to meet its burden under the *Cahill* Standard. The record clearly demonstrates the absence of ANY such evidence.

In addition, the trial court misapplied the *Cahill* Standard by failing to address two additional elements required of Mobilisa under the federal statutes - intent and damages. TSB challenged the evidentiary support on both of these elements arguing that Mobilisa had failed to provide any evidence supporting them. Index 19. Thus, the Court also misapplied the *Cahill* Standard by failing to address these issues.

1. The Court Properly Adopted a Standard Requiring Plaintiff to Show It Would Overcome a Motion for Summary Judgment

As part of the *Cahill* Standard, a plaintiff seeking disclosure of an anonymous speaker's identity must demonstrate that it would survive a summary judgment motion brought against the claims in its complaint. *Cahill*, 884 A.2d at 462. The trial court properly adopted this standard. Index 25 at p. 1. Consequently, Mobilisa had the burden of producing evidence demonstrating that it would survive a motion for summary judgment challenging each of the four claims in its Complaint.

2. Summary Judgment Standard

Summary judgment is appropriate if no genuine issues of material fact exist and the moving party is entitled to judgment as a matter of law. Ariz. R. Civ. P. Rule 56(c); *Orme School v. Reeves*, 166 Ariz. 301, 309, 802 P.2d 1000, 1008 (Ariz. 1990). Summary judgment should be granted if the facts produced in support of the claim or defense have so little probative value, given the quantum of evidence required, that reasonable people could not agree with the conclusion advanced by the proponent of the claim." *Id.* Importantly here, because the *Cahill* Standard required the Plaintiff to demonstrate that it would overcome summary judgment, the burden of coming forward with evidence to support its various claims was Plaintiff's. *Id.* at 310, 802 P.2d 1009.

A party moving for summary judgment need make only a prima facie showing that no genuine issue exists on an essential element of each claim. *See Dobson v. Grand Int'l Bhd. Of Locomotive Eng'rs.*, 101 Ariz. 501, 505, 421 P.2d 520, 524 (1966). Indeed, a party moving for summary judgment need merely point out by specific reference to the relevant discovery that no evidence existed to support an essential element of the claim. *Id.* Once a movant has made such a prima facie showing, the nonmovant has the burden to produce sufficient evidence to show that there is a genuine issue. The nonmovant "cannot defeat a motion for summary judgment and require a trial by a bare contention that an issue of fact exists." *Id.* Rather, it "must show that evidence is available which would justify a trial of the issue." *Id.*

3. The Trial Court Erred in Disregarding an Essential Element in Each of Mobilisa's Claims – Unauthorized Access to Mobilisa's Computers

The trial court erroneously limited its ruling to deciding whether a question of fact existed as to whether the Ludlow Email had been obtained wrongfully. This ruling disregards a critical essential element that exists in each of the claims in Mobilisa's Complaint – intrusion into *its* computer system. This error is material. For, Mobilisa provided no evidence that John Doe intruded into its computer system in any of its various memoranda. In fact, Mobilisa's own evidence suggests he did not do so. Given the absence of any evidence supporting this essential element and considering the plethora of alternative theories that could explain how John Doe obtained the Ludlow Email, Mobilisa could not withstand a summary judgment motion on any of its claims.

a. Each of Mobilisa's Claims Require as an Essential Element Unauthorized Access to Mobilisa's Computers

In its Complaint, Mobilisa alleged violations of the Stored Communications Act, 18 U.S.C. §2701 (Count I); the Computer Fraud and Abuse Act, 18 U.S.C. §§1030 (a)(4), (a)(5) (Counts II and III); and, trespass to chattels (Count IV). All four of these claims include as an element that John Doe obtained *unauthorized access to Mobilisa's computers*. Indeed, Mobilisa pled John Doe's unauthorized access to its computers in each cause of action in its Complaint.

i. Stored Communications Act, 18 U.S.C. §2701

The Stored Communications Act ("SCA"), 18 U.S.C. §2701, prohibits one from intentionally accessing "without authorization a facility through which an

electronic communication service is provided." 18 U.S.C. §2701 (a)(1). Further, the SCA prohibits an individual from intentionally exceeding an authorization to access a facility and "thereby [obtaining] . . . access to a wire or electronic communication while it is in electronic storage in such system."[4] 18 U.S.C. §2701 (a)(2).

For an otherwise criminal statute, Section 2707 of the SCA provides for a civil remedy. Pursuant to §2707, Mobilisa seeks a civil remedy for John Doe's unauthorized use of Mobilisa's computers and computer systems and Mobilisa's "mobilisa.com" email accounts.

ii. Computer Fraud and Abuse Act, 18 U.S.C. §§1030

Mobilisa has alleged as separate counts violations of §1030(a)(4) and §1030(a)(5)(iii) of the Computer Fraud and Abuse Act, 18 U.S.C. 1030, *et seq.* 18 U.S.C. §1030(a)(4) prohibits anyone from "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. §1030(a)(4). Similarly, 18 U.S.C. §1030(a)(5) prohibits anyone from intentionally accessing "a protected computer without

[4] This would not apply to a situation where an authorized user provides a third party with access to the authorized user's account. *See Sega Enters. v. MAPHIA*, 948 F. Supp. 923, 930 (D. Cal. 1996).

authorization, and as a result of such conduct, causes damage" where such conduct causes at least $5,000 in damages. 18 U.S.C. §1030(a)(5)(A)(iii) and (B)(i).

Again, for an otherwise criminal statute, Section 1030(g) of the Computer Fraud and Abuse Act provides for a civil remedy. Pursuant to §1030(g), Mobilisa seeks a civil remedy for John Doe's unauthorized use of Mobilisa's computers and computer systems and Mobilisa's "mobilisa.com" email accounts. Index 1 at ¶¶ 1, 7. 14, 18. Indeed, in its Complaint, Mobilisa alleges that John Doe "knowingly and with intent to defraud, accessed Mobilisa's protected computer system, without authorization and/or in excess of authorized access." Index 1 at ¶¶ 14, 18.

iii. Trespass to Chattels

Arizona has adopted the Restatement (Second) of Torts with respect to the tort of trespass to chattels. *Koepnick v. Sears Roebuck & Co.,* 158 Ariz. 322, 330-31, 762 P.2d 609, 617-18 (1988) ("The Restatement provides that the tort of trespass to a chattel may be committed by intentionally dispossessing another of the chattel or using or intermeddling with a chattel in the possession of another"). Mobilisa alleges that the Defendants have "knowingly, intentionally and without authorization used and intentionally trespassed upon Mobilisa's property." Index 1 at ¶ 24. This property, Mobilisa alleges, consists of its computers, computer networks, and email accounts. Index 1 at ¶¶ 22-24.

b. The Record Contains No Evidence Demonstrating that the Ludlow Email was Obtained by Unauthorized Access to Mobilisa's Computers

The Court below failed to require Mobilisa to produce some evidence that John Doe obtained the Ludlow Email through unauthorized access *to Mobilisa's*

computers, an essential element for each of the claims in its Complaint. For, the record clearly demonstrates the apparent and obvious absence of evidence demonstrating, or even suggesting, this occurred.[5]

In its Under Advisement Ruling, the Court concluded that "there is not sufficient verified evidence provided to the Court . . . for the Court to find that the underlying claim [sic] would survive a motion for summary judgment." Index 15. Mobilisa has presented no evidence since that ruling demonstrating that John Doe obtained the Ludlow Email through unauthorized access *to Mobilisa's computers, computer networks, or "mobilisa.com" email accounts.* Indeed, apart from the fact that John Doe had possession of the Ludlow Email, Mobilisa has provided absolutely no evidence that John Doe obtained the Ludlow Email wrongfully or, more importantly for summary judgment, that John Doe wrongfully obtained the Ludlow Email *through unauthorized access to Mobilisa's computers.*

In fact, Mobilisa's own evidence demonstrates that John Doe *did not* obtain the Ludlow Email from any Mobilisa computer, computer networks, or "mobilisa.com" email accounts. Nelson Ludlow, Chief Executive Officer and founder of Mobilisa, Inc., in his first declaration states that Mobilisa's computer systems are protected by a password system and a firewall. Index 1, see Ludlow Declaration, attached thereto, at ¶ 5. Indeed, he states "Mobilisa secures its computer and email systems in order to prevent the release of confidential or

[5] Whether by failing to address the proper question before the Court, or reaching an erroneous conclusion on the proper question, TSB contends the Court failed to recognize the clear absence of evidence on this issue.

classified information." *Id.*, see Ludlow Declaration at ¶ 3. He further states that Mobilisa, a high-tech company servicing government contracts:

> conducted searches of its computer systems . . . [which] included investigating the anonymous email and attempting to determine how the sender(s) had accessed Mobilisa's email storage systems and distributed the [email]. ***It was unable to identify the security breach. Mobilisa's Network Administrator and owner of the recipients network could not discover how the email was obtained.***

Id., see Ludlow Declaration at ¶ 6 (emphasis added). The inability of a corporation that provides "wireless and mobile systems, including infrastructure, applications, and support, to government and military entities" to find any unauthorized access to its systems is significant and telling. *Id.*, ¶ 2. The most able people to determine whether someone obtained unauthorized access to Mobilisa's systems found no evidence that this occurred.

At oral argument, Plaintiff's counsel admitted and conceded this point. Index 21, see transcript attached thereto, p. 18, lines 17-19 ("It is true that Mr. Ludlow said we can't find in our investigation any intrusion that we can pin this on."). In fact, Plaintiff's counsel admitted that "we don't even know who did it, let alone how they did it, when they did it." *Id.*, p. 29, lines 19-21. Consequently, there simply does not exist any evidence supporting Mobilisa's theories. Mobilisa's allegations merely represent insufficient guesswork.

Despite receiving an opportunity to supplement the record, Mobilisa failed to provide any evidence, verified or not, that further supported its allegations regarding unauthorized access to Mobilisa's computers. While the unsworn declarations of Nelson Ludlow and Shara Smith dated February 1, 2006 and