Luis v. Zang et al Doc. 109

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

v.

JOSEPH ZANG, et al.,

Defendants.

(Lead Case No. 1:11-cv-884)
Case No. 1:12-cv-629

Dlott, J.
Bowman, M.J.

REPORT AND RECOMMENDATION

Pursuant to an Amended Order of Consolidation filed on January 31, 2013, Lead Case No. 1:11-cv-884 and Case No. 1:12-cv-629 have been partially consolidated for purposes of pretrial proceedings. However, documents that relate to dispositive matters are to be filed solely in the case record to which the dispositive motion pertains. (*See* Doc. 101, Amended Order of Consolidation, ¶3). This Report and Recommendation ("R&R") pertains exclusively to a motion to dismiss filed by Defendant Awareness Technologies ("Defendant" or "Awareness") in Case No. 1:12-cv-629; therefore, this R&R is filed solely in the above captioned case.[1]

I. Procedural Background

Plaintiff Javier Luis, proceeding *pro se*, initiated this litigation in Florida by filing two separate complaints against various Defendants in both state and federal courts. Plaintiff's earlier filed state case was subsequently removed by Defendants to federal

[1]A prior R&R that pertained to dispositive motions in Case No. 1:12-cv-629 was filed in the record of Lead Case No. 1:11-cv-884, but that R&R was filed prior to the date of the Court's Amended Order of Consolidation. The prior R&R promised that the instant R&R would be filed on the remaining motion to dismiss in Case No. 12-cv-629 "as soon as practicable." (Lead Case No. 1:11-cv-884, Doc. 46 at 5). The Amended Order of Consolidation clarified that different filing rules apply to documents that pertain to

Dockets.Justia.com

court, and the two "nearly identical" cases were consolidated by the presiding district judge in Florida. (Doc. 17). On August 20, 2012, United States District Judge Virginia Hernandez granted the motions of several Defendants to transfer Plaintiff's case from Florida to this district, based upon improper venue in Florida, and the existence of a first-filed and closely related case in this Court. (Doc. 63, referring to Case No. 11-cv-884).

On August 28, 2012, a few days after transfer of the case to this Court, Defendant Awareness Technologies filed a motion to dismiss for failure to state a claim. (Doc. 68). That motion was rendered moot when Plaintiff filed an Amended Complaint. Defendant Awareness Technologies therefore filed the instant (second) motion to dismiss Plaintiff's Amended Complaint on September 21, 2012. (Doc. 77). Plaintiff filed a response to that motion, to which Defendant filed a reply. (Docs. 91, 95). With leave of Court, Plaintiff filed a sur-reply. (Doc. 97).

In his amended complaint, Plaintiff alleges that Defendant Awareness Technologies ("Awareness") is a software "maker" in Los Angeles, California, that is responsible for all "marketing and production" of a computer software product called "WebWatcher." (Doc. 39, ¶12). Plaintiff alleges that Defendant Awareness violated federal and state wiretapping laws when other individual defendants – unaffiliated with Awareness - purchased and installed WebWatcher software on a home computer in Ohio, for the purpose of permitting Joseph Zang to conduct electronic surveillance of his

---

dispositive matters.

then-wife, Cathy Zang.[2] Although Plaintiff alleges that he has never met Cathy Zang in person, he alleges that he virtually met her, via a "Metaphysics" internet chat room, in January or February 2009 (Doc. 39, ¶15). Shortly thereafter, Plaintiff alleges that he began to have "daily" communications, in the course of a "caring relationship" with Ms. Zang via the telephone and computer. (*Id*., ¶19-20).

Plaintiff alleges that Defendant Awareness "intentionally targets their product at spouses in their marketing campaigns- enticing them with the lure of finding out *everything* that goes on in the targeted computer's private accounts," in a manner that goes "far beyond…the legal monitoring of children and employees." (Doc. 39, Amended Complaint, ¶96). Plaintiff alleges that Awareness "knew or should have known that their powerful and potentially dangerous product needed to have more stringent measures built in against illegal interception of communications," and that Defendant is "therefore guilty of negligence and product liability in that its product was unsafely put in the hands of consumers who [Awareness] knew or should have known would use it for illegal purposes, and targeted…this behavior in their marketing campaigns." (*Id*.). In the same paragraph of the Amended Complaint, Plaintiff references an alleged settlement agreement between the Federal Trade Commission and a different company (non-party CyberSpy, LLC) concerning what Plaintiff alleges to be similar marketing practices for a similar product called "RemoteSpy."

With respect to Defendant's software product, Plaintiff alleges that his own computer (in Florida) "may have been infected" with spyware, through Plaintiff's internet

[2]Joseph Zang is one of the individually named Defendants, but Cathy Zang is not.

communications with Cathy Zang. (*Id.* at ¶81). Plaintiff alleges that his own oral, email, and instant message communications with Ms. Zang were wrongfully intercepted by Defendant Joseph Zang, both through the use of WebWatcher software, and via other audio and video recording devices. (*See id.,* ¶58-59).

Plaintiff alleges that Defendant Awareness (along with multiple other defendants), violated both the federal Wiretap Act and comparable Ohio and Florida state laws, by intercepting Plaintiff's oral and electronic communication, that all Defendants invaded his privacy and conspired to invade his privacy, that all Defendants collectively committed multiple violations of state common law. As a result Plaintiff claims entitlement to both monetary damages and injunctive relief against all Defendants.

II. Analysis

Awareness has moved to dismiss all claims against it pursuant to Rule 12(b)(6), for failure to state a claim. Defendant primarily argues that WebWatcher does not "intercept" any communications, such as that term consistently has been defined under the federal Wiretap Act and parallel state statutes. Additionally, Defendant argues that as a mere manufacturer, it cannot be held liable under any of the theories asserted by Plaintiff for the alleged wrongful use of its software product. Last, Defendant contends that Plaintiff's allegations fail to state a claim under any of the asserted common-law theories, including but not limited to invasion of privacy, bullying and harassment, civil conspiracy, intentional and negligent infliction of emotional distress, conversion, unjust

enrichment, aiding and abetting and defamation.

A. Standard of Review

Under Rule 8 of the Federal Rules of Civil Procedure, a plaintiff need only plead "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). However, in recent years, the Supreme Court has brought greater focus to that pleading standard, holding first in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 563, 127 S.Ct. 1955, 1969 (2007) that the "famous" no-set-of-facts formulation "has earned its retirement" and instituting a new standard that a complaint must contain facts sufficient to "state a claim to relief that is plausible on its face" *Id.* In *Ashcraft v. Iqbal*, 556 U.S. 662, 129 S.Ct. 1937 (2009), the Supreme Court explained: "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. at 678.

Under *Iqbal*, a trial court evaluating a complaint must cipher out "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements" from legal conclusions that are supported by factual allegations. *Id*. The first step is to identify the elements of the plaintiff's claim, in order to determine which allegations are mere legal conclusions, as opposed to factual allegations entitled to the "assumption of truth." *Id*. at 679 ("We begin...by identifying the allegations in the complaint that are not entitled to the assumption of truth"). To survive a Rule 12(b)(6) motion to dismiss, a plaintiff must provide more than "labels and conclusions, and a formulaic recitation of the elements of a cause of action." *Twombly*, 550 U.S. at 555. The complaint must

contain "either direct or inferential allegations respecting all the material elements to sustain a recovery under some viable legal theory." *Lewis v. ACB Business Servs., Inc.*, 135 F.3d 389, 406 (6th Cir. 1998)(internal quotation marks and additional citation omitted).

Pro se complaints are held to a less rigorous standard than those drafted by attorneys, but the court is not required to discover or create a claim that is not pleaded. *Williams v. Curtin*, 631 F.3d 380, 383 (6th Cir. 2011); *see also Clark v. Nat'l Travelers Life Ins. Co.*, 518 F.2d 1167, 1169 (6th Cir. 1975). A plaintiff is still required to plead more than "an unadorned, the-defendant-unlawfully-harmed-me accusation." *Ashcroft v. Iqbal*, 556 U.S. at 678. Applying these standards and for the reasons that follow, the Court recommends that Defendant's motion to dismiss in this case be granted.

B. Defendant's Arguments

1. Whether WebWatcher "Intercepts" Electronic Communications

Both the Federal Wiretap Act, 18 U.S.C. §2510 et seq., and similar statutes in Ohio and Florida, currently prohibit the interception of "any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). However, when the federal wiretap law known as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 was first enacted, it was designed to protect telephone communications, not email, instant messaging ("IM"), or other forms of electronic, internet-based communication that are commonplace today. In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA") in order to extend the reach of the existing wiretap law to transmissions of electronic data by

computer. The ECPA did this through two provisions: Title I, known as the Wiretap Act, and an entirely new section in Title II, called the Stored Communications Act, *see* 18 U.S.C. §2701, *et seq*. In general, the Stored Communications Act protects communications that are "stored" electronically on computers, but does not provide the same degree of protection as offered by Title I (the Wiretap Act). However, many courts have noted that the intersection of the two statutes is "a complex, often convoluted, area of the law." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002)(internal quotation marks and additional citations omitted).

Despite its nod to the computer age, when the ECPA was enacted in 1986, email communication was still relatively uncommon. As often happens when existing laws are used in new ways, courts have struggled to determine whether, and under what circumstances, the Wiretap Act applies to modern and ever-evolving norms of electronic communication. In short, the existing statutory scheme often appears "ill-suited to address modern forms of communication." *Id.*

The Sixth Circuit has yet to address the issue presented in this case: whether the Wiretap Act prohibits the use of software commonly known as "spyware" to obtain another person's emails and/or a record of other computer activities However, other federal courts consistently have held that a defendant's access and review of email and other electronic communications does not violate the Wiretap Act unless it is "contemporaneous" with the intended recipient's access. *See also State v. Poling*, 160 Ohio Misc.2d 84 (Ohio Mun. 2010). The courts adopting this holding have reasoned that the term "intercept" as defined in the Wiretap Act requires interception of the

communication either *before* it reaches the intended recipient, or "contemporaneous with transmission" – but not *after* it reaches that destination when presumably, the data is placed in electronic storage. *See, e.g., United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003).

As another district court within the Sixth Circuit has explained:

> The general reasoning behind these decisions is that based on the statutory definition and distinction between "wire communication" and "electronic communication," the latter of which conspicuously does not include electronic storage, Congress intended for electronic communication in storage to be handled solely by the Stored Communications Act. This interpretation is reasonable and consistent with the language of the statute.

Bailey v. Bailey, 2008 WL 324156 at *4 (E.D. Mich., Feb. 6, 2008).

In light of this historical context, including the differences between the Wiretap Act and the Stored Communications Act, the undersigned turns to the issue at hand. According to an affidavit filed by the CEO of Defendant Awareness, the software at issue in this case is designed to record "various activities…such as e-mails sent *and received*, websites visited, keystrokes typed and *transcripts of online chats*." (Doc. 77-1 at ¶5, emphasis added). Without defining the time frame in which this event occurs, the CEO further avers that the software sends all of the recorded activity over the internet to "an online account," where it can be viewed at a later time. (*Id*. at ¶¶6-7).

Defendant relies on several cases involving "keylogger" software to argue that such software has been held not to "intercept" electronic communications under the Wiretap Act, because it only accesses "stored" data. For example, in *Bailey* as in the instant case, a husband surreptitiously installed keylogger software on his then-wife's

computer. The court granted summary judgment to the husband on the Wiretap Act and comparable Michigan state law claims, based upon evidence that "the key logger only allowed Defendant Bailey to learn [email and IM account] passwords, which were used to [later] access and copy Plaintiff's email and messages," without any "contemporaneous" interception of those messages. *Id*. at *5. By contrast, the court denied summary judgment on plaintiff's claims under the Stored Communications Act and for invasion of privacy. *Accord Miller v. Meyers*, 766 F. Supp.2d 919, 923-924 (W.D. Ark 2011)(holding that husband's secret use of keylogger program to access then-wife's email account violated Stored communications Act, but not the Wiretap Act, in absence of "contemporaneous" interception).

In response to Defendant's motion, Plaintiff argues from a policy standpoint that what defines an "intercept" under the Wiretap Act has been "greatly misunderstood and misinterpreted by jurists and attorneys alike." (Doc. 91 at 4). Plaintiff urges expansion of the reach of the Wiretap Act, citing *United States v. Councilman*, 418 F.3d 67, 83 (1st Cir. 2005)(*en banc*). However, *Councilman* is not on point.

Councilman focused on the determination of whether obtaining another's email while that email is in "transient electronic storage" during the moments of transmission constitutes an "interception" under the Wiretap Act, as opposed to merely accessing data from "storage." After an elaborate explanation of the process by which email is electronically transmitted from computer to computer in briefly stored "packets" of information, the First Circuit rejected the Defendant's argument that his criminal indictment under the Wiretap Act could not stand because an email message "cease[s]

to be an 'electronic communication' during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage." *Id.* at 79. Notably, *Councilman* expressly declined to address "the question of whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient, or instead, extends to an event that occurs after a message has crossed the finish line of transmission…." *Id.* at 80.

Plaintiff more persusively cites *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010) and *Shefts v. Petrakis*, 758 F. Supp.2d 620 (C.D. Ill., 2010). In *Szymuszkiewicz*, the Seventh Circuit affirmed the criminal conviction of a defendant who had secretly programmed his supervisor's email program to duplicate and send to him "within the same second" all emails that were sent to her. *Id*., 622 F.3d at 704. In affirming the conviction, the court rejected the defendant's argument that his actions did not violate the Wiretap Act because he did not "intercept" the emails contemporaneously. The court held that although the emails may have been forwarded to the defendant while in temporary "storage," the process would have been completed so close in time that it was "contemporaneous by any standard." *Id*. at 706. Similarly, in *Shefts*, the court held that software that discreetly logs copies of text messages for later viewing constitutes an "interception" under the Wiretap Act.

Based upon *Szymuszkiewicz* and *Shefts*, as well as the reasoning of a third recent case within the Sixth Circuit, Plaintiff urges this Court to conclude that Awareness violated the Wiretap Act because its software was used to route "a copy of an email…back through the internet to a third party's email address." *See Klumb v.*

Goan, 884 F. Supp.2d 644 (E.D. Tenn., 2012). For the same reason, Plaintiff distinguishes *Steiger*, the seminal "contemporaneous" case on which Defendant relies.[3] Unlike *Steiger*, Plaintiff alleges that the software at issue here transmits the captured data through the internet to a remote location.

Both Plaintiff and Defendant also cite *United States v. Barrington*, 648 F.3d 1178 (11th Cir. 2011), a case in which university students who installed keylogger software on registrar computers in a grade-changing scheme were convicted under the Wiretap Act. The evidence demonstrated that the keylogger software had been configured to send the captured data to two email addresses associated with the Defendant and his co-conspirators. *Id.* at 1201. Nevertheless, the Eleventh Circuit held that a sentencing enhancement under the Wiretap Act could not stand, because "use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not *at that time* being transmitted *beyond* the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce)." (*Id*. at 1202, emphasis added). Although the court recognized that the keylogger software at issue "*could* be used to contemporaneously capture information or signals being transmitted beyond the user's computer," the Government had failed to point to evidence that the keylogger software had that capacity and was actually used by

[3]In *Steiger*, the Eleventh Circuit upheld the Defendant's child pornography conviction, holding that the Government had not violated the Wiretap Act when it used incriminating evidence from a private citizen who "hacked" into the Defendant's computer and accessed pornographic images stored on the hard drive. The court held as a matter of first impression that the Act applies only to "real-time interception of electronic communications." *Id*., 318 F.3d at 1049. In so doing, the court acknowledged that its new "contemporaneous" interpretation would mean that "very few seizures of electronic communications from computers will constitute 'interceptions,'" "unless some type of automatic routing software is used." *Id.* at 1050 (additional citations omitted).

defendants in that manner. *Id.* at 1203. Therefore, based on its conclusion that proof of a "contemporaneous" interception was not clearly demonstrated, the court rejected the sentencing enhancement imposed by the trial court. However, the court ultimately upheld the same enhancement under a different guidelines provision. *Id.*

The Defendant further relies on *Rene v. G.F. Fishers, Inc*., 817 F. Supp.2d 1090 (S.D. Ind 2011), in which the court held that a defendant's use of keylogger software did not violate the Wiretap Act where the software only captured the transmission of keystrokes internally between the local computer and its attached keyboard, a transmission that the court reasoned "required no connection with interstate or foreign commerce to reach its destination." *Id*., at 1094; *accord United States v. Ropp*, 347 F. Supp.2d 831 (C.D. Cal. 2004). The undersigned respectfully disagrees with *Rene* and *Ropp* to the extent that those two cases could be read as supporting an overly narrow interpretation of "electronic communications." Instead, the undersigned agrees that "it is the communication itself that must affect commerce, not the means of interception." *Shefts v. Petrakis*, 2012 WL 4049484 at *6 (C.D. Ill. Sept. 13, 2012)(noting that the definition of "intercept" does not require any effect on interstate commerce). In any event, the software at issue requires an on-line account for functionality, thereby creating the requisite connection with interstate commerce.

As in *Shefts*, the undersigned draws a distinction between "keylogger" software that does not simultaneously transmit the user's data over the internet, and the type of "spyware" (whether or not termed "keylogger" software)[4] that is "web-based." *See id*., at

[4]Traditionally, "keylogger" software refers to software that records keystrokes made by the user of

*8-9 (holding that spyware that contemporaneously transmitted "screen shots" of computer activity to a remote location violates the Wiretap Act). Unlike the cases relied upon by Defendant, the facts presented involve immediate (or close to immediate) interception of keystrokes on a computer and transmission to the "spy's" electronic account. For that reason, Plaintiff asserts that the use of Defendant's keylogging software satisfies the definition of an "intercept[ion]" under the Wiretap Act.

In its reply memorandum, Defendant attempts to distinguish WebWatcher from the "eBlaster" software discussed in *Klumb v. Goan*, because that software automatically routed the former husband's emails to the former wife's account in "a blink of an eye," whenever the husband opened his emails. *Id.* Defendant protests that its product "does not have this functionality," citing its CEO's affidavit. However – aside from confirming that WebWatcher forwards the recorded activity to an "online account," for "later" review - the affidavit filed by Defendant is wholly silent regarding *when* WebWatcher forwards the recorded information to the secret account. Plaintiff argues that the marketing materials for WebWatcher imply that the forwarding occurs very close to real-time. In addition, in holding that spyware can violate the Wiretap Act if it transmits captured or recorded information over the internet, the court in *Klumb v. Goan* suggested that the timing of that secret transmission is irrelevant:

> Whether the email is rerouted within a "blink-of-an-eye" is not of primary importance to the router switching analysis. If it were, a smart

---

the computer on which the software is installed. However, Plaintiff alleges that Defendant's software does more than merely record keystrokes, because it also saves and/or records entire IM conversations and other "screen" data. A portion of the recorded data originated from Plaintiff, from a remote computer on which WebWatcher was (presumably) not installed. The affidavit submitted by the CEO confirms that much broader data than keystrokes is captured by the spyware at issue.

> programmer could simply program the software to wait a certain amount of time before rerouting the email through the internet to the unauthorized third party. The point is that a program has been installed on the computer which will cause emails sent at some time in the future through the internet to be rerouted automatically through the internet to a third party address when the intended recipient opens the email for the first time.

884 F. Supp.2d at 661. While *Klumb v. Goan* implies a rethinking of the "contemporaneous" standard, the cases that most narrowly construe that requirement are from other circuits and are not controlling. By contrast, *Klumb* is persuasive as a recent civil case published within this circuit. For that reason, Defendant's contention that no "intercept" occurred under the Wiretap Act is rejected.

2. Whether Defendant Awareness Can Be Held Civilly Liable Under the Act

In its reply, Defendant additionally argues that, even if this Court were to agree with Plaintiff's interpretation of "intercept" under the Wiretap Act, Plaintiff's claims should be dismissed on grounds that Awareness – as the manufacturer – did not itself "intercept" Plaintiff's communications with Ms. Zang. As Defendant puts it, "Smith & Wesson is not legally responsible for a person's unlawful use of its guns." (Doc. 95 at 2). *But see Gootee v. Colt Industries, Inc*., 712 F.2d 1057 (6th Cir. 1983)(holding that in product liability action grounded on negligence, gun manufacturer could be held liable if it failed to guard against dangers posed by foreseeable misuse). The Court agrees that Defendant itself cannot be deemed to have "intercepted" any of Plaintiff's communications. However, Plaintiff's *pro se* pleadings must be liberally construed.

Plaintiff advocates for a theory of liability based upon prosecutions of other manufacturers of spyware/software. Plaintiff points first to a lawsuit filed by the Federal

Trade Commission against a company called CyberSpy, the manufacturer of a product Plaintiff claims to be virtually identical to WebWatcher. Plaintiff alludes to the parties' terms of settlement to argue that Defendant Awareness should be found to illegally market WebWatcher. Second, Plaintiff points to the existence of a criminal indictment against the software manufacturer of a product called "Loverspy."

Defendant protests that neither a settlement to which it was not a party, nor the mere existence of a criminal indictment against a different manufacturer, has any bearing on this case. Defendant is accurate, to the extent civil liability under the Wiretap Act depends wholly on whether Congress intended to provide a private right of action for the violation alleged by Plaintiff.

Plaintiff's amended complaint generally references the civil remedies available under the Wiretap Act, which not only prohibits individuals and entities from surreptitiously intercepting electronic communications, but also criminalizes the "[m]anufacture, distribution, possession, and advertising" of "devices" that can be used for interception. *See* 18 U.S.C. §2512. At least for purposes of the pending motion to dismiss, Plaintiff has alleged conduct by Defendant that could be interpreted as a violation of 18 U.S.C. §2512. In fact, in his sur-reply, Plaintiff argues specifically that the criminal prohibition against advertising any device for "surreptitious interception" authorizes his civil claims in this case.

Contrary to Plaintiff's theory, courts in the Sixth Circuit universally have held that 18 U.S.C. §2520(a) does not provide a private right of action for criminal violations of 18

U.S.C. §2512.[5] *See, e.g., Bailey*, *supra* at *7 (citing *DIRECTTV, Inc. v. Treworgy*, 373 F.3d 1124 (11th Cir. 2004)); *DIRECTTV, Inc. v. McCool*, 329 F. Supp.2d 1025 (M.D. Tenn. 2004); *DIRECTTV, Inc. v. Smith*, 2004 WL 1247665 (S.D. Ohio, March 31, 2004).

Furthermore, Plaintiff's claims against Defendant fail as a matter of law, because the provision of the Wiretap Act that provides for a private civil remedy, 18 U.S.C. §2520(a), limits the category of viable defendants to those individuals or entities that have "intercepted, disclosed, or intentionally used [a device] in violation of this chapter." Although manufacturers are not explicitly excluded, the choice of verbs used in the plain language of the statute makes clear that the statute "does not contemplate imposing civil liability on software manufacturers and distributers for the activities of third parties." *Potter v. Havlicek*, 2008 WL 2556723 at *7 (citing *Searcy v. Microsoft Corp*., 2005 WL 1153114 at *1 (M.D. Fl. May 4, 2005). For the same reasons, Defendant's motion to dismiss Plaintiff's parallel claims under state law should be granted.

3. Common Law Claims

Plaintiff's common law claims against Defendant also should be dismissed. Plaintiff argues that those claims, which include invasion of privacy, conspiracy to commit invasion of privacy, civil conspiracy, bullying and harassment, intentional and negligent infliction of emotional distress, conversion and unjust enrichment, and aiding and abetting, all apply to the Defendant's actions in manufacturing and marketing its WebWatcher product. (Doc. 91 at 18). Plaintiff asserts that "only discovery can disclose the necessary facts relating to the extent of Awareness's guilt and liability."

[5]Cases that hold to the contrary, cited by Plaintiff in his sur-reply, represent a minority view not

(*Id.*).

Plaintiff's argument puts the cart before the horse. In order to proceed with his claims against Defendant, the *Iqbal* standard requires Plaintiff to allege facts that are sufficient to state a claim. As Defendant points out, Plaintiff does not allege that Defendant Awareness had any personal knowledge of Mr. Zang's intended use of its WebWatcher product, either at the time Mr. Zang purchased the product, or at any time thereafter. Even the most liberal construction of Plaintiff's amended complaint finds no allegation that Awareness had any agreement with Mr. Zang or with any other named Defendant to intercept Plaintiff's communications. In short, there are no simply no factual allegations on which Defendant Awareness could be held liable for invading Plaintiff's privacy, or for engaging in any type of "conspiracy" to invade Plaintiff's privacy. Likewise, no plausible allegations are included in the amended complaint that could support any of the remainder of Plaintiff's common law claims against Awareness.

III. Conclusion and Recommendation

For the reasons discussed herein, **IT IS RECOMMENDED THAT**:

The motion of Defendant Awareness Technologies to dismiss all claims against it (Doc. 77) should be **GRANTED**. Plaintiff Luis's claims against that Defendant alone in Civil Case No. 1:12-cv-629 should be dismissed.

s/ Stephanie K. Bowman
Stephanie K. Bowman
United States Magistrate Judge

---

adopted by courts within this circuit.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

v.

JOSEPH ZANG, et al.,

Defendants.

Case No. 1:12-cv-629
Dlott, J.
Bowman, M.J.

NOTICE

Pursuant to Fed. R. Civ. P 72(b), any party may serve and file specific, written objections to this Report and Recommendation ("R&R") within **FOURTEEN (14) DAYS** of the filing date of this R&R. That period may be extended further by the Court on timely motion by either side for an extension of time. All objections shall specify the portion(s) of the R&R objected to, and shall be accompanied by a memorandum of law in support of the objections. A party shall respond to an opponent's objections within **FOURTEEN (14) DAYS** after being served with a copy of those objections. Failure to make objections in accordance with this procedure may forfeit rights on appeal. *See Thomas v. Arn,* 474 U.S. 140 (1985); *United States v. Walters,* 638 F.2d 947 (6th Cir. 1981).