UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

THOMAS FARRELL HAYES,	)	
	)	
Plaintiff,	)	Case No. 1:08-cv-187
v.	)	
	)	*Judge Edgar*
SPECTORSOFT CORPORATION,	)	
	)	
Defendant.	)	

MEMORANDUM

Plaintiff Thomas Hayes originally brought this action for alleged violations of the federal Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, along with several state statutory and common law claims in the Circuit Court of Hamilton County, Tennessee. [Court Doc. No. 1-1, Complaint]. Defendant SpectorSoft Corporation ("SpectorSoft") removed the action to this court on the basis of complete diversity of the parties pursuant to 28 U.S.C. § 1332 and on the basis of this court's original jurisdiction pursuant to 28 U.S.C. § 1331. [Court Doc. No. 1]. SpectorSoft now moves for summary judgment dismissal of all of Plaintiff's claims against it. [Court Doc. No. 10]. Plaintiff opposes the motion. [Court Doc. No. 14]. The court has reviewed the record, the arguments of the parties, and the relevant law and has determined that SpectorSoft's motion will be **GRANTED**.

I. Background

The parties do not appear to disagree upon most of the relevant material facts at issue in this action. The facts viewed in the light most favorable to the Plaintiff are as follows. Plaintiff's Complaint alleges that around October 29, 2005 either Mary Jo Davis or Alice Hayes, Plaintiff's former wife, purchased a software program called the "Spector Professional Edition

for Windows" or "Spector Pro." Complaint, ¶ 5. Around November 10, 2005 either Ms. Davis or Ms. Hayes installed the "Spector Pro" software on Plaintiff's laptop computer in Hamilton County, Tennessee. *Id.* at ¶ 6. Plaintiff alleges that around November 12, 2005 either Ms. Davis or Ms. Hayes purchased a software program called "eBlaster for Windows" from SpectorSoft and that on November 18, 2005 one of the two women installed the software on his laptop. *Id.* at ¶¶ 7-8. Plaintiff contends that following the installation of these software programs the software "recorded and transmitted over the Internet all chat conversations, instant messages, e-mails sent and received, and the websites visited by Plaintiff whenever he used his laptop computer. . . . Upon receipt of such electronic communications, Spectorsoft re-transmitted such electronic communications to Mary Jo Davis in Silver Spring, Maryland." *Id.* at ¶¶ 8-9. Plaintiff alleges that Ms. Davis and Ms. Hayes used and disclosed or endeavored to use or disclose some of the information gained from obtaining access to Plaintiff's Internet usage. *Id.* at ¶ 11.

Plaintiff has submitted a report by his computer software expert, Clifton Goodgame, who described how SpectorSoft's software works. His report indicates that

> eBlaster for Windows and Spector Pro for Windows are "key logger" software programs that capture all instant messages, sent and received e-mails, web searches, online chats, file transfers, electronic data and other activity from the computer on which such programs are installed (the "target computer"). eBlaster differs from Spector Pro in that the eBlaster program has the ability to transmit the captured information from the target computer via e-mail to a location designated by the installer. This is accomplished by using an e-mailer client built into the eBlaster application and does not require the use of the e-mail account of the user of the target computer. Capture of the above-described electronic data is virtually contemporaneous with the activity on the target computer. The software is designed to permit the transmission of captured e-mails contemporaneously with the transmission of and receipt of such e-mails by the target computer or to store the e-mails and send them later. In addition, the eBlaster software generates "Activity Reports" which aggregate data regarding activities conducted on the target computer. Such "Activity Reports" are periodically transmitted via e-mail to a location designated by the installer. Such software operates surreptitiously in

> that it can capture the above-described electronic data without the knowledge of the user of the target computer on which it has been installed. The eBlaster program is designed to retransmit such electronic data from the target computer to another location via e-mail without informing the user of the target computer on which it is operating.

[Court Doc. No. 14-1, Expert Report of G. Clifton Goodgame ("Goodgame Report"), p.2].

The parties dispute whether SpectorSoft knew of the illegal use of the SpectorSoft software to gain access to Plaintiff's private laptop communications. Plaintiff alleges that SpectorSoft knew or should have known about such usage. Complaint, ¶ 12. SpectorSoft contends that it "did not know Plaintiff's wife and sister were misusing the software. SpectorSoft did not know who owned or predominantly used the particular computer on which SpectorSoft software was installed. Neither did SpectorSoft know anything about what consent had been obtained regarding monitoring or installation." [Court Doc. 10-1, Affidavit of Ronald L. Chesley, Jr. ("Chesley Aff."), ¶ 14].

Plaintiff asserts that Ms. Davis and Ms. Hayes, neither of whom is a party to this action, violated his right to privacy and violated the ECPA, a part of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 *et seq.* Complaint, ¶ 13. Such behavior, Plaintiff alleges, caused him severe mental anguish and humiliation. *Id.* at ¶ 14.

Plaintiff asserts several vaguely defined causes of action against SpectorSoft for its role in allowing his personal computer usage to be captured by Ms. Davis and Ms. Hayes. He alleges that SpectorSoft "aided and abetted" Ms. Davis and Ms. Hayes in the violation of his statutory and common law rights. He asserts that SpectorSoft violated 18 U.S.C. § 2511(3)(a) and Tenn. Code Ann. § 39-13-601(c)(1) by "intentionally divulging the contents of electronic communications by Plaintiff and electronic communications to Plaintiff to persons other than the

addressee or intended recipient of such electronic communications." Complaint, ¶ 16. The Complaint also asserts that SpectorSoft was

> negligent in the manufacture, construction and design of its Spector Pro and eBlaster software programs, in its regulation of the use of such software programs by Mary Jo Davis and Alice Suzanne Hayes, and in its failures to warn Plaintiff of the possible illegal use of such software programs. Such software programs are "defective" and "unreasonably dangerous" within the meaning of Tennessee law.

Complaint, ¶ 17. Plaintiff's Complaint seeks damages and punitive damages.

SpectorSoft's co-founder and vice-president, Ronald Chesley, Jr., has filed an affidavit in support of SpectorSoft's position that explains how the SpectorSoft software at issue in this case works. Chesley Aff. Mr. Chesley provided information regarding the primary purposes of SpectorSoft's software:

> This software is designed to make it easier for parents to monitor their children's Internet use and for employers to monitor their employees' Internet use. The vast majority of Spectorsoft's customers use the software for those two purposes, and Spectorsoft software has literally helped save children from child predators. It has also been used to save businesses from employee malfeasance and greatly improve workplace productivity. It is also used by law enforcement and probation personnel. Additionally, some people use the software as an easy personal archiving system.

Chesley Aff., ¶ 5. Mr. Chesley also testified in his affidavit that "SpectorSoft's license agreement requires the software installer to agree to install the software only on a computer that he or she owns or on a computer on which he or she has been given explicit permission to install the software. The software cannot be installed without the installer "clicking" his or her agreement to those terms." *Id.* at ¶ 10. Exhibit 2 filed with Mr. Chesley's affidavit demonstrates a printed version of the software licensing agreement. The installer of the software must click a box labeled "yes" below the following language in order to use the software:

> You agree to inform anyone who [sic] you may record that their Internet and PC

> activity is subject to being recorded and archived.
> You agree to install this software ONLY on a computer that you own or on a computer which you have been given explicit permission to install. You agree to NOT install this software on any computer you do not own or on any computer you have not been given explicit permission to install.
> Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install Spector, you must accept this agreement.

[Court Doc. 10-1, p. 25; *see also*, pp. 29-30]. Mr. Chesley's affidavit also explains the process by which the SpectorSoft servers route an individual e-mail to its final determined destination as provided by the purchaser and/or installer of the software:

> More than 800,000 messages travel through SpectorSoft's communications servers on an average day. The messages are only in the server for a fleeting moment. They are not opened or stored in the server. Their content [sic] remain a complete secret to SpectorSoft. The server simply serves as an intermediate part of a relay system as the message travels from an originating point to an end point. As a communication enters the server, the server immediately begins to relay it forward. . . . At no point are the contents of the communication "divulged" while in transmission on SpectorSoft's server any more than they are divulged while in transmission on AOL's server. . . . SpectorSoft does not and cannot monitor the more than 800,000 emails that travel through its servers on the average day. SpectorSoft never sees the content of any such emails. Even if SpectorSoft desired to review email content (which it does not), the manpower necessary to review 800,000 emails a day would be enormous and cost-prohibitive. . . . Moreover fundamentally, even if emails were opened and read, that would still tell SpectorSoft nothing about whether the sending or forwarding of an email was authorized or was supposedly wrongful in some way. Even if Spectorsoft reviewed the emails, such review would not inform Spectorsoft of whether an email was obtained with proper consent or under proper authority as a parent, employer, government representative or other person.

Chesley Aff., ¶¶ 20-23.

During a deposition of Mr. Chesley that related to an action between Plaintiff and Ms. Hayes, Mr. Chesley testified that SpectorSoft previously marketed its software to spouses, but that the company no longer did so. [Court Doc. Nos. 14-2 through 14-4, Deposition of Ronald

L. Chesley, Jr. ("Chesley Dep."), p. 83]. Mr. Chesley indicated that "[i]n the past there were marketing messages that indicated the husband and wife could monitor the activities of their computer using our products," but he testified that such marketing was discontinued around 2003. *Id.* at 84. Plaintiff submits exhibits to the Goodgame Report which indicate that his expert, Clifton Goodgame, was able to locate websites that specifically marketed SpectorSoft's software to spouses who desired to access private communications of partners whom they suspected of infidelity. *See* [Court Doc. No. 14-1, pp. 12-16].

Plaintiff claims that SpectorSoft has violated the ECPA by providing Ms. Davis and Ms. Hayes with software that enabled them to gain access to Plaintiff's private communications. He also alleges that SpectorSoft's activities have violated his state law rights, including his rights under the Tennessee Wiretap Act ("TWA"), Tenn. Code Ann. § 39-13-601(c)(1). He brings claims of aiding and abetting and general negligence, as well as a claim for liability under Tennessee's Products Liability Act, Tenn. Code Ann. § 29-28-105(b).

II. Standard of Review

Summary judgment is appropriate if there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c). The burden is on the moving party to show conclusively that no genuine issue of material fact exists, and the Court must view the facts and all inferences to be drawn therefrom in the light most favorable to the nonmoving party. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986); *Morris v. Crete Carrier Corp.*, 105 F.3d 279, 280-81 (6th Cir. 1997); *60 Ivy Street Corp. v. Alexander*, 822 F.2d 1432, 1435 (6th Cir. 1987).

Once the moving party presents evidence sufficient to support a motion under Fed. R.

Civ. P. 56, the nonmoving party is not entitled to a trial merely on the basis of allegations. The nonmoving party is required to come forward with some significant probative evidence which makes it necessary to resolve the factual dispute at trial. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986); *White*, 909 F.2d at 943-44; *60 Ivy Street*, 822 F.2d at 1435. The moving party is entitled to summary judgment if the nonmoving party fails to make a sufficient showing on an essential element of the nonmoving party's case with respect to which the nonmoving party has the burden of proof. *Celotex*, 477 U.S. at 323; *Collyer v. Darling*, 98 F.3d 211, 220 (6th Cir. 1996).

The judge's function at the point of summary judgment is limited to determining whether sufficient evidence has been presented to make the issue of fact a proper jury question, and not to weigh the evidence, judge the credibility of the witnesses, and determine the truth of the matter. *Anderson v. Liberty Lobby*, 477 U.S. 242, 252, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986); *60 Ivy Street*, 822 F.2d at 1435-36. "The mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient; there must be evidence on which the jury could reasonably find for the plaintiff." *Anderson*, 477 U.S. at 252; *see also Bailey v. Floyd County Bd. of Educ.*, 106 F.3d 135, 140 (6th Cir. 1997). If the Court concludes that a fair-minded jury could not return a verdict in favor of the nonmoving party based on the evidence presented, it may enter a summary judgment. *Anderson*, 477 U.S. at 251-52; *University of Cincinnati v. Arkwright Mut. Ins. Co.*, 51 F.3d 1277, 1280 (6th Cir. 1995); *LaPointe v. UAW, Local 600*, 8 F.3d 376, 378 (6th Cir. 1993).

III. Analysis

I. Claims Under 18 U.S.C. § 2511(3)(a) and Tenn. Code Ann. § 39-13-601

Plaintiff alleges that SpectorSoft has violated the federal ECPA, specifically 18 U.S.C. § 2511(3)(a). This statutory provision states:

> Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

18 U.S.C. § 2511(3)(a). Tennessee's statutory provision under the TWA, Tenn. Code Ann. § 39-13-601, is substantially similar. *See* Tenn. Code Ann. § 39-13-601(c)(1). The ECPA provides that:

> Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520(a). Such relief may include equitable and declaratory relief, damages, and attorneys' fees. *See* 18 U.S.C. § 2520(b).

The ECPA defines "electronic communication" as:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include –
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device . . .; or
> (D) electronic funds transfer information . . .

18 U.S.C. § 2510(12). The term "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic

communications." 18 U.S.C. § 2510(15). SpectorSoft admits for the purposes of its motion for summary judgment that none of the exceptions listed in paragraph (b) of 18 U.S.C. § 2511(3)(b) apply to the company, and it further admits that it provides an electronic communication service to the public. *See* [Court Doc. No. 11, p. 5]. However, it contends that it did not intentionally divulge the contents of the electronic communications while they were in transmission to someone other than an addressee or intended recipient.

The parties have not provided this court with cases that are analogous to the claims made here, and there appear to be few such recorded cases. However, several cases have discussed the meaning of the ECPA in other contexts. For example, in *Shubert v. Metrophone, Inc.*, the Third Circuit analyzed the ECPA with respect to the divulgence of cellular telephone communications. 898 F.2d 401, 403-06 (3d Cir. 1990). In discussing the required *mens rea* for a violation of 18 U.S.C. § 2511(3)(a) the Third Circuit noted:

> Congress was well aware of the vulnerability of cellular transmissions when it enacted § 2511(3)(a) which prohibits a communication service provider from intentionally divulging the contents of a communication while in transmission of that service. Yet it did not expressly provide that the mere act of the cellular transmission of a communication without scrambling or encryption was an intentional divulgence of a communication's contents.
>
> Our conclusion is buttressed by the circumstance that the Privacy Act amended sections 2510 and 2511 of the Wiretap Act to change the required *mens rea* for a violation from "willful to intentional". Pub.L. No. 99-508, § 101(f), 100 Stat. 1853 (1986); Senate Report, 1986 Code Cong. & Admin. News at 3577. This amendment was intended:
>
> > to underscore that inadvertent interceptions are not crimes under the Electronic Communications Privacy Act.
> >
> > As used in the Electronic Communications Privacy Act, the term 'intentional' is narrower than the dictionary definition of 'intentional.' 'Intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the

> causing of the result must have been the person's conscious objective. An 'intentional' state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. *Since one has no control over the existence of circumstances, one cannot 'intend' them*.

Id. at 405 (quoting Pub.L. No 99-508, § 101(f), 100 Stat. 1853 (1986); Senate Report, 1986 Code Cong. & Admin. News at 3577) (emphasis added); *See also, In re Pharmatrak Inc. Privacy Litigation*, 329 F.3d 9, 22-23 (1st Cir. 2003).

In *In re Pharmatrak, Inc. Privacy Litigation*, the First Circuit remanded the case to the district court for determination of whether the defendant company intentionally violated 25 U.S.C. § 2511(1)(a) of the ECPA. 329 F.3d 9, 22-23 (1st Cir. 2003). In discussing the meaning of the term "intentional" in the ECPA and in its legislative history, the First Circuit noted:

> Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the ECPA. An act is not intentional if it is the product of inadvertence or mistake. There is also authority suggesting that liability for intentionally engaging in prohibited conduct does not turn on an assessment of the merit of a party's motive. That is not to say motive is entirely irrelevant in assessing intent. An interception may be more likely to be intentional when it serves a party's self-interest to engage in such conduct.

329 F.3d at 23.

On remand the district court discussed whether a web-monitoring corporation's gathering of certain personal information of internet users for use by pharmaceutical companies was intentional in violation of 25 U.S.C. § 2511(a)(1) of the ECPA. *In re Pharmatrak, Inc. Privacy Litigation*, 292 F.Supp.2d 263 (D. Mass. 2003). The court analyzed whether the inadvertent transmission of users' personal information to the web-monitoring company's server constituted an "intentional interception" within the meaning of 18 U.S.C. § 2511(a)(1):

> Defendants have provided undisputed descriptions of how pieces of personal information were transmitted to their servers. According to the Defendants, programming errors made by three different third parties caused these transmissions. . . . Because the transmissions were the result of circumstances beyond their control, Defendants argue that they could not have intended to collect the information. Their assertion is supported by the First Circuit's definition of intentional: "Since one has no control over the existence of circumstances, one cannot 'intend' them."
>
> Plaintiffs do not dispute the descriptions of how the information was transmitted. But they attempt to circumvent the conclusion by arguing that, because [the defendant] did not implement certain safeguards to prevent these sorts of transmissions, it must have intended to collect personal data. It is beside the point, however, whether such safeguards existed and whether they could have been used to prevent these transmissions. Even assuming that they did exist and could have been used, Pharmatrak would at most be liable under a theory of negligence, or even gross negligence. Neither is sufficient to satisfy the specific intent requirement under the [ECPA].

Id. at 267-68. The court granted the web-monitoring company's motion for summary judgment due to the plaintiffs' failure to prove that any interception of personal data was intentional. *Id.* at 268.

Federal courts have upheld license agreements or contracts which require a purchaser to accept certain terms of use prior to accessing the right to use computer software. *See e.g.*, *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996) (noting that "[s]hrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general . . .). In *Zeidenberg* the Seventh Circuit determined that an end-user license agreement accompanying software was enforceable where the purchaser was only able to use the software "after the software splashed the license on the screen and would not let him proceed without indicating acceptance." 86 F.3d at 1452. *See also, Moore v. Microsoft Corp.*, 741 N.Y.S.2d 91, 92 (N.Y. App. Div. 2002) (determining that end user licensing agreements were valid where their terms were "prominently displayed on the program user's computer screen

before the software could be installed").

In this action Mr. Chesley testified in his affidavit that:

> a completely separate screen appears during installation of the software which requires, as a prerequisite to installation, the installer to "agree to install [the software] only on a computer that I own" and to inform any computer user that the software has been installed and that their usage is subject to monitoring. Again, the installer must click his or her agreement in order to proceed with installation. . . . Thus, the installer of SpectorSoft software is faced with these use restrictions on two separate occasions while installing the software, and installation cannot proceed without the installer's agreement to those restrictions.

Chesley Aff., ¶ 11. Mr. Chesley further asserted that "SpectorSoft does not and cannot monitor the more than 800,000 emails that travel through its servers on the average day. SpectorSoft never sees the content of any such emails." *Id.* at ¶ 23.

With respect to the specific allegations at issue in this case, Mr. Chesley contends that

> SpectorSoft did not know Plaintiff's wife and sister were misusing the software. SpectorSoft did not know who owned or predominantly used the particular computer on which SpectorSoft software was installed. Neither did SpectorSoft know anything about what consent had been obtained regarding monitoring or installation. . . . Based on all that SpectorSoft knew, the software was being used properly, in accordance with the terms of the license agreement, and just as it is typically used – as protection for children or protection for businesses.

Chesley Aff., ¶ 14.

Plaintiff does not attempt to rebut SpectorSoft's evidence demonstrating a lack of intent to divulge Plaintiff's private communications. Instead, Plaintiff attempts to argue that SpectorSoft intended to divulge private communications because other non-SpectorSoft websites marketed SpectorSoft's software to spouses who suspected their partners of cheating. *See* [Court Doc. No. 14-1]. However, SpectorSoft indicated that it no longer markets its software to spouses. Chesley Dep., pp. 83-84. Plaintiff's only other evidence of intent is found in unsupported allegations in his Complaint. There is no other substantive, probative evidence

creating a genuine issue of material fact regarding whether SpectorSoft intended to divulge Plaintiff's private communications.

In addition, SpectorSoft had every right to expect that its software should be used in accordance with the licensing agreement it provides. *See e.g., ProCD, Inc.*, 86 F.3d 1447. Such agreements are enforceable when they require a purchaser to click on messages such as "Yes" or "I agree" in order to install software. *Id.* at 1452. Moreover, Plaintiff has offered no evidence to contradict SpectorSoft's evidence indicating that it never read Plaintiff's electronic communications and that it does not monitor all of the electronic communications that cross over its server on a daily basis. Thus, SpectorSoft's role in divulging Plaintiff's private communications is akin to the defendants' role in divulging private information in *In re Pharmatrak, Inc. Privacy Litigation.* 292 F.Supp.2d at 267-68. Its role in divulging communication pertaining to the Plaintiff might constitute negligence, but SpectorSoft's actions do not rise to the level necessary to show "intentional" disclosure of information as required under the ECPA. There is no indication that it was SpectorSoft's "conscious objective" to disclose Plaintiff's private communications. *See Shubert v. Metrophone, Inc.*, 898 F.2d at 403-06.

Plaintiff provides this court with no cases applying the ECPA to facts analogous to the facts found here. And this court has located no such authority. To hold Defendant liable under the ECPA for Ms. Hayes' and Ms. Davis' conduct, of which it was unaware and which breached the terms of its licensing agreement, could result in several unintended results. Plaintiff suggests that SpectorSoft should have provided information to him as a computer user informing him and reminding him that his computer was being monitored. Such notices would reduce the efficacy

of the legitimate uses for SpectorSoft software, such as employee and parental monitoring. Further, the failure to implement such safeguards merely suggests negligence, rather than intentional disclosure of private communications. *See In re Pharmatrak, Inc. Privacy Litigation*, 292 F.Supp.2d 267-68. Requiring SpectorSoft to monitor all of the communications that traverse its servers would also be unwieldy, and as SpectorSoft contends, even if it did review all of the electronic communications, it would still be unclear to SpectorSoft whether those communications resulted from illegal usage of its software. *See* Chesley Aff., ¶¶ 21-23. Although there is authority relating to the illegal interception of spousal communication, Plaintiff directs the court's attention to no authority that holds the public server liable for the spouse's breach of a licensing agreement that enabled the spouse to capture her partner's private electronic communications. This court concludes that any divulgence by SpectorSoft was inadvertent, and thus, it did not have the necessary *mens rea* for liability under the ECPA.

The court does not need to address SpectorSoft's other arguments pertaining to whether it divulged Plaintiff's communication in violation of the ECPA because this court has determined that even if such divulgence occurred, it was not intentional as required by the ECPA.

Tennessee law also requires that divulgence of electronic communications be "intentional." *See* Tenn. Code Ann. § 39-13-601(c)(1). Further, courts interpreting both the ECPA and the TWA have interpreted them in the same way using federal case authority due to the dearth of Tennessee cases interpreting the TWA. *See Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 979 (M.D. Tenn. 2008) (agreeing with parties that analysis of Tennessee law "should be based on how federal courts have analyzed the relevant issues under the [Federal Wiretap Act], because there is very limited TWA case law and the relevant TWA and [Federal

Wiretap Act] provisions employ identical language"). Plaintiff's claim under the TWA will also be dismissed because there is no genuine issue of material fact regarding SpectorSoft's intent to divulge Plaintiff's private communications. For these reasons, SpectorSoft's motion for summary judgment on Plaintiff's ECPA and the TWA claims will be **GRANTED**.

B. Aiding and Abetting Claim

Plaintiff's Complaint states that "Spectorsoft aided and abetted Mary Jo Davis and Alice Suzanne Hayes in the violation of Plaintiff's statutory and common law rights." Complaint, ¶ 15. Tennessee courts have found that:

> [t]he common law civil liability theory of aiding and abetting required that:
>
> > the defendant knew that his companions' conduct constituted a breach of duty, and that he gave substantial assistance or encouragement to them in their acts.
>
> Accordingly, civil liability for aiding and abetting requires affirmative conduct. Failure to act or mere presence during the commission of a tort is insufficient for tort accomplice liability.

Carr v. United Parcel Service, 955 S.W.2d 832, 836 (Tenn. Sup. Ct. 1997) (overruled on other grounds by *Parker v. Warren Cty. Utility Dist.*, 2 S.W.3d 170, 176 (Tenn. Sup. Ct. 1999)) (quoting *Cecil v. Hardin*, 575 S.W.2d 268, 272 (Tenn. Sup. Ct. 1978)); *see also, Harris v. Dalton*, No. E2000-02115-COA-R3-CV, 2001 WL 422964, *3 (Tenn. Ct. App. Apr. 26, 2001).

The court concludes that with respect to this claim, Plaintiff has not created a genuine issue of material fact regarding whether SpectorSoft aided and abetted the invasion of his privacy. There is no evidence that SpectorSoft took an affirmative act that encouraged Ms. Davis or Ms. Hayes to violate Plaintiff's rights. In fact, SpectorSoft attempted to protect the rights of persons like Plaintiff by requiring Ms. Davis to accept its licensing terms prior to being

allowed to install its software. There is similarly no evidence that SpectorSoft knew anything about how Ms. Davis and Ms. Hayes were using its software. Plaintiff appears to argue that the fact that other web-based companies marketed SpectorSoft's products to spouses concerned about adultery constitutes sufficient evidence of aiding and abetting an invasion of his privacy. SpectorSoft itself did not market its product for such uses, and it provided its users with a licensing agreement that it had reason to believe was valid. *See ProCD, Inc.*, 86 F.3d 1447. Further, even a broad-based marketing campaign does not provide the affirmative act of specific encouragement or assistance to the individuals at issue in this case. Plaintiff's aiding and abetting claim will be **DISMISSED**.

C. Product Liability Claim

Tennessee's Products Liability Act provides that a seller of a consumer product may be liable for "injury to a person or property caused by the product" if "the product is determined to be in a defective condition or unreasonably dangerous at the time it left the control of the manufacturer or seller." Tenn. Code Ann. § 29-28-105(b). The plaintiff bears the burden of demonstrating that a product is either defective or unreasonably dangerous. *See Johnson v. Manitowoc Boom Trucks, Inc.*, 406 F.Supp.2d 852, 857 (M.D. Tenn. 2005). The Act defines a "product liability action" as one brought "for or on account of *personal injury, death or property damage* caused by or resulting from the manufacture, construction, design, formula, preparation, assembly, testing, service, warning instruction, marketing, packaging or labeling of any product." Tenn. Code Ann. § 29-28-102(6) (emphasis added). A "defective condition" is one that "renders [a product] unsafe for normal or anticipatable handling and consumption." Tenn. Code Ann. § 29-28-102(2). The Act defines "unreasonably dangerous" as dangerous

> to an extent beyond that which would be contemplated by the ordinary consumer who purchases it, with the ordinary knowledge common to the community as to its characteristics, or that the product because of its dangerous condition would not be put on the market by a reasonably prudent manufacturer or seller, assuming that the manufacturer or seller knew of its dangerous condition.

Tenn. Code Ann. § 29-28-102(8).

In interpreting the Tennessee Act, the district court in *Johnson* noted:

> . . . there are two tests for determining whether a product is "unreasonably dangerous." A product is unreasonably dangerous if it is more dangerous than would be contemplated by an ordinary consumer (the "consumer expectation test"), or if the product is so dangerous it would not be put on the market by a reasonably prudent manufacturer (the "prudent manufacturer test"). Under Tennessee law, the two tests are distinct, have different elements, require different forms of proof, and are neither mutually exclusive nor mutually inclusive. . . . The prudent manufacturer test requires the evaluation of a number of factors, drawn from the writing of Deans Wade, Prosser and Keeton, including: the safety aspects of the product, the likelihood or probable seriousness of an injury, the manufacturer's ability to eliminate the unsafe character of the product without impairing the product's utility or making it too expensive, the user's ability to avoid danger by exercise of care, the user's awareness of the danger inherent in the product, and the feasibility of spreading the loss.

406 F.Supp.2d at 857 (citing *Ray v. BIC Corp.*, 925 S.W.2d 527, 531 (Tenn. Sup. Ct. 1996)).

Further, under Tennessee law

> [a]s a general rule, an injury in and of itself is not proof of a defect and thereby does not raise any presumption of defectiveness. . . . A departure from the required standard of care is not demonstrated by simply showing that there was a better, safer, or different design which might have avoided the injury. A manufacturer is not required to incorporate the ultimate safety features in a product. The manufacturer is not an insurer of its product. It is not required to design a perfect or accident-proof product.

Shoemake v. Omniquip Int'l., Inc., 152 S.W.3d 567, 573 (Tenn. Ct. App. 2004) (citing *Fulton v. Pfizer Hosp. Prod. Group, Inc.*, 872 S.W.2d 908, 911 (Tenn. Ct. App. 1993); *Curtis v. Universal Match Corp.*, 778 F.Supp. 1421 (E.D. Tenn. 1991)) (other citations omitted).

The parties disagree on whether software constitutes a product within the meaning of the

Products Liability Act. In addition, Plaintiff's expert opines that SpectorSoft's software is both "defective" and "unreasonably dangerous." *See* Goodgame Report, p. 7. He suggests that there are measures SpectorSoft could have taken to ensure that its software is not mishandled, such as alerting users to monitoring. However, this is not enough to trigger liability for a defective product under Tennessee law. *See Shoemake*, 152 S.W.3d at 573.

In addition, Plaintiff's Complaint is noticeably lacking in any suggestion of the kind of injury required by the Act – personal injury, death, or property damage. Tenn. Code Ann. § 29-28-102(6). Plaintiff's Complaint alleges only the following damages that the court can discern: "Plaintiff has suffered severe mental anguish and humiliation as a result of the violation of his Tennessee and federal statutory and common law rights." Complaint, ¶ 14. Elsewhere he contends that he has suffered "damages" due to SpectorSoft's "negligence." *Id.* at ¶ 17.

Plaintiff has cited to no Tennessee authority suggesting that a products liability claim can be brought for emotional injuries alone, unaccompanied by some sort of physical injury or actual damage to property. Plaintiff also does not allege in his Complaint that the alleged invasion of his privacy actually damaged his property, such as his computer or his business. The cases upon which Plaintiff relies for support of his products liability action are cases based on severe physical injuries. *See Ray v. BIC Corp.*, 925 S.W.2d at 528 (addressing product liability claim relating to use of a cigarette lighter that caused severe injuries, including brain damage, to young child and destroyed apartment building); *Rutherford v. Polar Tank Trailer, Inc.*, 978 S.W.2d 102, 103 (Tenn. Ct. App. 1998) (addressing product liability claim arising from physical injuries caused by spilling asphalt). As Plaintiff has provided no legal support for the position that a claim for damages under the Product Liability Act includes a claim unaccompanied by physical

injury, death or property damage, the court must **DISMISS** Plaintiff's claim under Tennessee's Products Liability Act.

D. Negligence Claim

Similarly, Plaintiff fails to provide appropriate legal support for his general negligence claim. Plaintiff argues that rather than simply addressing his claim as a products liability action, this court should also consider whether his action supports a "general negligence" claim. However, as stated *supra*, Plaintiff has failed to show any general physical injuries or damage to property usually warranted in a general negligence claim. Although he does not state his claim specifically as such, Tennessee law does recognize a claim for general emotional distress caused by the negligent actions of another in the form of a negligent infliction of emotional distress claim. *See Eskin v. Bartee*, 262 S.W.3d 727, 733 (Tenn. Sup. Ct. 2008). The Tennessee Supreme Court has established that where a case is purely one for emotional injury unaccompanied by damages for physical injury or other damages – a "stand-alone" negligent infliction of emotional distress claim – it:

> should be analyzed under the general negligence approach . . . In other words, the plaintiff must present material evidence as to each of the five elements of general negligence – duty, breach of duty, injury or loss, causation in fact, and proximate or legal, cause – in order to avoid summary judgment. Furthermore, we agree that in order to guard against trivial or fraudulent actions, the law ought to provide recovery only for "serious" or "severe" emotional injury. A "serious" or "severe" emotional injury occurs "where a reasonable person, normally constituted, would be unable to adequately cope with the mental stress engendered by the circumstances of the case." Finally, we conclude that the claimed injury or impairment must be supported by expert medical or scientific proof.

Camper v. Minor, 915 S.W.2d 437, 446 (Tenn. Sup. Ct. 1996).

Plaintiff attempts to argue that SpectorSoft owed him a duty. However, the negligence cases upon which he relies are cases involving some form of physical injury combined with the

presence of a special relationship. *See Satterfield v. Breeding Insulation Co.*, 266 S.W.3d 347 (Tenn. Sup. Ct. 2008) (negligence claim based on cancer causing death of employee's daughter where employee was exposed to years of asbestos fibers on clothing that was transferred to the family home); *Cornpropst v. Sloan*, 528 S.W.2d 188 (Tenn. Sup. Ct. 1975) (violent attack to plaintiff in shopping mall parking lot) (abrogated by *McClung v. Delta Square Ltd. Partnership*, 937 S.W.2d 891 (Tenn. Sup. Ct. 1996)); *Giggers v. Memphis Housing Authority*, 277 S.W.3d 359 (Tenn. Sup. Ct. 2009) (negligence action against landlord pertaining to shooting death of tenant by another tenant).

> Under Tennessee law
>
> > [i]n general, all persons have a duty "to use reasonable care to refrain from conduct that will foreseeably cause injury to others." We determine whether a duty existed in a particular case by evaluating the risk involved. "A risk is unreasonable and gives rise to a duty to act with due care if the foreseeable probability and gravity of harm posed by defendant's conduct outweigh the burden upon defendant to engage in alternative conduct that would have prevented the harm."
> >
> > The general duty of care does not include an affirmative duty to act for the protection of another, however, "*unless* the defendant 'stands in some special relationship to either the person who is the source of the danger, or to the person who is foreseeably at risk from the danger.'" The special relationship doctrine carves out an exception to the general rule that there is no duty to act for the protection of a third party.

Biscan v. Brown, 160 S.W.3d 462, 478-79 (Tenn. Sup. Ct. 2005) (quoting *Turner v. Jordan*, 957 S.W.2d 815, 818 (Tenn. Sup. Ct. 1997) and *McCall v. Wilder*, 913 S.W.2d 150, 153 (Tenn. Sup. Ct. 1995)). Plaintiff cites to no Tennessee authority suggesting that a manufacturer of spyware software owes a duty to avoid emotional injury to the victim of the misuse of that software in violation of the software's licensing agreement. Plaintiff fails to demonstrate legal support for the proposition that SpectorSoft had a special relationship with either Ms. Davis or with Plaintiff

or that SpectorSoft assumed a duty of care towards Plaintiff. Thus, based on the lack of legal authority for such a position, this court declines to find that SpectorSoft owed Plaintiff a duty.

Further, Plaintiff has failed to fulfill the specific proof requirements of a "stand-alone" negligent infliction of emotional distress claim. Plaintiff presents no evidence of his severe or serious emotional distress. Nor does he attempt to support his claim for emotional damages with any expert or scientific proof of such damages. Without such evidence of severe emotional distress, Plaintiff's negligence claim that asserts only anxiety and mental distress as damages and thus constitutes a "stand-alone" negligent infliction of emotional distress claim must be **DISMISSED**. *See Camper*, 915 S.W.2d at 446.

IV. Conclusion

As discussed *supra*, the court concludes that Plaintiff's claims must be **DISMISSED**. Defendant SpectorSoft's motion for summary judgment will be **GRANTED**.

A separate judgment will enter.

/s/ R. Allan Edgar
R. ALLAN EDGAR
UNITED STATES DISTRICT JUDGE