

Comment,
SPOUSAL ABUSE THROUGH SPYWARE:
THE INADEQUACY OF LEGAL
PROTECTION IN THE MODERN AGE*

Introduction

Imagine a situation of domestic abuse, where the wife lives in constant fear. The husband is physically abusive only in rare events, so the truth goes unnoticed by outsiders. Yet he is constantly mentally and emotionally abusive, controlling where the wife goes, who she talks to, and what money she spends. He tracks her moves by monitoring her computer activity. Any web-sites she visits, he knows about. Any e-mail she sends, he reads. All instant messaging she engages in, he will see. All pin numbers, credit cards numbers, and passwords she has are exposed to him. When she seeks help by e-mailing a mental health professional or a women's shelter, he learns about it instantly and takes the measures necessary to ensure she goes no further in her search for help. This is just one example of the dangers of spyware¹ and why it must be considered as a form of domestic abuse when one spouse uses it to dominate and control the other.

The current legal scheme, under both state and federal law, is inadequate to address the problem of spyware within the context of the marital relationship. This Comment uses the state of Missouri as a model to demonstrate the flaws. No criminal statutes effectively address the problem of marital spying. Some civil causes of action exist that might potentially address spyware, but they are not well developed or targeted to put an end to this

* The author would like to thank her husband, Nicholas Clevenger, for his continued support and Nancy Levit, Curators' and Edward D. Ellison Professor of Law, for her guidance, support, and comments.

¹ Merriam Webster's On-Line Dictionary defines "spyware" as "software that is installed in a computer without the user's knowledge and transmits information about the user's computer activities over the Internet." Merriam-Webster, <http://www.merriam-webster.com/dictionary/spyware> (last visited Feb. 28, 2008). For an overview on spyware, see Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433 (2005).

form of abuse. Even the federal Wiretap Act² and Missouri's Wiretap Act³ fall short in giving redress to one spouse who is being tracked, monitored, and controlled by the other.

The fact that no effective legal remedies exist against the use of spyware only highlights the danger of it. The spouse whose safety is threatened because he or she cannot leave the relationship has no recourse except to wait until the other spouse turns physically abusive, at which time the victim could seek shelter under the domestic assault statutes.⁴

But waiting until the physical abuse begins should not be a victim's only plan for safety. The victim of spousal spyware is failed by the laws that do not recognize it for what it is—a mechanism by which a predator can monitor, control, and dominate his or her prey. There need to be amendments to the current criminal and civil schemes to provide a remedy for the victim of domestic abuse through spyware before the abuse escalates to an even more dangerous form.

This Comment argues that the use of spyware in intimate relationships to control a partner is a form of domestic abuse that is currently unrecognized by the law. Part I will first explain what spyware is. Part II will analyze why current civil and criminal legal schemes are inadequate to address spyware as a form of domestic abuse. The final part of this Comment will serve as a guide for advising the client, including how to detect and remove spyware and evidentiary issues regarding the use of spyware.

I. What Is Spyware

In general terms, “spyware” is software installed on a computer without the user's knowledge or consent.⁵ The goal of spyware is to monitor the conduct of whoever is using the computer. By taking a snapshot of whatever is on the computer's screen every few seconds, spyware has the ability to monitor everything that a user does, including the tracking of emails, chat room activity, financial transactions, drafting documents, and

² 18 U.S.C. § 2510.

³ MO. REV. STAT. §§ 542.400-.422 (2006).

⁴ Missouri's domestic abuse statutes will be addressed in Part II of this Comment.

⁵ Sharon D. Nelson & John W. Simek, *Spy v. Spy: Electronic Snooping by Husbands, Wives, & Lovers*, 28 FAM. ADVOC. 20, 20 (Winter 2006).

web surfing. Some spyware is designed to monitor keystrokes, which can lead to the disclosure of pin numbers, passwords, credit card numbers, and other sensitive information.⁶

Spyware may be installed on a computer through several different methods. One way is when a user who is on-line encounters a pop-up message that requires the user to click on "yes" or "no," where either choice results in the spyware being automatically and unknowingly installed on the user's computer.⁷ Spyware might also be installed when a user purposely downloads a program from the Internet, not realizing that spyware will be automatically and unknowingly installed with it.⁸ Perhaps the simplest way for spyware to be installed on a computer is for a user who has access to the computer to buy spyware software and then install it the same way any other type of software is installed.

II. Addressing Abusive Use of Spyware Under Current Criminal and Civil Schemes

Under the current federal and state schemes, little legal redress exists in Missouri for the spouse who is a victim of spyware by the other spouse. Criminal statutes written before spyware technology had evolved render those statutes ineffective in dealing with the problem. The same is true of civil causes of action. In more recent years new technology has led to both state and federal legislation seeking to address the electronic monitoring of communication. Even these legal schemes fall short because they were written primarily to combat the electronic monitoring of telephone calls. While computer tampering is now illegal in Missouri, as will be addressed below, even this remedy offers little, if any, redress for a spouse who is being victimized through spyware.

⁶ Shan Sivalingam, *Suing Based on Spyware? Admissibility of Evidence Obtained from Spyware in Violation of Federal and State Wiretap Laws*, 3 SHIELDER J. L. COM. & TECH. 9, Winter 2007, at 3.

⁷ *Id.*

⁸ *Id.*

A. *Spyware Under Missouri's Criminal Laws*

Five possibilities exist for criminal prosecution of spyware in Missouri: domestic assault, stalking, invasion of privacy, computer tampering, and the Missouri Wiretap Act. The feasibility of criminally prosecuting spyware in each of these contexts will be addressed in turn.

1. *Spyware as Domestic Assault*

Domestic assault statutes provide little, if any, recourse for a computer user whose spouse has installed spyware on his or her computer. In Missouri, if a person causes or attempts to cause physical injury to his or her spouse, that person is guilty of second degree domestic assault.⁹ If that person attempts to kill or knowingly cause serious physical injury to a spouse, he or she would be guilty of domestic assault in the first degree.¹⁰ It is only third degree domestic assault that includes something other than physical injury or the fear of physical injury as a punishable offense: the isolation of a spouse “by unreasonably and substantially restricting or limiting [the spouse’s] access to other persons, telecommunication devices or transportation.”¹¹

No courts in Missouri, or any other state, have addressed the issue of whether covertly installing spyware on a spouse’s computer constitutes domestic assault. The best possibility, however remote, for pursuing the use of spyware on a spouse as a form of domestic assault is to argue that the spyware is a form of isolation as recognized in third degree domestic assault.

The quite obvious problem with this approach is that spyware does not isolate the user, it monitors him or her. If anything, the spying spouse will *encourage* the computer-using spouse to use the computer to communicate with those outside the home so as to better monitor the using spouse’s communications, internet activities, and financial habits. It may be difficult as a factual matter to prove that the spying spouse intended to isolate the using spouse. Perhaps if the using spouse knows about the spyware, he or she might be isolated for purposes of the statute because he or she will no longer use the computer to commu-

⁹ MO. REV. STAT. § 565.073 (2006).

¹⁰ MO. REV. STAT. § 565.072 (2006).

¹¹ MO. REV. STAT. § 565.074 (2006).

nicate with the world outside of his or her home. But the using spouse's fear of using the computer alone probably will not suffice for purposes of the statute since he or she can still communicate with those outside the home through more traditional means.

2. *Spyware as Stalking*

Stalking under Missouri law resembles stalking under the statutes of other states.¹² In Missouri, stalking consists of purposely and repeatedly harassing or following a person with the intent to harass that person.¹³ Aggravated stalking occurs when a person "purposely and repeatedly harasses or follows [another] with the intent" to harass, and also "makes a credible threat with the intent to place that person in reasonable fear of death or serious physical injury."¹⁴ "Harasses" as defined for purposes of stalking means "to engage in a course of conduct directed at a specific person that serves no legitimate purpose, that would cause a reasonable person to suffer substantial emotional distress, and that actually causes substantial emotional distress to that person."¹⁵ "Course of conduct" is defined as "a pattern of conduct composed of a series of acts, which may include electronic or other communications, over a period of time, however short, evidencing a continuity of purpose."¹⁶

As with domestic assault, Missouri courts have not addressed whether using spyware on one's spouse constitutes stalking. The current definitions in Missouri's stalking statute are not adequate to address a spouse who is using spyware to monitor his or her spouse's behavior. Regarding computer activity, the statute requires the stalker to engage in a pattern of conduct involving electronic communications that causes substantial emotional distress to the victim.¹⁷ The statute is designed to cover things

¹² Stalking is criminal in all fifty states; most states include the requirement of a "credible threat"; and many states require that the stalker intends to cause fear or actually does cause the victim fear of injury or death. Alan Rubel, *Claims to Privacy and the Distributed Value View*, 44 SAN DIEGO L. REV. 921, 942 n.45 (2007).

¹³ MO. REV. STAT. § 565.225.2 (2006).

¹⁴ *Id.* at § 565.225.3.

¹⁵ *Id.* at § 565.225.1(3).

¹⁶ *Id.* at § 565.225.1(1).

¹⁷ *Id.* at § 565.225.

such as sending harassing emails or text messages or making repeated obscene phone calls.

Using spyware to track a spouse's computer activity does not involve overt harassment through electronic communications. Monitoring one's activity is too passive an activity to fall under the statute's purview, even if that monitoring is being used to control another. Where this statute might provide some remedy to a spouse being spied on is if the spying spouse monitors the victim's computer activity to find out the various places where the victim is going to be, and then shows up at those places.

Perhaps the biggest barrier to using the statute to prosecute the use of spyware on one's spouse as stalking is the requirement of "substantial emotional distress." A spouse who does not know he or she is being tracked through spyware is *still* being tracked, although they may not be suffering substantial emotional distress. It is the pattern of abusive control that spyware perpetuates, and it is this pattern that is not sufficiently addressed by the stalking statute. Changing the statute so that it focuses on the spy's wrongful actions instead of his or her ability to incite fear in the victim is a simple way to help remedy the problem.¹⁸

3. *Spyware as an Invasion of Privacy*

While it cannot be argued persuasively that spyware is anything but an invasion of the user's privacy, the Missouri statutes pertaining to the crime of privacy invasion afford no remedy for the victim whose spouse uses spyware to monitor his or her computer activities. The crime of invasion of privacy involves some sort of photographing or videotaping of a person, unbeknownst to that person, while he or she is fully or partially nude.¹⁹ As it currently stands, this crime does not include electronic spying on one's spouse, even if such activity gives the spying spouse access to the victim's personal e-mails, electronic documents, financial activities, passwords, general Internet activity, or other personal

¹⁸ In 2004 Wisconsin made such a change to its stalking statute. The amendment made "knowledge (as opposed to intent) that conduct could cause serious emotional harm or fear" sufficient to qualify the activity as stalking. Mary L. Boland, *Model Code Revisited: Taking Aim at the High-Tech Stalker*, 20 CRIM. JUST. 40, 56 (Spring 2005).

¹⁹ MO. REV. STAT. §§ 565.252-.253 (2006)

information. The crime of invasion of privacy is an insufficient avenue for the prosecution of spousal spyware as a form of domestic abuse.²⁰

Some states have an intrusion upon seclusion privacy tort, imposing liability on “one who intentionally intrudes, physically or otherwise, upon the . . . seclusion of another or his private affairs. . . if the intrusion would be highly offensive to a reasonable person.”²¹ But problems exist with using this tort in the context of spousal spying through spyware. The expectation of privacy is lower when the two parties are married and living together than when the parties are strangers.²² It may be difficult to show that the use of spyware on one’s spouse is “highly offensive to a reasonable person” with this lowered expectation of privacy. Another problem is that the defense of consent can be raised.²³ A computer that is shared by both spouses in the marital home may imply consent and bar the cause of action.²⁴

4. *Spyware as Computer Tampering*

Missouri has three statutes that directly address unauthorized computer use.²⁵ Simply accessing a computer without authorization, or reasonable grounds to believe one has authorization, is a crime.²⁶ Physically taking computer equipment without authorization, or reasonable grounds to believe one has authorization, is also a violation of Missouri law.²⁷ The same is true if someone modifies data or programs on the computer without the proper authorization.²⁸ Accessing a computer

²⁰ Great variety exists among the states regarding the tort of invasion of privacy. See RESTATEMENT (SECOND) OF TORTS § 652A (1977), Reporter’s Note for an overview of which states recognize the tort of invasion of privacy.

²¹ RESTATEMENT (SECOND) OF TORTS § 652B (1977).

²² Camille Calman, *Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers*, 105 COLUM. L. REV. 2097, 2126 (2005).

²³ *Id.*

²⁴ *Id.*

²⁵ MO. REV. STAT. §§ 569.095-.099 (2006). Under Missouri Revised Statutes section 537.525 (2006), a person may seek compensatory damages and attorney’s fees in a civil cause of action if one of these computer tampering statutes are violated.

²⁶ *Id.* at § 569.099.1(1).

²⁷ *Id.* at § 569.097.1.

²⁸ *Id.* at § 569.095.1(1).

and intentionally examining information about another person without reasonable grounds to believe one has the authorization to do such snooping is also a crime.²⁹

Missouri courts have not addressed whether these computer tampering statutes may be used to prosecute the spouse who uses spyware to track the activities of the other spouse. Installing spyware requires accessing the computer, so at a minimum it can be argued that spyware installation is a violation of Missouri Revised Statutes section 569.099, which prohibits accessing a computer without authorization. The spying spouse is using spyware to discover personal information about the unsuspecting spouse, which is arguably a violation of Missouri Revised Statutes section 569.095.1(5), prohibiting intentional examination of information about another person.

The question of whether these computer tampering statutes will be a successful conduit for prosecuting a spying spouse will likely turn on whether the spying spouse had authorization, or had reasonable grounds to believe he or she had authorization, to install the spyware and view the using spouse's computer activity without that spouse's knowledge of the spyware. Since most computer tampering cases in Missouri have arisen in the context of an employee accessing information on the employer's computer,³⁰ case law does not indicate what constitutes "reasonable grounds" for a spouse to believe he or she is authorized to access his or her spouse's computer or modify that computer.

To guide their decisions in this uncharted territory, courts could turn to the analysis used in search and seizure cases where the question of whether one spouse had actual or apparent authority to consent to the search arises. A spouse is presumed to have actual authority to consent to all searches of the marital home.³¹ This presumption may be rebutted "by showing that the consenting spouse was denied access to the particular area searched."³² Under this reasoning, a spouse is presumed to have consent to use any computer kept in the marital home. Only by a clear showing that the spying spouse had been denied access to

²⁹ *Id.* at § 569.095.1(5).

³⁰ *See Martha's Hands, L.L.C. v. Starrs*, 208 S.W.3d 309 (Mo. Ct. App. 2006).

³¹ *United States v. Gevedon*, 214 F.3d 807, 810-11 (7th Cir. 2000).

³² *Id.* at 811.

the computer by the other could the spouse being spied upon win the argument that the spying spouse violated the computer tampering statutes.

Courts might also look at whether the victim spouse gave implied consent for the spyware to be installed on the computer. Implied consent “is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.”³³ To show implied consent, the spying spouse would have to demonstrate that the victim spouse knew about the spyware and did in some way not protest its continued use.³⁴

It is likely that a court would look at the facts surrounding the case to determine how reasonable it was for a spouse to believe he or she had the authority to use or modify the computer. Various facts that might be pertinent include whether one or both spouses owned the computer, whether all the members of the household used the computer or just one spouse used it, and whether the computer was password protected.³⁵ These factors indicate what a reasonable person would know to be his or her level of authority over the computer. The more factors there are indicating only one spouse owned the computer and never intended anyone else to use it, the more likely the spouse who installed the spyware could be successfully prosecuted under one of the computer tampering statutes.

5. *Spyware as a Violation of the Missouri Wiretap Act*

The Missouri Wiretap Act³⁶ prohibits a person from knowingly intercepting any wire communication³⁷ or using any electronic device to intercept oral communications transmitted by radio³⁸. The Act also makes it a crime for one to knowingly use or disclose the contents of any wire communication which he or

³³ State v. Martinelli, 972 S.W.2d 424, 430-31 (Mo. Ct. App. 1998) (citations omitted).

³⁴ *Id.*

³⁵ See, e.g., Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (holding that a housemate had authority to consent to a general search of the computer she and her housemate shared, but lacked authority to consent to a search of the other housemate’s password protected files).

³⁶ MO. REV. STAT. §§ 542.400-.422 (2006).

³⁷ *Id.* at § 542.402.1(1).

³⁸ *Id.* at § 542.402.1(2).

she knows was obtained illegally.³⁹ “Intercept” for purposes of the Act is the “aural acquisition of the contents of any wire communication through the use of any electronic or mechanical device.”⁴⁰ “Wire communication” entails any communication made with the aid of “wire, cable, or other like connection between the point of origin and the point of reception.”⁴¹

Missouri courts have not yet addressed the question of whether the Missouri Wiretap Act pertains to spyware used to gather information from a user’s computer or to read a user’s emails. While the Act could be amended to specifically include the interception of e-mails and the viewing of all the other information contained on a computer, as it stands currently, prosecuting the use of spyware by one spouse on the other as a violation of the Missouri Wiretap Act may be difficult because the Act was not created to address that situation. Passed in 1989, the Act was designed to prevent the taping of telephone conversations, conversations transmitted by radio, and in-person conversations when the parties did not know they were being recorded.⁴²

Viewing another’s e-mails could fall into the scope of the Act because those communications are transmitted by the “aid of wire, cable, or other like connection.”⁴³ But the Act only makes this behavior a crime if the content of the wrongly viewed e-mail is either *disclosed* or *used* in some way.⁴⁴ This does little to help the spouse whose mate is secretly reading the other’s e-mails and monitoring the other’s internet activity to control and manipulate the other. Conceivably, a spying spouse could escape liability by not overtly disclosing or using the contents of the email. Unless he or she blatantly acts upon information contained in an email, one could claim he or she simply read the email without ever acting upon the contents.

Outside the context of e-mail, the protection offered to the spyware victim is even less certain. Nothing in the Missouri Wiretap Act purports to protect general computer use or general

³⁹ *Id.* at §§ 542.402.1(3) and (4).

⁴⁰ *Id.* at § 542.200(6).

⁴¹ *Id.* at § 542.400(12).

⁴² *Phillips v. American Motorist Ins. Co.*, 996 S.W.2d 584 (Mo. Ct. App. 1999).

⁴³ MO. REV. STAT. § 542.400(12) (2006).

⁴⁴ *Id.* at §§ 542.402.1(3) and (4).

information contained on one's personal computer. Surfing the internet, typing a document, drafting a letter, tracking one's finances—none of these things falls under the umbrella of "wire communication" that might be protected by the Act if simply reviewed by the spying spouse. At best the Act could protect a spouse from having his or her e-mails be read without authorization. When it comes to protecting all the other information stored on the computer, the victim whose spouse is using spyware on them is helpless.

B. *Spyware Under Missouri's Civil Scheme*

Five civil causes of action exist in Missouri under which using spyware on a spouse could conceivably be brought: negligent infliction of emotional distress, intentional infliction of emotional distress, invasion of privacy, trespass to chattels, and the civil remedy provided in the Missouri Wiretap Act. As will be discussed, these remedies are inadequate to address the problem of one spouse using spyware to dominate and control the other. These causes of action did not arise in the context of spyware or spousal abuse, so the victim is left trying to squeeze spyware into a scheme into which it was never designed to fit.

Additionally, in the case of spousal abuse, the victim's desire is typically to be outside the reach of his or her abuser. Civil remedies, which usually result in an award of money damages if successful, do not provide any sort of safety for a spouse seeking to be free from the abuse.

1. *Negligent Infliction of Emotional Distress*

Two elements comprise negligent infliction of emotional distress in Missouri: the defendant should have realized that his or her actions included an unreasonable risk of causing the emotional distress, and the emotional distress is medically diagnosable and severe enough to be medically significant.⁴⁵ This cause of action might be successful in the case of a spouse who is severely emotionally abused if the abuse results in a harm so great it can be diagnosed medically. Using spyware to spy on a spouse, on its own, is unlikely to cause enough emotional harm

⁴⁵ Gibson v. Brewer, 952 S.W.2d 239, 248-49 (Mo. 1997).

to rise to the level required under this tort, although it may be a part of a pattern that does rise to such a level.⁴⁶

Torts such as negligent infliction of emotional distress highlight the need for either a new cause of action addressing spyware as a form of domestic abuse or amended current causes of action to include spyware. Spyware used by one spouse to control another is part of a greater pattern of dominance and control that leaves the victim vulnerable and limited in the help he or she can seek.⁴⁷ Patterns of dominance and control, such as those suggested by using spyware on one's spouse, are often signs that more physically dangerous abuse is occurring or likely to occur.⁴⁸ Unless this tort is modified, it will provide little, if any, remedy to a spouse who has been spied on through his or her computer.

2. *Intentional Infliction of Emotional Distress*

To be successful in bringing an intentional infliction of emotional distress action in Missouri a plaintiff must show: that the defendant acted in an extreme and outrageous way; the defendant's conduct intentionally or recklessly caused severe emotional distress; bodily harm resulted.⁴⁹ The Missouri Supreme

⁴⁶ See *Simmons v. Simmons*, 773 P.2d 602 (Colo. Ct. App. 1988), and *Hogan v. Tavzel* 660 So.2d 350 (Fla. Dist. Ct. App. 1995), where underlying claims of battery provided the basis for bringing an intentional infliction of emotional distress claim.

⁴⁷ "Domestic Violence" is defined by the U.S. Department of Justice and the National Domestic Violence Hotline "as a pattern of abusive behavior in any relationship that is used by one partner to gain or maintain power and control over another intimate partner." United States Department of Justice, Office on Violence Against Women, <http://www.ovw.usdoj.gov/domviolence.htm> (last visited Feb. 28, 2008).

⁴⁸ See Christine N. Carlson, *Invisible Victims: Holding the Educational System Liable for Teen Dating Violence at School*, 26 HARV. WOMEN'S L.J. 351, 365 (Spring 2003), stating "Twenty percent of female homicide victims nationwide are between the ages of fifteen and twenty-four . . . investigation into these victims' dating relationships typically revealed [that] patterns of control and physical abuse by their partners that escalated over time (citations omitted); see also Karla Fischer, et al., *The Culture of Battering and the Role of Mediation in Domestic Violence Cases*, 46 SMU L. REV. 2117, 2119 (1993), analyzing the systematic patterns of control and dominance that defines abusive relationships.

⁴⁹ *Gibson*, 952 S.W.2d at 249.

Court has held that the conduct must have been “so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community.”⁵⁰ The most obvious barrier to intentional infliction of emotional distress being a viable cause of action to the victim of spyware is the requirement that bodily harm results from the conduct.

This cause of action could be viable in certain narrow situations. Assuming the abused spouse temporarily left the other, a spying spouse might use the computer to discover the victim’s whereabouts. If the abusive spouse then showed up and physically injured the victim, perhaps there would be an intentional infliction argument. The victim would first have to convince the court that using spyware on one’s spouse is extreme and outrageous. Then, he or she would have to demonstrate severe emotional distress and bodily harm.

Courts have not yet had a chance to apply intentional infliction of emotional distress in such a situation involving the use of spyware on one’s spouse. It is likely that whether the use of spyware is seen as “extreme and outrageous” will be a question of fact where a jury will analyze various factors, including whether the spying spouse had authorization to use the computer. In *Miller v. Brooks*⁵¹, an estranged husband sued his wife for intentional infliction of emotional distress because the wife instructed private detectives she had hired to secretly install a video camera in the husband’s bedroom. The court held that whether such conduct constituted the “extreme and outrageous conduct” needed to sustain the husband’s claim for intentional infliction of emotional distress was a question of fact for the jury.

3. *Invasion of Privacy*

The tort of invasion of privacy encompasses several different theories. A person is liable for invasion of privacy if he or she intrudes on the plaintiff’s seclusion, publicly discloses embarrassing private matters, publicly places the plaintiff in an untrue light, or uses the plaintiff’s name or likeness to his or her own advantage.⁵² The last three of these do not usually apply to the situa-

⁵⁰ *Warren v. Parrish*, 436 S.W.2d 670, 673 (Mo. 1969).

⁵¹ 472 S.E.2d 350 (N.C. Ct. App. 1996).

⁵² *Nemani v. St. Louis Univ.*, 33 S.W.3d 184, 185 (Mo. 2000).

tion of a spouse being dominated and controlled through spyware.

Seeking legal redress under the first form of invasion of privacy, intrusion on the plaintiff's seclusion, might apply to a spouse who is using spyware on the unknowing spouse. This tort consists of three elements in Missouri: a secret and private subject matter exists; the plaintiff has a right to keep that subject matter private; and defendant obtained information about that private subject matter through means that are unreasonable.⁵³

Conceivably, the victim spouse would be successful in bringing an action for intrusion on seclusion if the abuser used spyware to obtain information such as pin numbers, passwords, bank account numbers, etc. This is the type of information that is designed to be protected and kept secret. The problem lies in the special nature of the marital relationship. Unless the couple has gone through great means to keep their financial interests, accounts, and records secret and separate from each other, it will be very hard to show that the abuser spouse did not have a right to the information upon which he is intruding.⁵⁴ If the information being intruded upon is something such as what web sites the victim spouse has visited, then the case will be even harder to prove, since this is not generally considered "secret and private subject matter."⁵⁵

4. *Trespass to Chattels*

This cause of action arises when one person, without authorization or justification, intentionally interferes with another's use of his or her own personal property.⁵⁶ Trespass to chattels involves the actual taking of another's personal property or exercising control over the property in a manner inconsistent with the

⁵³ St. Anthony's Med. Ctr. V. H.S.H., 974 S.W.2d 606, 609-10 (Mo. Ct. App. 1998).

⁵⁴ See *Trulock*, 275 F.3d at 403.

⁵⁵ A case filed in federal district court in Michigan is being asked to address the question of whether using spyware on one's spouse is an invasion of privacy in Michigan. At this point in the proceedings, the court has denied summary judgment on this issue, stating that whether the use of spyware on one's spouse is objectionable to a reasonable person is a question of fact for the jury. *Bailey v. Bailey*, Case 2:07-cv-11672-SFC-MKM (E.D. Mich. 2008).

⁵⁶ *Foremost Ins. Co. v. Public Serv. Comm'n*, 985 S.W.2d 793, 797 (Mo. Ct. App. 1998).

owner's intention.⁵⁷ This tort has generally been used when a physical object has been taken from its rightful owner.⁵⁸

Missouri courts have not addressed whether electronic access to information on a person's personal computer could be covered by this cause of action. It is very unlikely that a court would extend trespass to chattels to include spyware used by one spouse against the other. The use of spyware does not involve taking personal property from the victim, so the action could only be successful if the victim could show the spying spouse exercised "control over the [computer] in a manner inconsistent with the owner's intention."⁵⁹ If the computer is owned by both spouses then this cause of action could not be brought at all because the installation of spyware would be consistent with the owner's intention if the spying spouse owns, or jointly owns, the computer. If the spouse being spied upon is the sole owner of the computer, then he or she might be successful in a trespass to chattel suit if he or she could show the spying spouse had no right to use the computer and exercised wrongful control over the computer.⁶⁰

5. Civil Remedy Under Missouri's Wiretap Statute

If a person's wire communication is intercepted or disclosed in violation of the Missouri Wiretap Act, that person may bring a civil cause of action against the one who wrongfully intercepted the communication.⁶¹ If the plaintiff is successful in this action, he or she may be awarded actual damages, punitive damages, and attorney's fees.⁶² This remedy could be quite strong for the plaintiff whose wire communications have been intercepted and used in a detrimental way. As discussed above, however, the

⁵⁷ *Tubbs v. Delk*, 932 S.W.2d 454, 456 (Mo. Ct. App. 1996).

⁵⁸ See *Foremost Ins. Co.*, 985 S.W.2d 793 (where trespass to chattel action brought for the improper removal of a Department of Housing and Urban Development seal from a mobile home); *Tubbs*, 932 S.W.2d 454 (trespass to chattel action brought where plaintiff's camera was taken from him); *Schrader v. Summerville*, 763 S.W.2d 717 (Mo. Ct. App. 1989) (where trespass to chattels action was brought for the wrongful appropriation of plaintiff's farm truck and grain box).

⁵⁹ *Tubbs*, 932 S.W.2d at 456.

⁶⁰ See *Miller*, 472 S.E.2d at 355.

⁶¹ MO. REV. STAT. § 542.418.2 (2006).

⁶² *Id.*

Missouri Wiretap Act likely gives no protection to the spouse who is being victimized through spyware, rendering this civil remedy useless to the victim whose spouse is using spyware to dominate and control him or her.

C. *Spyware under the Federal Scheme*

It may be a common perception that spyware would fall under the purview of the federal Wiretap Act, nullifying the need for causes of action at the state level. However, the federal scheme provides little remedy to the spouse who is a victim of spying, leaving open the need for legal redress at both the state and federal levels.⁶³

1. *Computer Fraud and Abuse Act (“CFAA”)*

The CFAA focuses on wrongful access of a computer.⁶⁴ Originally enacted to allow certain computer crimes to be prosecuted federally, it was amended in 1986 and 1994 to allow a private cause of action for unauthorized use of a private computer.⁶⁵ A spyware victim may assert a civil cause of action under the CFAA if he or she can show one of the following: he or she suffered aggregate damages of \$5,000 within a one year period; modification or impairment of medical information; physical injury; a threat to public health or safety; damage to a computer system owned by the government.⁶⁶ The average individual computer user will not be able to demonstrate the last four of these elements.⁶⁷

A victim of spyware’s most likely chance of succeeding under the CFAA is if he or she can show damage of at least \$5,000 in a year’s time. But even this is a virtual impossibility unless it is the type of situation where the spy accessed financial

⁶³ “Installing software on a computer one owns jointly with someone else is perfectly legal under federal and state law.” Calman, *supra* note 22, at 2097-98.

⁶⁴ Laura W. Morgan, *Marital Cybertorts: The Limits of Privacy in the Family Computer*, 20 J. AM. ACAD. MATRIM. LAW. 231, 242 (2007).

⁶⁵ *Id.*

⁶⁶ 18 U.S.C. § 1030.

⁶⁷ Alan F. Blakely, Daniel B. Garrie & Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn’t Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. 25, Nov. 16, 2005, at para. 16.

information and then drained money, in excess of \$5,000, from an account. Furthermore, the damage caused by spyware in the case of an abused spouse is more likely to be the kind of emotional and psychological damage that cannot be reduced to a monetary figure.

Spousal abuse threatens the public on a collective level. Financial loss,⁶⁸ increased health care costs,⁶⁹ and emotional and behavioral problems in children⁷⁰ can all be traced to domestic abuse. Stalking victims commonly need psychological counseling to help them cope with the trauma of what they have been through.⁷¹ Current legal remedies do not adequately address public health threats such as these.

2. *Electronic Communications Privacy Act ("ECPA")*

The Electronic Communications Privacy Act⁷² was originally designed in 1968 to address the interception of "wire or oral" communications.⁷³ Recognizing the shortcomings of the ECPA in addressing new methods of communication, Congress amended the Act with the ECPA in 1986 to include electronic communications.⁷⁴ This amendment gave to data and electronic

⁶⁸ "The annual cost of lost productivity due to domestic violence is estimated as \$727.8 million with over 7.9 million paid workdays lost per year." Corporate Alliance to End Partner Violence, citing Costs of Intimate Partner Violence Against Women in the United States, 2003, Centers for Disease Control and Prevention, National Center for Injury Prevention and Control, http://www.caepv.org/getinfo/facts_stats.php?factsec=2 (last visited Feb. 28, 2008).

⁶⁹ Women who suffer domestic abuse seek medical attention more often than those who do not, making annual health care costs significantly higher. Corporate Alliance to End Partner Violence, http://www.caepv.org/getinfo/facts_stats.php?factsec=6 (last visited Feb. 28, 2008).

⁷⁰ "Children who witness domestic violence may suffer acute and long-term emotional disturbances, including nightmares, depression, learning difficulties, and aggressive behavior. Children also become at risk for subsequent use of violence against their dating partners and wives." (citations omitted), Corporate Alliance to End Partner Violence, http://www.caepv.org/getinfo/facts_stats.php?factsec=7 (last visited Feb. 28, 2008).

⁷¹ "Thirty percent of female stalking victims and 20 percent of male stalking victims seek psychological counseling as a result of their victimization. They are significantly more likely to fear for their personal safety than people who have never been stalked." *Id.*

⁷² 18 U.S.C. § 2510.

⁷³ Morgan, *supra* note 66, at 233.

⁷⁴ *Id.*

transmissions the same protection already enjoyed by oral and wire communications.⁷⁵

The ECPA still is not adequate for dealing with the situation where a spouse is using spyware to spy on the other spouse because it applies only to the interception of *in transit* electronic information, not *stored* electronic information.⁷⁶ This disparity allows spyware to remain outside the scope of the ECPA by a two step process: recording the user's keystrokes and then transmitting the information to the spy.⁷⁷ This system of intercepting the information while it is temporarily stored, not while being transmitted, allows the typical spousal spying behavior to avoid the implications of the ECPA.⁷⁸

3. *Stored Wire and Electronic Communications and Transactional Records Act ("Stored Communications Act")*

The Stored Communications Act is Title II of the ECPA.⁷⁹ The Stored Communications Act "regulates the intentional access of stored electronic communications and records."⁸⁰ The victim of spyware can bring a private cause of action under the Stored Communications Act.⁸¹ To be successful, the victim must show that the access to his or her computer was to "a facility through which an electronic communication service is provided," intentional, in excess of authorization, to obtain, alter, or prevent a wire or electronic communication, and one that involved a communication kept in the electronic storage of the computer.⁸²

All of these elements, except the third one, are relatively easy for the victim of spyware to satisfy.⁸³ The whole purpose of spyware is to use an individual's computer as the vehicle by

⁷⁵ *Id.* at 234.

⁷⁶ Blakely et al., *supra* note 69, at 28.

⁷⁷ *Id.*

⁷⁸ *Id.* See also *Bailey*, 2:07-cv-11672-SFC-MKM (summary judgment granted to defendant husband who used spyware to learn wife's passwords and subsequently access her emails because such activity does not intercept any electronic files).

⁷⁹ Morgan, *supra* note 66, at 238.

⁸⁰ *Id.*

⁸¹ 18 U.S.C. §§ 2701-11.

⁸² *Id.* at § 2701(a).

⁸³ Blakely et al., *supra* note 69, at 20-26.

which it can obtain electronic information, easily satisfying the first element.⁸⁴ The intent element is relatively easy to prove by showing the spy actually accessed the computer's information.⁸⁵ The element requiring the spy to obtain electronic communication may be satisfied without much difficulty because the broad definition of "electronic communication" entails just about everything spyware is designed to track.⁸⁶ The final element is also not difficult to establish because the nature of spyware is to access information that is kept in electronic storage on the computer.⁸⁷

It is the third element of the Stored Communications Act, where the spy exceeds his or her authorization by installing the spyware, for the victim of spyware who is seeking legal redress under the Stored Communications Act. If the spyware installation occurred as a result of the user clicking through boilerplate language to download a different type of software, then this "click through" consent might count as the user giving authorization for the spyware to be installed.⁸⁸ Legislatively redefining "authorization" to exclude click through boilerplate language might solve the problem of satisfying this element, allowing the victim of spyware to succeed in his or her action against the spy.⁸⁹

In the case of a spouse using spyware to track and monitor the using spouse, there will be problems with the authorization prong. It will be very difficult for the victim spouse to show that the spying spouse did not have authorization to use the computer. The victim spouse can probably only show the spying spouse lacked authorization if the victim is the sole owner of the computer, he or she is the sole user of the computer, and he or she password protects the computer. Absent a showing of these types of factors that indicate the spying spouse had no authorization to use the computer, the spouse who is a victim of spyware

⁸⁴ *Id* at 22.

⁸⁵ *Id* at 23.

⁸⁶ *Id* at 25.

⁸⁷ Blakely et al., *supra* note 69, at 26.

⁸⁸ See *iLan Sys. Inc. v. Netscout Serv. Level Corp.*, 183 F. Supp.2d 328 (D. Mass. 2002) (holding that a boilerplate click through gave authorization for the installation of spyware).

⁸⁹ Blakely et al., *supra* note 69, at 27.

will probably fail in an action brought under the Stored Communications Act.

III. Advising the Client

In situations of domestic abuse, sound legal advice is critical for the client's safety and emotional well being. If a spouse suspects he or she is being spied on, it is important to know how to immediately address the spyware. If a client wants to use spyware on the other spouse, it is also important to know how to advise that client.

A. Preventing and Detecting Spyware

One may guard against being a victim of spyware through some simple measures. Installing good antispyware programs that will seek out the spyware and then destroy it is the best option.⁹⁰ Such programs that seek and destroy spyware include: Spy Sweeper, Ad-aware Pro, Spyware Eliminator, AntiSpy, XoftSpy, and Spyware Doctor.⁹¹ To increase one's chances of catching and eliminating all spyware on his or her computer, more than one of these anti-spyware programs should be run on the computer once a week.⁹² A firewall and a spam blocker program should also be installed on one's computer to help combat spyware.⁹³

It is important to note the methods that will *not* work in detecting spyware. Anti-virus software will not protect a computer against spyware.⁹⁴ Checking the list of installed computer programs will not reveal spyware programs that are on the computer.⁹⁵ Pressing control-alt-delete to view the programs currently running on the computer will not reveal spyware either.⁹⁶

In addition to installing and running several anti-spyware programs, a computer user should regularly update his or her op-

⁹⁰ Nelson & Simek, *supra* note 5, at 22.

⁹¹ *Id.*

⁹² *Id.*

⁹³ Spybot, <http://www.safer-networking.org/en/articles/recommendations.html> (last visited Mar. 28, 2008).

⁹⁴ Nelson & Simek, *supra* note 5, at 22.

⁹⁵ *Id.*

⁹⁶ *Id.*

erating system and web browsing software.⁹⁷ Advise a client to only download free software from reputable websites that can be trusted.⁹⁸ When downloading software, advise a client to read the licensing agreement and to keep his or her browser security setting at “medium” or higher.⁹⁹

One particular spyware program, called KeyKatcher, is most commonly used in the case of spousal spying where the spouses reside together.¹⁰⁰ KeyKatcher is a small device that one places between the computer’s keyboard and the keyboard port on the PC.¹⁰¹ Some of the KeyKatcher devices resemble a flash drive, while others look very similar to other types of plug and play units.¹⁰² Similar to a bugging device, KeyKatcher stores several weeks’ worth of keystrokes, which can then be removed and downloaded onto another computer.¹⁰³ Using KeyKatcher requires continued physical access to the computer, so it does not work well in situations where the spy and the victim do not live together.¹⁰⁴ To get rid of this form of spyware, the device should be physically removed and then destroyed.

B. Evidentiary Issues

The federal Wiretap Act does not allow the admission of evidence of a communication obtained through wiretapping in violation of the Act.¹⁰⁵ The exclusionary provision prohibits any evidence obtained through an illegally intercepted wire communication from being admitted at any trial or hearing in any court.¹⁰⁶ This rule of exclusion applies to federal and state proceedings as well as to criminal and civil proceedings.¹⁰⁷

⁹⁷ *Id.*

⁹⁸ Sean Carroll, *How to Avoid Spyware*, PC Magazine, <http://www.pcmag.com/article2/0,2704,1524265,00.asp>

⁹⁹ *Id.*

¹⁰⁰ Nelson & Simek, *supra* note 5, at 22..

¹⁰¹ KeyKatcher Home Page, <http://www.keykatcher.com/> (last visited Mar. 27, 2008).

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ Nelson & Simek, *supra* note 5, at 22..

¹⁰⁵ 18 U.S.C. § 2515.

¹⁰⁶ *Id.*

¹⁰⁷ Ann B. Frick & Marjorie J. Long, *Interspousal Wiretapping and Eavesdropping: An Update—Part II*, 24 *COLO. LAW.* 2569, 2569 (1995).

For this exclusionary rule to apply, “federal courts have consistently required that electronic communications be acquired contemporaneously with transmission in order to be intercepted within the meaning of the federal statute.”¹⁰⁸ How “interception” is construed by the court will therefore dictate whether the evidence is excluded.

Missouri does not allow communications obtained in violation of its Wiretap Act to be introduced as evidence in any civil or administrative proceedings.¹⁰⁹ An exception does exist, however: in civil actions brought pursuant to Missouri Revised Statutes section 542.418.2., the illegally obtained communication is admissible.¹¹⁰ In spite of the statute’s language, a trial court’s admission of evidence obtained through the violation of Missouri’s Wiretap Act will not be overturned if its admission is deemed harmless.¹¹¹

C. *The Significance of Spyware*

When a client is the victim of physical or sexual domestic abuse, safety issues need to be immediately addressed. The likelihood of future violence needs to be assessed.¹¹² If the threat of future violence exists, the attorney should assist the client in creating a plan for the client’s safety or refer the client to someone who can adequately help the client with such a plan.¹¹³

What is less obvious is how to assist a client with abuse that has taken the form of dominance and control, but not outright physical violence. That is the type of situation into which abuse through the use of spyware falls. Tracking a spouse through his or her computer habits establishes a pattern of control that can

¹⁰⁸ Sivalingam, *supra* note 6, at 4.

¹⁰⁹ MO. REV. STAT. § 542.418.1 (2006).

¹¹⁰ Missouri Revised Statute section 542.418.2 creates a civil cause of action permitting actual damages, punitive damages, and attorney’s fees to be brought by any person whose wire communications were illegally intercepted in violation of Missouri’s Wiretap Act.

¹¹¹ See *Lee v. Lee*, 967 S.W.2d 82 (Mo. Ct. App. 1998) (trial court’s admission in a dissolution action of recordings of husband’s telephone conversations that wife obtained in violation of Missouri Wiretap Act found to be harmless and therefore no error in admitting them).

¹¹² John M. Burman, *Lawyers and Domestic Violence: Raising the Standard of Practice*, 9 MICH. J. GENDER & L. 207, 240 (2003).

¹¹³ *Id.*

lead to a type of imprisonment that likely will not be taken as seriously as other, more “traditional” forms of abuse.

This type of imprisonment means the abusive spouse can monitor the victim’s contact with the victim’s support network by reading the victim’s e-mails and instant messages to those supporters. The abusive spouse can view whatever websites the victim has visited, thereby limiting the victim’s ability to research shelters and resources to help him or her leave the abusive relationship. Any e-mail communications the victim has with his or her attorney would be compromised. The abuser can gain access to the victim’s passwords and pin numbers if he or she uses them on the computer, which could lead to the abuser monitoring what financial transactions the victim has engaged in or might result in the abuser draining the victim’s financial accounts. The effects of spyware are far reaching. It will take careful advice to steer the client in the direction of protection and freedom from the abuse.

IV. Conclusion

At best, spyware is a nuisance that slows a computer and discloses personal information the user would rather not have disclosed. At worst, it is a tool for domination and control that can be used to scare, manipulate, and trap a victim into submission and helplessness. For a spouse who wants ultimate control over the other, it is a powerful tool that enables the abuser to monitor who the victim spouse communicates with, what financial transactions the victim engages in, and what documents that spouse drafts.

Currently, no criminal or civil remedies exist that effectively deal with the problem of spousal abuse through spyware. Civil remedies are inadequate largely because they came about at times well before the existence of spyware or computers and have not been adapted to include spyware. Criminal statutes that are designed to address computer tampering will probably not help the spouse who is a victim of spyware because it is implied in the marital relationship that a computer in the residence is accessible to both spouses. Even criminal statutes pertaining to domestic assault fall short because spyware does not overtly restrict the victim’s freedom of communication. One of the simplest ways to allow prosecution of a spouse using spyware to track, monitor, or control the other is to amend the current stalk-

ing statute¹¹⁴ to focus on the spy's knowledge that the conduct could cause substantial emotional distress and the spy's intent to cause the victim distress, rather than whether he or she actually succeeded in causing the emotional distress.

The federal and Missouri Wiretap Acts also provide little help to the spousal spyware victim because of their requirements that the wrongly viewed communication be used or disclosed in some way. There is also the matter of whether or not the spying spouse had authorization to use the computer.

Spyware can be difficult to detect. But by installing and running various spyware detection programs, unauthorized spyware can be found and removed from the victim's computer. It is important to advise a client in an abusive situation to not use the computer in the marital home without first checking for spyware by way of a spyware detection program. A client who has not yet appropriately checked the computer for spyware should not use the computer to write any e-mails, visit any websites, type in any passwords, or engage in any instant messaging that he or she would not want the abusive spouse to see.

It is also important to discourage a client who suspects his or her spouse of cheating from using spyware to confirm his or her suspicions. Evidence obtained through spyware is generally inadmissible and will do the client no good in most courts.¹¹⁵

The use of spyware on one's spouse to track, monitor, dominate, and control the victim spouse is an effect way to prevent that spouse from leaving the relationship or seeking help. Because it is not yet perceived to be as severe as other forms of abuse, it is not effectively addressed in today's legal schemes. A simple shift in the thought patterns of legislatures, citizens, victims, and advocates could go along way in empowering and protecting victims of domestic abuse.

Katherine Fisher Clevenger

¹¹⁴ MO. REV. STAT. § 565.225 (2006).

¹¹⁵ Frick & Long, *supra* note 109, at 2569.