August 17, 2010


Terese E Laubscher
Domestic Violence and Spyware: How and Why Spousal Abuse Through Spyware Lies

Outside the Protection of California Law and a Proposal for Reform

Terese Laubscher

May 3, 2010

Laubs100@chapman.edu
I. Introduction.

Imagine a situation of domestic violence where the wife lives in a state of constant fear of her husband.\(^1\) Instances of physical violence are very rare, so outsiders remain unaware of the abuse. The husband is constantly mentally and emotionally abusive, controlling where his wife goes, when she goes there, whom she speaks to, what she reads, and what money she spends. He is able to maintain control by monitoring her computer use, viewing every email she sends, every website she visits, and every chat in which she engages. He has access to her pin numbers, credit card numbers, and her social security number, and the wife does not even realize it. He knows the names, addresses, email addresses, and telephone numbers of all her family, friends, and coworkers. He knows if and when she contacts an attorney or battered woman’s shelter. If she is even thinking about leaving the relationship, he will know about it by viewing the content of her emails to her friends and family and her web browsing activities. He has the potential to be perpetually one step ahead of his wife, preventing every action she takes to assert her autonomy, search for help, or leave the relationship.

Under California’s criminal and civil scheme, the wife has no redress, should she find out about her husband’s spying. Her safety is threatened because the law does not protect her until her husband turns physically violent or overtly threatening, and her

\(^1\) Women are victims of domestic violence and men are perpetrators in the majority of cases. Men perpetrate approximately eighty-five to ninety percent of heterosexual partner violence reported to law enforcement. See, e.g., Bureau of Just. Statistics, “U.S. Dep’t of Just., Special Report: Intimate Partner Violence 2 (2000). For that reason, I will often use female pronouns when referring to victims of domestic violence and male pronouns when referring to perpetrators. The discussion in this article is also applicable to female violence against males.
ability to leave the relationship is compromised for as long as her computer activities are being monitored.

A victim should not have to wait until her abuser has become violent or threatening before she can take legal action. Changes in California’s criminal and civil schemes are required, so that the law provides a remedy for victims of spyware use by their spouse before the abuse escalates to a point of physical danger.

This paper argues that spousal monitoring through spyware is a form of domestic violence which California law currently does not recognize. Part II will explain what spyware is and how it is a form of domestic violence. Part III will analyze how current criminal and civil schemes in California are inadequate to address spousal use of spyware as a form of abuse. Part III will analyze why interspousal privacy has historically been unrecognized by the law, and will conclude with a proposed civil and criminal statute which remedies the holes found in California’s civil and criminal schemes.

II. Spousal Monitoring Through Spyware is Domestic Violence.

Spyware is monitoring software which allows an installer to essentially spy on the computer user, gathering information while remaining undetected in doing so. Current legal conceptions of what domestic violence is do not capture this type of ongoing monitoring behavior, and instead focus on specific acts of physical violence. Criminalizing spyware comports with other modern day proposals to redesign the statutory framework to reflect that domestic violence is more than discrete acts of violence, but an ongoing attempt to gain coercion and control over another.
A. What is Spyware?

Spyware is a type of monitoring software that is installed on a user’s computer without that person’s knowledge or consent. The software may be installed by one who has physical access to the computer, but can also be insidiously installed through email attachments that appear benign, such as a greeting card, or through hacking into a computer system via the internet. Spyware may also take the form of a device that is installed onto a keyboard to log every key stroke and store the data inside the device for the installer to retrieve whenever they next have access to the computer.

The software has the ability to monitor everything the user does on the computer, either through logging every keystroke and/or taking screen shots at regular intervals and then sending activity reports to the installer, usually through email. The information gathered can include passwords, credit card and Social Security numbers, the content of emails and activity on forums and in chat rooms.

Earthlink conducted a study in 2004 which found that, of the 2.1 million PCs scanned, there were nearly 54.8 million spyware applications found on the user’s computers. A great deal of the so-called “spyware” found on a typical user’s computer is actually “adware,” which is designed not to capture a user’s personal information, but...
to track their browsing habits to assist advertisers.\textsuperscript{7} True spyware remains undetectable on the computer system and many forms of antivirus and anti-adware software will not detect its presence on a system. It is therefore very difficult to ascertain how pervasive the use of actual spying software is.

As of 2004, it is estimated that some 73\% of American adults communicate via the internet – a figure that rises to 85\% for adults aged 18-27, 87\% for the 28-39 group, and 84\% for ages 40-49.\textsuperscript{8} Spyware manufacturers target their advertising towards spouses, with phrases like, “Catch cheating spouse,” and the programs typically cost under $100, which is considerably less than what one would pay for a private detective.\textsuperscript{9} While it is not currently known how many spouses are spying on one another with spyware, given that the majority of American adults communicate over the internet and given the ease and accessibility of spyware, the potential for it to become a tool of spousal abusers is enormous.

B. How is Spyware Domestic Violence?

In practice, domestic violence is an ongoing attempt by a batterer to gain total power and control over his victim. A batterer will utilize coercion and threats, intimidation, emotional abuse, isolation, economic abuse, male privilege, and minimizing and blaming in order to gain total control.\textsuperscript{10} On the “Power and Control Wheel,”\textsuperscript{11}

\textsuperscript{7} See supra note 2 at 21.
\textsuperscript{10} The Domestic Abuse Prevention Project, “Power and Control Wheel,” http://www.theduluthmodel.org/documents/PhyVio.pdf (last visited April 21, 2010).
\textsuperscript{11} See id.
physical and sexual violence are only the spokes that keep the control wheel in motion, utilized by batterers when the many other methods of domination have seemingly failed.

A batterer using spyware has the ability to extend his control into every area of the woman’s life – her finances, her relationships with friends, family, children, and co-workers. He can access her sensitive financial information and obtain all of her passwords. Because he can monitor with whom she is communicating and can read what she is saying, he is two steps ahead in knowing whether she is making arrangements to leave the relationship, or whether she is speaking with an attorney or a battered women’s advocate.

A batterer using spyware may never need to cross the lines into physical violence in order to gain total domination over his victim. His knowledge is his power, and by the time a victim becomes aware that her computer activities are being monitored, most of the damage has already been done. Once a batterer has knowledge of his victim’s passwords and sensitive personal information, it is very difficult for a victim to regain her privacy and ensure that the information will not be used against her, even after she has left the abusive relationship.

A victim can find herself almost paralyzed—afraid to use computers or electronic devices for fear she may still be under surveillance, afraid to leave the relationship out of fear that he already knows where she is going, or afraid to anger the batterer in any way, for fear that he has enough information on her to retaliate by causing serious damage to her finances or her professional or personal lives. A batterer using spyware has tremendous power over his victim, both during and after the relationship.
The true harm of domestic violence is precisely this type of deprivation of liberty, but the law currently fails to capture this harm. The criminal law is premised on a transactional model that focuses on discrete instances of physical violence or assault, and thereby hides the true context in which the abuse is occurring. These instances of physical violence are just one moment in time in what is typically a long history of the batterer scheming to gain total power over the victim, often through use of nonphysical means.

To understand why many of the harms suffered by battered women percolate outside of the boundaries of the law, it is important to understand the history of domestic violence law generally. Up until the late nineteenth century, marriage was structured to give a husband superiority over his wife in most aspects of the relationship, which included a right to corporal punishment or “chastisement” if she defied his authority. It was not until 1920 that all states had made the practice of wife beating illegal. In recent decades, domestic violence advocates have focused much of their efforts on forcing law enforcement and prosecutors to enforce laws that were already on the books, through “no drop” prosecution and mandatory arrest policies.

To a large degree, their attempts at procedural reform of the criminal justice system have been successful, but the laws that law enforcement are being pushed to enforce focus on discrete acts of violence or assault, and not on the ongoing pattern of

---

14 See id. at 969.
15 See id. at 970.
16 See id.
violence and its true harm.\textsuperscript{17} In order to give context to these discrete incidents, prosecutors must often rely on battering experts or evidentiary exceptions to bring in the entire history of the relationship—when it is, in fact, not history at all, but part of the ongoing crime.\textsuperscript{18}

Because the law itself does not adequately describe what domestic violence is, expert testimony is at times also necessary to repair a battered woman’s credibility, to explain to a jury why she stayed in the relationship or is afraid to testify, and to explain why a woman would commit a crime against her batterer in self-defense. As a result, the law has tended to explain battered women by focusing on the traumatizing psychological effect of battering on a woman—Battered Women Syndrome, “learned helplessness,” and the like—rather than on the actual conditions of entrapment in which she finds herself.\textsuperscript{19}

Professors Tuerkheimer\textsuperscript{20}, Stark\textsuperscript{21}, and others,\textsuperscript{22} have argued extensively for reforms in the way the criminal law characterizes the crime of domestic violence, pushing for a shift towards viewing it as a crime of pattern and intent. Tuerkheimer proposes that the existing legal structures be incorporated into a revised domestic violence statute, so that two or more incidents of violating one existing criminal statute, such as battering, against a current or former partner, would evidence of a course of conduct intended to result in substantial power and control over the victim.\textsuperscript{23} Criminalizing spyware use between spouses would enable such behavior to be part of that course of conduct. In that respect,

\textsuperscript{17}See id. at 972.
\textsuperscript{18}See id. at 997-8.
\textsuperscript{19}See supra note 12 at 1004-6.
\textsuperscript{20}See supra note 13.
\textsuperscript{21}See supra note 12.
\textsuperscript{22}See also, Alafair S. Burke, Domestic Violence as a Crime of Pattern and Intent: An Alternative Recategorization, 75 Geo. Wash. L. Rev. 552 (April 2007); Elizabeth M. Schneider, Symposium on Recategorizing Violence Against Women by Intimate Partners: Critical Issues; Epilogue: Making Recategorization of Violence Against Women Real, 58 Alb. L. Rev. 1245 (Spring 1995).
\textsuperscript{23}See supra note 12 at 1019-20.
this paper’s analysis of the ways in which spyware use by spouses falls within the cracks of the law compliments Tuerkheimer’s proposal, and also serves as yet another example of why such reforms of the law are necessary.

III. Analysis of Current California Law.

The criminal and civil scheme fails to adequately protect victims of spousal abuse through spyware because the laws either focus on physical injury, a threat of physical injury, or they fail to specifically state whether the trespasses and privacy invasions they address can occur between spouses, who often jointly own or jointly use their personal computers.

A. Criminal Statutes.

Current criminal abuse statutes fail to address spyware use because they either require a physical injury, physical contact, an attempt to make physical contact, or a threat to cause injury. Criminal computer tampering and invasion of privacy statutes do not specifically address instances where the parties are sharing a personal computer, and this leaves open the question of whether spouses are actually protected from one another under these statutes.

1. Spyware as Domestic Assault and Battery.

California has added criminal domestic battery laws specifically geared towards domestic violence victims, but they provide zero protection for a victim of spyware because they all require corporal contact or injury.

The “infliction of corporal injury” statute makes it a felony to willfully inflict corporal injury on a present or former spouse, cohabitant, former cohabitant, or the
mother or father of one’s child.\textsuperscript{24} The corporal injury must result in a “traumatic condition,” which is defined as, “a condition of the body, such as a wound or external or internal injury, whether of a minor or serious nature, caused by a physical force.”\textsuperscript{25} Spyware does not result in any physical injury.

Likewise, California’s domestic battery statute prohibits "any willful infliction of force or violence upon a current or former intimate partner."\textsuperscript{26} This is a simple battery statute, which unlike the corporal injury statute, does not require an injury. Any form of unwanted physical contact will suffice.\textsuperscript{27} A spyware victim would not have any protection under this statute, as spyware involves no physical contact with the person of another.

California’s criminal assault statues do not apply because they require an attempt to make violent or unwanted physical contact with one’s person, and such an attempt does not occur when one uses spyware against another.\textsuperscript{28}

None of the domestic assault and battery laws in California’s penal code cover the type of harm that spyware causes.

\textsuperscript{24} Cal. Penal Code §273.5 (Deering 2009) ("(a) Any person who willfully inflicts upon a person who is his or her spouse, former spouse, cohabitant, former cohabitant, or the mother or father of his or her child, corporal injury resulting in a traumatic condition, is guilty of a felony, and upon conviction thereof shall be punished by imprisonment in the state prison for two, three, or four years, or in a county jail for not more than one year, or by a fine of up to six thousand dollars ($6,000) or by both that fine and imprisonment.”).

\textsuperscript{25} See id.

\textsuperscript{26} Cal. Penal Code §243(e)(1) (Deering 2010) ("A battery is any willful and unlawful use of force or violence upon the person of another.”).

\textsuperscript{27} Judicial Council Of California Criminal Jury Instruction 841- Simple Battery: Against Spouse, Cohabitant, or Fellow Parent (Penal Code 243(e)(1)) ("The slightest touching can be enough to commit a [domestic] battery if it is done in a rude or angry way. Making contact with another person, including through his or her clothing, is enough. The touching does not have to cause pain or injury of any kind.”) See also People v. Rocha, 3 Cal.3d 893, 900 (Cal. 1971) ("It has long been established, both in tort and criminal law, that the least touching’ may constitute battery. In other words, force against the person is enough, it need not be violent or severe, it need not cause bodily harm or even pain, and it need not leave any mark.”).

\textsuperscript{28} Cal. Penal Code §240 (Deering 2010) ("An assault is an unlawful attempt, coupled with a present ability, to commit a violent injury on the person of another.”).
2. Spyware as Criminal Cyberstalking.

California’s stalking statute covers stalking behavior accomplished by electronic means, but is still insufficient to cover spyware use. The statute provides that “any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety” is guilty of the crime of stalking.\(^{29}\) The statute provides that the credible threat may be performed through electronic means and may be implied through a course of conduct, but the actor making the threat must *intend* to put the victim in reasonable fear for his or her safety or the safety of his or her family.\(^{30}\) A user of spyware often has no such intent, and so the statute fails to protect many victims of cyberstalking.

California led the nation in enacting the first stalking statute in 1990.\(^{31}\) The legislature decided to criminalize stalking in recognition of the fact that what may appear benign or merely annoying (i.e., following behavior), can often be the precursor to physical confrontations and violence, and the legislature expressed their desire to give victim’s a remedy before the stalking behavior reaches that point.\(^{32}\) But the statute’s requirement that the actor possess the specific intent to place the victim in fear has been

\(^{29}\) Cal. Penal Code §646.9 (Deering 2009) (“(a) Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking, punishable by imprisonment in a county jail for not more than one year, or by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment, or by imprisonment in the state prison.”).

\(^{30}\) See id.

\(^{31}\) Christine B. Gregson, Comment, California’s Ant stalking Statute: The Pivotal Role of Intent, 28 Golden Gate U.L. Rev. 221. See also Joseph C. Merschman, Note, The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation, 24 Harv. Women’s L.J. 255.

\(^{32}\) Gregson, see supra note 31 at 233-237.
criticized for its failure to cover certain cases of physical stalking, as well as the more recently criminalized electronic stalking scenarios.\textsuperscript{33}

In a traditional stalking scenario, where the actor physically follows the victim, rather than using electronic monitoring, the actor often wishes to remain hidden from the victim’s view, and has no intent of placing the victim in fear. This is even more the case when electronic means, such as spyware, are used. Spyware, by its nature, is a form of spying\textsuperscript{34} on another and the monitoring is purposely done in secret. The moment at which the victim of spyware becomes aware of the monitoring, the information gathered becomes almost useless to the spy, as the victim now knows to cease or limit the use of their computer(s).

California’s criminal cyberstalking statute offers no remedy for a victim of spyware.

3. Spyware as a Criminal Threat.

California’s criminal threat statute covers electronic communications, but would not cover spyware use because it requires that the actor threaten bodily injury. The statute makes in unlawful for one to willfully threaten “to commit a crime which will result in death or great bodily injury to another person.”\textsuperscript{35} The statute would therefore not cover spyware, since the installation of spyware on one’s computer does not

\textsuperscript{33} Gregson and Merschman, \textit{see supra} note 31.

\textsuperscript{34} Merriam-Webster Online, \url{http://www.merriam-webster.com/dictionary/spy} (last visited April 23, 2010) (“Spy” is defined as “to watch secretly, usually for hostile purposes”).

\textsuperscript{35} Cal. Penal Code §422 (Deering 2010) (“Any person who willfully threatens to commit a crime which will result in death or great bodily injury to another person, with the specific intent that the statement, made verbally, in writing, or by means of an electronic communication device, is to be taken as a threat, even if there is no intent of actually carrying it out, which, on its face and under the circumstances in which it is made, is so unequivocal, unconditional, immediate, and specific as to convey to the person threatened, a gravity of purpose and an immediate prospect of execution of the threat, and thereby causes that person reasonably to be in sustained fear for his or her own safety or for his or her immediate family’s safety, shall be punished by imprisonment in the county jail not to exceed one year, or by imprisonment in the state prison. . .”).

11
constitute a threat to commit bodily harm to another person. The threat conveyed must be “unequivocal, unconditional, immediate, and specific,”\textsuperscript{36} so even if spyware could be construed as conveying a threat of future harm, it would most likely not fall under this statute.

Spyware could not be considered a criminal threat under California law.

4. Spyware as Criminal Harassment.

California’s statute criminalizing harassing telephone and electronic communications does not apply to spyware because the law requires that the actor intend to harass the victim with his or her contact. The statute prohibits any contact made with a telephone or an electronic device that either threatens physical injury or is repeated.\textsuperscript{37} The actor must have the intent to annoy or harass.\textsuperscript{38} A user of spyware is not sending out any type of communication to their victim, nor would the user possess the intent to harass or annoy, as spyware users typically intend for their monitoring to remain a secret. Even if the victim were to become aware of the monitoring and felt annoyed and/or harassed, the victim would have no remedy under this statute unless he or she could prove the actor’s intent.

Victims of spyware do not appear to have a remedy under the electronic harassment statutes.

\textsuperscript{36} See id.

\textsuperscript{37} Cal. Penal Code §653m(a)-(b) (Deering 2009) (“(a) Every person who, with intent to annoy, telephones or makes contact by means of an electronic communication device with another and addresses to or about the person any obscene language or addresses to the other person any threat to inflict injury to the person or property of the person addressed or any member of his or her family, is guilty of a misdemeanor. [. . . .] (b) Every person who, with intent to annoy or harass, makes repeated telephone calls or makes repeated contact by means of an electronic communication device, or makes any combination of calls or contact, to another person is, whether or not conversation ensues from making the telephone call or contact by means of an electronic communication device, guilty of a misdemeanor.”).

\textsuperscript{38} See id.
5. Spyware as Criminal Computer Tampering.

It is unclear how much protection California’s criminal computer tampering statute would afford spouses who share a computer, as this statute requires that the tampering be done without permission. The statute criminalizes many different forms of accessing, modifying, damaging, copying, transmitting, and/or using data from a computer system, and spyware would certainly fall under those activities. But every act must be done “knowingly and without permission.” The statute itself does not contain a definition of what “permission” is or who would be considered an authorized user of the computer. There does not appear to be any case law involving the use of this statute in a domestic violence or marital context. The statute could foreseeably apply to spyware use between intimates who are not married and who do not share ownership and/or use of a computer, but it likely would not apply to spouses, both of whom may be deemed authorized users of a computer, either because they both use it or because they jointly own it under California community property law.

The applicability of California’s computer tampering law to spyware use between spouses is doubtful.

6. Spyware as a Criminal Invasion of Privacy.

The applicability of California’s criminal invasion of privacy statutes to spyware being used in a marital context is unclear. There are two sections in the Invasion of Privacy Act which seem to describe the type of monitoring that spyware accomplishes.

---

40 See id.
One section prohibits the unauthorized interception of information while it is in transit\textsuperscript{41} and the other prohibits eavesdropping on confidential communications.\textsuperscript{42} These statutes carry the same uncertainty as the computer tampering statute, discussed above, because whether the conduct is criminal or not hinges on whether the actor is an authorized user or whether the communication was confidential, and there is no case law applying the Act in a marital context. An authorized user of a computer system could be a spouse who jointly owns the computer or who regularly uses it. A court could find that spouses do not have the requisite reasonable expectation of privacy that their communications on such a computer be confidential and private.\textsuperscript{43}

\textsuperscript{41} Cal. Penal Code §631(a) (Deering 2009) ("(a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment in the state prison, or by both a fine and imprisonment in the county jail or in the state prison.").

\textsuperscript{42} Cal. Penal Code §632(a), (c) (Deering 2009) ("(a) Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.") ("(c) The term “confidential communication” includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.").

\textsuperscript{43} Flanagan v. Flanagan, 180 F. Supp. 2d 1089 (Cal. 2002) (finding that a conversation is confidential, for purposes of Cal. Penal Code §632, if a party to the conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded).
The applicability of the invasion of privacy statues in a marital context is doubtful.

B. Civil Statutes and Common Law.

Many of the civil actions discussed in this section require proof of damages, and victims very often do not suffer any damages beyond the intrusion into their peace of mind and solitude. Beyond this hurdle, the civil scheme fails victims in many of the same ways the criminal scheme does: the statutes either require physical injury, fear of physical injury, or they do not address whether spouses are afforded privacy between each other.

1. Spyware as Civil Stalking.

California’s civil stalking statute does not adequately cover spyware because it contains a requirement that the victim be in fear for his or her safety. Like the criminal statute,\(^44\) it encompasses stalking through electronic means, but unlike that statute, the civil version does not require the actor have the specific intent to create fear, but merely an intent to “follow, alarm, or harass.”\(^45\) A user of spyware frequently has the intent to follow, but a problem arises with the civil statute’s requirement that the victim

\(^{44}\) See supra note 29 and accompanying text.

\(^{45}\) Cal. Civ. Code §1708.7(a) (Deering 2009) (“(a) A person is liable for the tort of stalking when the plaintiff proves all of the following elements of the tort: (1) The defendant engaged in a pattern of conduct the intent of which was to follow, alarm, or harass the plaintiff. In order to establish this element, the plaintiff shall be required to support his or her allegations with independent corroborating evidence. (2) As a result of that pattern of conduct, the plaintiff reasonably feared for his or her safety, or the safety of an immediate family member. For purposes of this paragraph, “immediate family” means a spouse, parent, child, any person related by consanguinity or affinity within the second degree, or any person who regularly resides, or, within the six months preceding any portion of the pattern of conduct, regularly resided, in the plaintiff’s household. (3) One of the following: (A) The defendant, as a part of the pattern of conduct specified in paragraph (1), made a credible threat with the intent to place the plaintiff in reasonable fear for his or her safety, or the safety of an immediate family member and, on at least one occasion, the plaintiff clearly and definitively demanded that the defendant cease and abate his or her pattern of conduct and the defendant persisted in his or her pattern of conduct. (B) The defendant violated a restraining order, including, but not limited to, any order issued pursuant to Section 527.6 of the Code of Civil Procedure, prohibiting any act described in subdivision (a).”).
“reasonably feared for his or her safety” as a result of the stalking.\textsuperscript{46} The statute does not capture the true harm of spyware, which is not the fear it creates, but the intrusion on the victim’s autonomy and privacy. The civil statute does not supply an adequate remedy for victims who are not in fear, but who simply want to maintain their privacy.

2. Spyware under the Domestic Violence Prevention Act.

It is not clear from the Act’s definition of abuse and its list of enjoinable offenses whether there is a remedy for the use of spyware. The Act defines abuse as “(a) Intentionally or recklessly to cause or attempt to cause bodily injury. (b) Sexual assault. (c) To place a person in reasonable apprehension of imminent serious bodily injury to that person or to another. (d) To engage in any behavior that has been or could be enjoined pursuant to Section 6320.”\textsuperscript{47} Spyware does not fit (a) or (b) and does not always result in (c).

Section 6320 of the Act gives the court the authority to enjoin a party from “molesting, attacking, striking, stalking, threatening, sexually assaulting, battering, harassing, telephoning, including, but not limited to, annoying telephone calls as described in Section 653m of the Penal Code. . .”.\textsuperscript{48} One could make the argument that spyware is a form of harassing or stalking, but it is not a form of harassment or stalking under California civil and criminal statutes.\textsuperscript{49} Whether spyware is deemed stalking or harassment, for purposes of the Act, could hinge on which judge is hearing the motion. These statutes do not provide an adequate or reliable remedy for a victim of spyware, in part because the civil and criminal statutory framework does not encompass spyware.

\textsuperscript{46} See id.  
\textsuperscript{47} Cal. Fam. Code §6203 (Deering 2009).  
\textsuperscript{48} Cal. Fam. Code §6320(a) (Deering 2009).  
\textsuperscript{49} See supra notes 29 and 37 and accompanying text

California’s Consumer Protection Against Computer Spyware Act would afford no remedy to spouses who share a computer. The Act specifically and thoroughly addresses spyware software, but one only provides a remedy when a person who is not an “authorized user” has installed the software on the system. An “authorized user” is defined as a person “who owns or is authorized by the owner or lessee to use the computer.” Like the criminal computer tampering and invasion of privacy statutes, this statute fails to protect spouses who either jointly own a computer through California community property law, or who both regularly use the computer. This Act does afford a remedy for spouses.


A victim of spyware could bring an action in tort for the intentional infliction of emotional distress, but it is not a perfect remedy. Under California law, the tort requires that the defendant’s conduct be outrageous, that the defendant intended to cause or recklessly disregarded the probability that extreme emotional distress would result, and that the plaintiff did suffer extreme emotional distress. Assuming a spyware victim could convince a court that this type of monitoring is outrageous, the victim would then have to show that he or she suffered severe emotional distress and that this was the

51 Cal. Bus & Prof. Code §22947.1(b) (Deering 2009) (“(b) "Authorized user," with respect to a computer, means a person who owns or is authorized by the owner or lessee to use the computer. An "authorized user" does not include a person or entity that has obtained authorization to use the computer solely through the use of an end user license agreement.”).
52 See id.
53 See supra note 39 and accompanying text.
54 See supra note 41.
55 State Rubbish Collectors Ass’n v. Siliznoff, 38 Cal. 2d 330 (Cal. 1952) (finding that defendant had established a cause of action for intentional infliction of emotional distress by showing that plaintiff intentionally subjected him to mental suffering incident to serious threats to his physical well-being, even though the threats may not have constituted a technical assault).
defendant’s intent. As spyware user’s typically intend for their behavior to remain secret, it would be difficult to show that the actor intended severe emotional distress and many victims are not brought to a level of distress that could be characterized as severe.

Even a negligent infliction of emotional distress action would still require that the victim suffer severe emotional distress, and many spyware victims are not at that level. Spyware victims primarily want to stop the spying behavior to prevent further actions from the defendant which could result in extreme distress in the future.

While some spyware victims may have a tort action for infliction of emotional distress against their spouse, many do not.

5. Spyware as a Trespass to Chattels.

A spyware victim would not have a tort action for trespass to chattels because spyware typically does not impair or damage the function of a computer system. In California, one has an action for trespass to chattels against an actor who has intermeddled with or damaged their personal property. In recent years, the tort has been used in cases involving unauthorized uses of computers, such as computer hacking, but the California Supreme Court has held that the tort does not encompass trespasses which neither damage nor impair the function of a plaintiff’s computer system. Most forms of spyware do not cause any damage to the computer system, nor do they impair the use of the system. Spyware is purposely designed that way. The spyware serves no purpose for the installer if the victim is not able to regularly use their computer or if the victim

57 Thrifty-Tel v. Bezenek, 46 Cal. App. 4th 1559 (Cal. 1996) (finding that the act of defendant’s minor children hacking into plaintiff’s computer to retrieve a confidential code amounted to a trespass to chattels, not conversion).
58 Intel Corporation v. Hamidi, 30 Cal. 4th 1342 (Cal. 2003) (holding that the tort of trespass to chattels does not encompass, and should not be extended to encompass, electronic communications which neither damage nor impair the function of a plaintiff’s computer system).
becomes aware of the installation because their system is not functioning properly. A victim of spyware is not likely to recover under a trespass to chattels theory.

6. Spyware as an Invasion of Privacy by Intrusion.

The tort of intrusion upon seclusion does not afford an adequate remedy for a spouse who is being victimized by another spouse because it is unclear whether the victim-spouse has a reasonable expectation of privacy. At common law, the tort protects a plaintiff’s interest in the peace of mind gained from seclusion and isolation, and does not require that any publicity be given to the person whose interest is invaded.\[59\] The elements are (a) an intrusion into a private place, conversation, or matter, (b) in a manner highly offensive to reasonable person.\[60\]

Spyware involves an invasion into private conversations and matters, but the tort is proven only if the plaintiff had a subjective expectation of privacy that is objectively reasonable.\[61\] While spouses typically have a lower expectation of privacy between one another than they do with the outside world, there is still some zone of privacy that they retain between themselves.\[62\] To what extent a court would be willing to extend that zone is uncertain.

---

\[59\] *Vescovo v. New Way Enters., Ltd.*, 60 Cal. App. 3d 582 (Cal. 1976) (finding that a cause of action for invasion of privacy was shown because plaintiff child sought to recover for the physical intrusion by various unsavory characters on her own solitude, not for derogatory information about her mother in the ad).

\[60\] *Forsher v. Bugliosi*, 26 Cal. 3d 792 (Cal. 1980) (finding that the elements of a cause of action for invasion of privacy was stated because the depth of the intrusion was too miniscule).

\[61\] *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200 (Cal. 1998) (finding that triable issues of fact existed as to whether defendants broadcast journalists invaded plaintiff accident victims' privacy by accompanying plaintiffs in the helicopter and as to whether defendants tortiously intruded by listening to plaintiff's confidential conversations with a nurse at the rescue scene, without plaintiff's consent, and that defendants had no U.S. Const. amend. I privilege to intrude on plaintiffs' seclusion and private communications).

\[62\] *See infra* Part IVA.
The intrusion must also be one which would be highly offensive to a reasonable person. It would seem that a reasonable person would find being spied on by one’s spouse to be highly offensive. But with no cases available deciding the issue, a victim who pursues a cause of action under an intrusion of seclusion theory faces a high degree of uncertainty as to which way a judge would rule.

Although the intrusion upon seclusion tort accurately describes the harm created by spyware use, it does not satisfactorily protect one from an intrusion by his or her own spouse.

Neither the civil nor the criminal scheme in California provide a satisfying remedy for a victim of spousal abuse through spyware. The harm of this type of abuse is most analogous to an invasion of privacy by seclusion, but the law is not clear or settled on whether interspousal privacy actually exists. The next section of this paper discusses why it should exist and proposes a criminal and civil statute which specifically addresses spyware use between spouses.

IV. Proposals for Reform.

California law should be reformed in the following ways: (A) the law should reflect that there is a reasonable expectation of privacy in marriage which would protect spouses from spyware use against one another, and (B) there should be a criminal and civil statute which specifically criminalize and provide remedies for domestic abuse through spyware.

Miller v. National Broadcasting Co., 187 C.A.3d 1463 (Cal. 1986) (finding that plaintiff must meet the Restatement test of "highly offensive to a reasonable person" and explaining that a court determining the existence of offensiveness would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder’s motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded).
A. Spyware Should Be Treated as an Invasion of Privacy.

Traditional notions of privacy were created with an aim to protect an individual’s private or personal life from the outside world, but not to protect spouses from one another. Just as the old doctrine of coverture fails to reflect society’s current ideas of marriage, so is any notion that there is no expectation of privacy within a marriage.

1. Expectation of Privacy in Marriage.

The idea of a common law right to privacy was first introduced by Samuel Warren and Louis Brandeis in their oft-cited Harvard Law Review article from 1890. In it, the authors briefly tracked the evolution of the law, from a focus on protecting the physical world of property, to the corporal world of bodily sensations, and then later into the world of ideas, thoughts, and feelings, as reflected through nuisance, assault, and intellectual property laws. The authors expressed concern that recent technological innovations, particularly cameras used by the press, were creating evermore intrusions into the private lives of ordinary persons, and this led them to formulate the concept of a right to privacy, or a right “to be let alone.” Following their article, Dean Prosser described four different types of privacy invasions, and these were later incorporated into the Restatement of Torts.

Brandeis and Warren were primarily focused on intrusions from the outside world into the sphere of one’s personal and family life, not on intrusions between spouses. The discussion a privacy right between spouses would likely have seemed ridiculous at that

---

65 See id. at 193-5.
66 See id. at 195-6.
68 The four privacy torts are intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity that places a person in a false light. Restatement (Second) of Torts §652A-E (1977).
time, given that up until the nineteenth century, the legal doctrine of coverture applied to married women.\(^\text{69}\) Under coverture, a woman’s legal identity was merged into that of her husband upon marriage, forming one legal entity, with the wife subordinated to her husband.\(^\text{70}\) The wife gave all of her legal rights to her husband, including her right to own property, enter into contracts, and manage her earnings.\(^\text{71}\) When husband and wife were considered one entity under the law, the idea of there being any privacy between them would be nonsensical.

Over the last two centuries, the coverture doctrine has eroded, with the passage of the Married Women’s Property Act by various states, changes in divorce laws, and the erosion of the spousal immunity doctrine.\(^\text{72}\) The law has also begun to recognize a right of spouses to communicate privately with other persons.\(^\text{73}\) These trends seem to signal a societal and legal recognition that spouses are autonomous legal entities in partnership,\(^\text{74}\) and not a single entity. California law gives spouses the same rights and duties towards

---


\(^{70}\) *See id.*

\(^{71}\) *See id.*

\(^{72}\) *See id.* at 2113-4.

\(^{73}\) *See id.* at 2115.

\(^{74}\) Cal. Fam. Code §721 (Deering 2009) (“(a) Subject to subdivision (b), either husband or wife may enter into any transaction with the other, or with any other person, respecting property, which either might if unmarried. (b) Except as provided in Sections 143, 144, 146, 16040, and 16047 of the Probate Code, in transactions between themselves, a husband and wife are subject to the general rules governing fiduciary relationships which control the actions of persons occupying confidential relations with each other. This confidential relationship imposes a duty of the highest good faith and fair dealing on each spouse, and neither shall take any unfair advantage of the other. This confidential relationship is a fiduciary relationship subject to the same rights and duties of nonmarital business partners, as provided in Sections 16403, 16404, and 16503 of the Corporations Code, including, but not limited to, the following: (1) Providing each spouse access at all times to any books kept regarding a transaction for the purposes of inspection and copying. (2) Rendering upon request, true and full information of all things affecting any transaction which concerns the community property. Nothing in this section is intended to impose a duty for either spouse to keep detailed books and records of community property transactions. (3) Accounting to the spouse, and holding as a trustee, any benefit or profit derived from any transaction by one spouse without the consent of the other spouse which concerns the community property.”).
one another as nonmarital business partners. Our current conception of marriage resembles more of a contract than an institution, and the premise on which spousal immunity was based—that marital harmony trumps individual freedoms—is no longer consistent with society’s view of marriage.

The law of communications privacy has recognized a zone of privacy between spouses. Federal law imposes criminal penalties on “whoever” interferes with the postal mail, regardless of whether that person is taking or opening their own spouse’s mail. California has enacted laws designed to protect conversational privacy, and there seems little rational for creating a marital exception for electronic communications, but not for postal mail.

Every expectation of privacy must be objectively reasonable, and one naturally expects less privacy with their own spouse than they do with the outside world. Spouses are able to view mail left opened on the kitchen counter, they can eavesdrop on each other’s conversations that take place in the family home, and they often use one another’s personal computers. Spouses typically expect these types of intrusions, but few expect the type of intrusion created by spyware use, where one spouse is able to monitor everything the other spouse does on the computer—all while evading detection. There is certainly a reasonable expectation of privacy that remains between spouses.

---

75 See id.
76 18 U.S.C. §1702 (2000) (“Whoever takes any letter, postal card, or package out of any post office or any authorized depository for mail matter, or from any letter or mail carrier, or which has been in any post office or authorized depository, or in the custody of any letter or mail carrier, before it has been delivered to the person to whom it was directed, with design to obstruct the correspondence, or to pry into the business or secrets of another, or opens, secretes, embezzles, or destroys the same, shall be fined under this title or imprisoned not more than five years, or both.”).
77 See supra Part III.
2. Proposed Civil and Criminal Statute.

Given that none of California’s wiretap, spyware, and invasion of privacy statutes specifically address whether they apply to spouses, one who wishes to pursue a criminal or tort action against a spouse is left with a considerable amount of uncertainty as to which way the case would go. Whether an action would succeed could depend simply on the willingness of the judge to take interspousal privacy seriously. For this reason, this paper presents a previously proposed civil statute and proposes a new statute carrying criminal penalties. The new statutes require that all authorized users of a computer consent to the installation of the spyware.

Calman\(^{78}\) proposes a civil statute which reads as follows:

(a) Except as otherwise provided in this statute, any person who knowingly installs on a computer, or knowingly receives data from, surveillance software, keystroke recording software or hardware, or screenshot recording software or hardware, without the knowledge and consent of all authorized adult users of that computer, shall be subject to a civil action by any adult owner or adult authorized user of that computer whose computer activity or communication is intercepted, accessed, or disclosed.

(b) In an action under this section, appropriate relief includes -

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) It shall not be unlawful under this statute for an employer to install or receive data from a computer owned by the employer and used by an employee or independent contractor.

(d) It shall not be unlawful under this statute for a state or federal law enforcement officer, employee, or agent in the normal course of his or her official duties to use surveillance software or hardware if duly authorized by warrant.

\(^{78}\) See supra note 69.
(e) Whenever computer activity or communication has been intercepted or accessed as provided in section (a), no part of the contents of such communication or activity and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.79

The civil statute proposed by Calman would provide spouses who are being victimized by spyware a civil remedy for such abuse, including injunctive relief. With a statute on the books specifically addressing spyware and specifically providing that all authorized users of the computer must consent to its installation, a spouse wishing to receive a protective order under the Domestic Violence Protection Act would therefore have a stronger argument that spyware behavior is an enjoinable activity.80 The victim may also wish additionally to pursue an intentional infliction of emotional distress action, or an intrusion on seclusion action, and the existence of a spyware statute like the one Calman proposes would greatly aid such a plaintiff in showing the outrageousness of the behavior and in showing the offensiveness of the intrusion.81 Calman’s proposed civil statute provides appropriate civil remedies for a victim of spousal abuse through spyware.

In light of the enormous potential for spyware to be used in the domestic violence context,82 this paper would go a step further and create a companion criminal statute, one which specifically applies towards spouses and former spouses, cohabitants or former cohabitants, persons with whom the defendant has a current or former dating or engagement relationship, parties with a child in common, and parties related by

79 See supra note 69 at 2129-30.
80 See supra Part IIIB2.
81 See supra Part IIIB4,6
82 See supra Part IIB
consanguinity or affinity within the second degree.\(^83\) This would make the statute a domestic violence statute that protects all current or former partners, and not just spouses. As discussed in this paper, spouses are left particularly vulnerable to spyware abuse under California law, but there seems little reason to exclude the other listed classes of persons from the statute’s protection.

The criminal statute should include the language in subsection (a) of Calman’s civil statute, but should provide for criminal penalties, rather than a civil action. The appropriate criminal penalties should mirror the infliction of corporal injury on a current or former partner statute, the commission of which is a felony, punishable by “imprisonment in the state prison for two, three, or four years, or in a county jail for not more than one year, or by a fine of up to six thousand dollars ($6,000) or by both that fine and imprisonment.”\(^84\) The penalty for inflicting corporal injury on a former or current partner seems the best point of comparison for the spyware statute, which involves intentionally invading into the seclusion and privacy of one’s current or former partner or close relative.

The criminal invasion of privacy statute carries lesser penalties, making the crime a misdemeanor punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail or prison not exceeding one year, or

---

\(^83\) Cal. Fam. Code §6211 (Deering 2010) (“‘Domestic violence’ is abuse perpetrated against any of the following persons: (a) A spouse or former spouse. (b) A cohabitant or former cohabitant, as defined in section 6209. (c) A person with whom the respondent is having or has had a dating or engagement relationship. (d) A person with whom the respondent has had a child, where the presumption applies that the male parent is the father of the child of the female parent under the Uniform Parentage Act (Part 3 (commencing with Section 7600) of Division 12). (e) A child of a party or a child who is the subject of an action under the Uniform Parentage Act, where the presumption applies that the male parent is the father of the child to be protected. (f) Any other person related by consanguinity or affinity within the second degree.”).

\(^84\) See supra note 24 and accompanying text.
both.\textsuperscript{85} The criminal spyware statute this paper proposes should carry the harsher penalties imposed by the corporal injury on current or former partner. The harm of being spied on by one’s intimates should be viewed no differently than the harm of being physically injured by one’s intimates, as both are part of the larger ongoing attempt to gain coercive control which characterizes domestic violence.\textsuperscript{86}

The language in subsection (b) would therefore not be necessary in the criminal statute. The exception for employers in subsection (c), for law enforcement in subsection (d), and the evidentiary exclusion contained in section (e) should be included in the criminal statute as well.

Until California law reflects a right of interspousal privacy, through case law or otherwise, the civil and criminal statutes proposed in this paper are required in order to bring victims of spousal abuse of spyware under the law’s protection.

V. Conclusion.

Spyware has the ability to be a powerful tool for a batterer, whose objective is to gain total control over his victim in every area of her life. In California, the criminal and civil schemes do not provide an adequate or reliable remedy for a spouse-victim who wishes to take legal action against a spouse-batterer who has installed spyware on her computer. California should enact a civil and criminal statute that requires all authorized users of a computer to consent to the spyware installation. California privacy law should mirror current social and legal conceptions of marriage by reflecting that marriage is a partnership between autonomous individuals and that there is a zone of privacy that

\textsuperscript{85} See supra note 46 and accompanying text.  
\textsuperscript{86} See supra Part IIB.
spouses retain between themselves. This would go a long way towards ensuring that new forms of marital spying technology introduced in the future will not also fall outside the protection of the law.