

**THE ROLE OF INFORMATION SECURITY IN DOMESTIC ABUSE:  
A CALL TO ACTION**

Cindy Chadwick

Capstone- 68-595K-SP12  
Master of Science/Information Security  
Lewis University, Romeoville, IL

May, 2012

## Abstract

Information security is paramount to personal security for victims of domestic abuse. Victims therefore need knowledge of how to protect certain types of information in order to protect their own--and often their children's--personal safety. This paper will demonstrate that the information security community is well positioned to help in the already-established effort to secure the safety of domestic abuse victims, both through direct information safety counseling as well as through providing training, education and advice to domestic abuse service providers. A model is provided for integrating the contributions of these and other professionals into the service structure of established providers in order to maximize the benefits obtained. Another information security issue--collecting and presenting digital evidence--is also examined. Abusers seek to exert absolute control over their victims, including financial control. Therefore, when a victim leaves her abuser, she often does so with no financial means to use in subsequent restraining order or custody hearings. She is often, then, forced to collect and present her own evidence to substantiate her claims of abuse. Frequently, that evidence is in the form of electronic media. Judges, then, must have the knowledge needed to take such evidence under consideration without the benefit of having an expert computer forensics witness provided by the person who alleges abuse. Currently, much electronic evidence used to substantiate abuse is based on social-media and/or text messages. This is an emerging field of evidence in the courts, however, with admissibility being treated very differently within and between court jurisdictions. After addressing the law currently applied to evaluating the admissibility of electronic evidence--the Stored Communications Act of 1986--this paper argues for an updating, not only of the law but also of the way in which rules of evidence are created in response to evolving technologies.

## Table of Contents

<b>I. Introduction .....</b>	<b>Page 1</b>
<b>II. Background</b>	
<b>A. Domestic Abuse Definition and Patterns .....</b>	<b>Page 10</b>
<b>B. Why Domestic Abuse Victims         Need Information Security</b>	
1. What Is Information Security? .....	Page 16
2. Electronic Weapons: The Victim's Own Computer .....	Page 19
3. Electronic Weapons: Snooping Tools .....	Page 23
4. Electronic Weapons: Tracking Tools .....	Page 25
5. Electronic Weapons: Webcams .....	Page 28
6. Electronic Weapons: Publically-Available Information .....	Page 31
<b>III. Information Security and Documenting Abuse         for Presentation in Court</b>	
<b>A. The Significance of Evidence Collection         And Admissibility: <i>Tagle vs. Garcia</i> Case Study .....</b>	<b>Page 38</b>
<b>B. Challenges of Determining Admissibility         of Electronic Evidence .....</b>	<b>Page 44</b>

## Table of Contents (Cont'd)

### IV. Meeting the Need

#### A. Information Security Provision:

Education vs. Counseling .....	Page 51
--------------------------------	---------

#### B. Recommendations for the Information Security

Community .....	Page 56
-----------------	---------

#### C. Recommendations for Domestic Abuse

Service Providers .....	Page 60
-------------------------	---------

#### D. Recommendations for Legislation, Standards and Guidelines .....

Page 67

E. Recommendations for Further Research .....	Page 68
---	---------

#### F. Recommendations for Information Security Strategies for Domestic Abuse Victims .....

Page 71

V. Conclusions .....	Page 74
----------------------	---------

References .....	Page 80
------------------	---------

#### Appendix A:

Spyware and Tracking-Tool Advertisements .....	Page 84
--	---------

#### Appendix B:

Professional Organizations Resource List .....	Page 94
--	---------

## I. Introduction

The impetus for this paper was a chance remark made by an employee of a retail outlet for an international company that dominates the computer, cell phone, digital music and electronics markets. She relayed an incident in which a woman came into the store seeking help in retrieving text messages from her phone. The woman's intent was to use the messages in order to substantiate abuse by her spouse. Referencing the abuse, the woman reported that her husband often locks her in the attic of their home and then leaves the house for hours. When the employee recounting the story was asked if other instances wherein abuse victims sought help in retrieving evidence of abuse had occurred, she related that it is actually a trend observed in the store at which she works for this to happen several times a month.

One of the most striking elements of the account of the woman who related being held captive in her own attic was that she actually *identified* herself as an abuse victim. Much of what one reads in the news media regarding domestic abuse emphasizes the reluctance of those who are subjected to domestic abuse to identify themselves as an 'abuse victim', as it is a socially stigmatizing label that references an oftentimes taboo subject. As noted by the National Center for Victims of Crime [1], "Victims, because they fear the perpetrator and may be ashamed of their situation, may be reluctant to disclose the abuse to family, friends, work, the authorities, or victim assistance

professionals. As a consequence, they may suffer in silence and isolation.” The fact, then, that this women would identify herself to a complete stranger as an abuse victim appeared to be a reflection of the urgency of her plight and of the mission that she was on to document that plight.

Collection of electronic evidence<sup>1</sup> (computer forensics), it so happens, is an area of study in the field of information security. Thus, through one retail worker’s observations of a trend in a single electronics store, a very tentative connection was made between the profession of information security and the social issue of domestic abuse. There appeared to be a potential intersection between the two that merited exploration.

The first question to be addressed was whether or not other stores retailing similar electronic devices evidenced a similar trend of abuse victims turning to them for assistance in collecting digital evidence of abuse. To that end, a number of cell phone and computer stores were informally canvassed, all in the same state. The canvassing took place in ten stores in three geographic locations: a medium-sized city, a medium-sized town that serves as a bedroom community to that city, and a small town that is a satellite community to the state capitol. Approximately eighteen employees were interviewed, and both vendor-owned and authorized-dealer stores were canvassed. Employees of the latter were the most forthcoming about talking to a researcher about

---

<sup>1</sup> For the purposes of this paper, the terms ‘electronic evidence’ and ‘digital evidence’ will be used interchangeably.

the issue, although all would acknowledge in some way that their stores have also experienced abused women<sup>2</sup> coming in seeking assistance with digital issues related to the abuse. Authorized-dealer employees were more willing to put an estimate on how often their stores experience this type of request for assistance, and the most common answer was “three to four times a month.” Interestingly, some of the employees in these stores had formerly worked in the larger vendor-owned retail outlets, and they reported that they had observed the same trend in those stores, as well.

Abuse victims<sup>3</sup> were reported to seek help from these phone and electronics stores for two main purposes: 1. retrieving text messages sent from the abuser (in order to present them in court), and 2. learning how to remove spyware that was planted onto their phones and computers by the abusers. As to the latter of these two concerns, the forms of spyware specifically mentioned were keyloggers, which record every key typed on a device (including passwords), and GPS devices (described later in this

---

<sup>2</sup> Statistics on domestic abuse, its prevalence, and impact by gender vary greatly, partly due to the methodology used to collect the data (e.g. many victims do not report abuse to the authorities, so crime statistics on abuse will not reflect the true prevalence) and partly due to varying definitions of *domestic abuse* or *domestic violence*. The Domestic Violence Resource center, however, calculated a statistic from a report by the Bureau of Justice Statistics [29] that leaves no uncertainty about definitions of ‘violence’ or ‘abuse’: on average, more than three women and one man are murdered by their intimate partners in this country every day [30]. Due to the fact that domestic violence, on the whole, exerts a greater impact on women than men, then, this paper will address victims with the feminine gender. It is important to remember, however, that men are also sometimes the victims. It is noteworthy, as well, to keep in mind that intimate partner abuse may be same-gender (in the case of gay or lesbian intimate relationships.)

<sup>3</sup> It should be noted that, unlike the woman in the first account given of an abuse victim seeking help, many of these women do not identify themselves as being abuse victims, which, as mentioned above, is more to be expected. The store employees, however, report that there is no doubt in their minds as to these women’s status as abuse victims. They report that the women make references to needing information “for court”, that they are “emotional wrecks”, “nervous”, “constantly watching over their shoulder, looking back at the door,” and otherwise characterize them in ways that are descriptive of typical abuse victims.

paper), which are used to track the partner's movements. While the women's inquiries about retrieving text messages reflected a need for knowledge about electronic evidence collection, the help they sought in removing snooping devices and software raised the specter of a need on their part for information security knowledge and strategies of a more global nature. This broader intersection of the field of information security with the issue of domestic violence was the next area, then, to be explored.

To that end, a review was conducted of literature written by professionals working in the field of domestic abuse, along with writings by abuse victims who have used electronic forums and blogs to share their personal experiences. What emerged from these many voices was a stark, unified message: women in abusive relationships require near military-grade information security in order to protect not only their privacy but also their personal safety (and perhaps that of their children, as well.)

These preliminary investigations served to verify that there is indeed an intersection between the social issue of domestic abuse and the field of information security. This paper will demonstrate this connection and detail its implications for the victims of abuse, those who currently serve them, and the information security professionals who could join the ranks of the latter, to the great benefit of the former. It is hoped that, as a result of this illumination of the role that information security plays in domestic abuse, the information security community will recognize an opportunity



to share of their knowledge and skills in order to participate in the worthy cause of protecting domestic abuse victims.

Before one can understand the role that information security plays in domestic abuse, however, one must first have a good understanding of what domestic abuse is and the role within it played by the abuser's need for absolute control over his partner.

## II. Background

### A. Domestic Abuse Definition and Patterns

“Domestic abuse occurs when one person in an intimate relationship or marriage tries to dominate and control the other person. Abusers don't ‘play fair.’ They use fear, guilt, shame and intimidation to wear you down and gain complete power over you. They may threaten you, hurt you or hurt those around you. Domestic abuse that includes physical violence is called domestic violence.”

As this description of domestic abuse by U.S. Army victim advocate coordinator Cora Hodges [2] highlights, domestic abuse is not as simple as occasional outbursts of anger that lead to physical assault. Rather, it is a systematic effort to gain and maintain control over an intimate partner. Hodges says that the commonly-believed myth that domestic violence is a result of the abuser “losing control” thus misses the mark. Instead, she explains, violence is a very conscious choice that the abuser makes in his campaign to exert complete control over his partner’s life. This control is often exerted emotionally, physically, sexually, and financially. Importantly, it is also exerted over the information flow to and from the victim, which will be a focus of this paper.

Emotional abuse, according to phsyccentral.com [3], includes, “any action intended to degrade, humiliate or demean, both in public or private. This includes verbal threats, yelling, intimidation, harassment, criticism, lying, withholding information and isolation from family or friends.” Hodges notes that emotional abuse also often takes the form of shaming, blaming, and name-calling. This is far from an exhaustive list of the shapes emotional abuse might take<sup>4</sup>. The point to be made is that emotional abuse is a weapon wielded by the abuser in order to undermine the victim’s feelings of self-worth and independence. With her self-confidence eroded to nothing, the woman often believes the abuser when he tells her that she cannot make it without him.

Often an abuser will begin with emotional abuse and over time escalate to physical abuse. Physical abuse includes, “Any act of violence that is designed to control, hurt, harm or physically assault a partner. This includes pushing, punching, kicking, grabbing, pulling hair, choking, slapping, damaging property or valued items, the use of weapons and refusing to help a sick partner.” [3]

Abusive behavior can include sexual coercion and humiliation. Abusers may even drug their partner before initiating unwanted sexual behavior. One woman interviewed for this paper reported that her husband would drug her into

---

<sup>4</sup> It is important to note that one incident of such abusive behavior does not an abuser make. Rather, each of these behaviors is part of an overall *pattern* of emotionally-abusive behavior that leads to labeling the perpetrator as an ‘abuser’.

unconsciousness, and later she would awaken to discover him sodomizing her. Make no mistake: this is *not* an issue of sexual desire. Rather, it is again an effort to dominate, humiliate and--above all else--control.

Technology is emerging as a dominating force in how these abuse patterns are manifested in the relationship. Dr. Lynn Tovar [4], Associate Professor of Justice, Law and Public Safety Studies at Lewis University (Chicago), and her collaborators at California Lutheran University (Thousand Oaks), for instance, are exploring a relatively new element in the domestic abuse pattern: the abuser's use of text messaging to constantly monitor the moves of his victim and to exert a continual, unrelenting presence in the victim's daily life. In the second part of a two-part study on this subject, Dr. Tovar has begun conducting interviews with abuse victims. Initial interviews reveal that texting has enabled some abusers to insert themselves into the lives of their victims in ways unparalleled in times past. Now, the woman can go nowhere to escape her abuser. He will text her at work, at school, and as she does her errands or visits friends. These women report that they suffer from a constant lack of peace, that there is no escaping their abusers. Some women in relationships with men who stalk them via texting report that the man will keep them awake most of the night texting them. If they do not answer, he will become increasingly agitated, mean, and threatening. The resulting sleep deprivation, these women say, makes it difficult to focus and reason.

An often-raised question about domestic abuse is why the victim does not leave the abuser. While there are many reasons<sup>5</sup> that a victim will remain with her abuser, financial dependency is often a major factor for her continuing to stay in the relationship. Following are examples of ways in which an abuser may hold his victim under his financial control:

- controlling all family finances, including cash, bank accounts, and credit cards
- making all financial decisions, down to the last dollar spent
- allocating the victim only a small allowance, for which she is accountable for every cent spent
- taking away or stealing any money the victim has on her own
- withholding basic necessities such as food, clothes, medicine or shelter
- sabotaging the victim's job (making her miss work, calling or showing up at her job constantly, preventing her from using a car, etc.)

Compounding her lack of financial resources is the lack of credit. If the abuser has kept all accounts in his name, then the woman will have no credit history that can assist her, for instance, in getting a loan to help her leave and start a new life.

---

<sup>5</sup> The question of why women stay in abusive relationships is a stumbling block for many people. They cannot consider the plight of the abuse victim, because they cannot move beyond the question of, "Why doesn't she just leave?" The reader is encouraged to read the well-documented and thoughtful article [31] by Susan McGee that addresses this issue. McGee served as the director of a comprehensive domestic violence program in southeastern Michigan for over twenty years. Additional explanations are provided in a list [28] compiled by the Community Anti-violence Alliance.

Another characteristic of abusers that it is important to understand is that they are typically exceedingly good at appearing to be incapable of the acts that they commit. The Alabama Coalition Against Domestic Violence reports [5] that, “They (*abusers*) often appear charming and attentive to outsiders, and even to their partners, at first. Many perpetrators are very good at disguising their abusive behavior to appear socially acceptable. Once they develop a relationship with a partner however, they become more and more abusive.” Interviews with those who work with domestic abuse victims confirm the assessment that abusers often appear quite charming. That charm is often put to use to win over judges as well as police officers called to the scene of a domestic violence incident. Moreover, as it is the abuse victim who is emotionally battered, it is often she who appears to be the ‘unstable’ one in the relationship. By remaining cool, calm, rational-sounding and charming, the abuser may appear--even to family--to be the more believable of the pair, as the woman may come across, by contrast, as hysterical, incoherent and irrational. All of this, of course, is by design.

Another hallmark of abusers is their remarkable ability to manipulate others. Langbein and others note that abusers are so good at manipulating the system, in fact, that it is not unusual for the abuser to be the parent to whom custody of the couple’s children is awarded. The Alabama Coalition Against Domestic Violence notes that

abusers may also manipulate the system in the following ways [5]:

- Threatening to call Child Protective Services or the Department of Human Resources and making actual reports that his partner neglects or abuses the children.
- Changing lawyers and delaying court hearings to increase his partner's financial hardship.
- Telling everyone (friends, family, police, etc.) that she is "crazy" and "making things up."
- Using the threat of prosecution to get her to return to him.
- Telling police she hit him, too.
- Giving false information about the criminal justice system to confuse his partner or prevent her from acting on her own behalf.
- Using children as leverage to get and control his victim.

As previously noted, the abuser's need for complete control over his victim's life--and part of the way in which he realizes that control--extends to the flow of information to and from the victim. The dangers that this presents to the abuse victim are manifold and will be explored in the next section.

## B. Why Domestic Abuse Victims Need Information Security

### 1. What is Information Security?

The field of information security provides services to secure the confidentiality, the integrity, and the availability<sup>6</sup> of information. While many people associate this role with the protection of electronic data, ‘information’ means just that: information in any format, be it hardcopy (e.g. paper), digital (e.g. on a computer or cell phone), spoken (e.g. phone conversation), or nonconventional (e.g. in a school for the deaf, for instance, the confidentiality of conversations would be complicated by the fact that a signed conversation can be read from a much greater distance than a spoken conversation.) Information to be protected can even be *implied* information. For instance, if a person’s usual communication methods and patterns evidence a sudden and dramatic change, an ‘insider’ (someone who knows that person well) might be able to draw certain conclusions from these changes. It will be demonstrated that all of these concerns of the information security profession--confidentiality, integrity, and availability of information--are equally important to the abuse victim. In many cases, these concerns are arguably *more* important to her, for her very life may depend on her ability to secure her information.

---

<sup>6</sup> Confidentiality, integrity and availability are collectively known as *the CIA Triad*, a model commonly used in the Information Security profession to identify characteristics of information that need to be protected.



This last point is well-demonstrated by a case that involves information *confidentiality* that is cited by Cindy Southworth [6], Vice President of Development and Innovation at the National Network to End Domestic Violence (NNEDV). Southworth relates the account of an abused woman who had decided to leave her husband. The woman found a new home for herself and her two daughters and then emailed a friend to ask for help moving to her new home. She carefully deleted the email to prevent her husband from reading it and thereby discovering her plans. The husband, though, found the 'deleted' email in his wife's 'deleted email' folder on her computer and killed her. The lack of confidentiality of this woman's information, then, resulted in her murder. This case demonstrates that, for an abuse victim, information security can be of a more urgent and desperate nature than even that which is dealt with by the vast majority of practitioners within the information security field. Yet the abuse victim must deal with this continual threat while not possessing even a fraction of the knowledge that the professional has at his disposal.

While confidentiality of information was the issue in the case just cited, the importance of *integrity* of information is central to a practice employed by some abusers. 'Caller id spoofing' involves using a calling card that will allow a person to use a fake phone number and/or caller name.<sup>7</sup> An abuser can utilize a caller id spoofing card, for instance, to send text messages to a victim who has left him, in order to try to trick her

---

<sup>7</sup> In the information security field, this would be called a 'masquerade attack.'

into revealing her whereabouts [7]. A web search for the term ‘caller id spoofing’ will yield a number of sites that offer caller id spoofing cards, demonstrating that the tool is easily available and able to be ordered online.

The third element of information security, *availability*, refers to the ability of users to access information for which they have the right to do so. As applied to abuse cases, availability would generally refer to the abuse victim having the right to access her own information that she has either created or received (e.g. via email) on her own device. A recent case very dramatically illustrates this concept. While it is not known whether or not the man involved was a victim of long-standing abuse, the incident clearly illustrates the potential damage that can occur when a person is denied availability to their own personal information, and the malicious act perpetrated on him was just as clearly abusive. The case involved a graduate student who was nearing completion of his doctoral studies. He kept all of his digital information stored on iCloud (an online data storage service provided through Apple, Inc.) Subsequent to a divorce, the student’s ex-wife locked him out of his online data account and all of his connected devices, as well. This lock-out included his computer and his phone, as well as other Apple devices that he owned. Shortly after the lock-out, his ex-wife wiped all the data from his iCloud account, erasing the only copy he had of the doctoral thesis he had been working on for years. He also lost a lifetime of photographs and all his other documents and files. He had no backups of any of this data.

These three examples help to clarify the information security terms *confidentiality*, *integrity*, and *availability* and how these terms might apply to the social issue of domestic abuse. They barely begin to scrape the surface, however, in describing the arsenal of technological weapons available to the abuser who is intent on exerting complete control over his partner's life. This paper does not serve as an exhaustive treatise on spying and stalking tools and methods--such a treatment would require an entire book. Instead, a broad overview of these tools will be provided with examples of how they might be utilized by abusers. For the purposes of this paper, then, the technological weapons commonly wielded by abusers will be classified into five categories: the victim's own devices (and the hidden contents of their memory), snooping tools, tracking tools, webcams, and publically-available personal information. In regards to the last category, this paper will focus on public records and information that is available online. A review of these five classes of spying and stalking tools, though not all-inclusive, will nonetheless reveal the amazing extent to which an abuser is able to monitor, invade, and control the life of his victim.

## **2. Electronic Weapons: The Victim's Own Computer**

The woman who thought that she had deleted the email request for help in moving is a good example of how a victim's own device can be used against her. Had she used "CTRL + delete" (simultaneously holding down the 'Control' button and 'delete' buttons on her keyboard) to delete her email, it would not have gone to the

'deleted items' folder in her email box. However, it would not have been 'erased' or 'wiped' from her computer, either. Rather, when an item or file is deleted, it is simply removed from the file directory--the index visible to users for locating files. Other than removal from the file directory, absolutely nothing else about the file is changed at this time. Instead, the file now sits--*still intact*--on the device's hard drive. This is true regardless of the device type...whether it is a computer, cell phone, PDA, MP3 player, or other digital device. The space (memory) that the file takes up is now up for grabs, and at some point in the future a new file may be written over it. It is thus appropriately referred to as 'free space', even though the space is still occupied by the 'deleted' file. Due to the way memory is allocated, though, if a file is overwritten but the new file does not take up as much room as the old one did, then part of the old file may yet remain in the extra space, which is called 'file slack'.

It might seem that this information lingering in free and slack space is not a problem, since the file is no longer visible in the file directory. The determined abuser, however, has options for getting to these deleted files. One possibility is to image the device's hard drive. Imaging is a process that can be thought of as making a copy or taking a 'snapshot'<sup>8</sup> of the drive. This can then be taken to a computer forensics expert and analyzed. However, a much simpler way to probe the drive for deleted files would

---

<sup>8</sup> The term 'snapshot' is used as an analogy and is not to be confused with the technical process of *taking a snapshot* of a drive's state and then saving the state on that same drive for later use as a backup in case of drive failure.

be to use the free or low-cost software tools (e.g. Recover My Files) available for download online that can recover deleted files. One does not have to know the name of the deleted file in order to use these tools, either. A search could be conducted to recover all files of a particular file type, so that a search for '\*.msg' files, for instance, would find any deleted Outlook email messages that remain in free or slack space.

Regardless of the recovery method, for the person who searches it, a device's hard drive contains a treasure-trove of 'deleted' information in the free and slack space. In addition to deleted items, these memory areas can contain information that was never saved to the computer by the user, such as the addresses (URLs) of websites visited. Even clearing one's browsing history will not remove this information from the hard drive. Examples of files that may reside on the hard drive though they are not visible to the user--and even though the web browser's history may have been cleared--include the following:

- emails
- entire chat sessions
- URLs of web pages visited
- search phrases typed into the web browser search box
- images from web pages visited
- information entered into online forms
- documents

- images previously stored on the hard drive
- images from emails
- videos
- messages written on online forums
- cookies<sup>9</sup> that store usernames and passwords for websites
- devices, such as thumbdrives, that have been connected to the primary device  
(visible through disc imaging)

Many Internet users are aware that their web browser (or, in their minds, ‘their computer’) keeps track of the web searches that they make and the sites that they visit. This is called the ‘browsing history’, and it is stored in a small area of memory called a ‘cache.’ Browsers give users the option to ‘clear’ the browsing history. Just as with ‘deleted’ files, though, this does not remove the information from the hard disc but simply leaves it there to possibly be overwritten at some future date.

It can be seen from the above that anything that has ever been on or has ‘passed through’ one’s computer (cell phone, tablet, etc.) can remain on that device for a very long time--potentially for years. Given the determination of most abusers, it is crucial that abuse victims understand this fundamental concept. While they need not know the complexities of how this works, they do need to very clearly grasp that anything ever stored or viewed on their computer may later be retrieved and viewed by their abuser.

---

<sup>9</sup> A *cookie* is information that a web site stores on a visitor’s computer. Not all cookies are bad, but any cookie placed on a computer may potentially be visible through the methods discussed in this paper.

### 3. Electronic Weapons: Snooping Tools

In addition to collecting static information held on a device's hard disc, information from computers and cell phones can be collected, observed, and recorded dynamically, as well, utilizing a wide variety of snooping tools and devices. This means that all of a device user's actions can be tracked in real-time, as the user is typing, web searching, talking, texting, chatting, video-chatting, entering user names and passwords, and so on. Using the previously mentioned keylogger tool, all keystrokes typed can be recorded<sup>10</sup>. Other spyware allows for remote viewing of the user's monitor as the user is using the computer. Graphics, video-chats, social networking pages... anything that the user sees while using the computer can be screenshot and viewed by the person who installed the spyware<sup>11</sup>.

Snooping tools are frighteningly easy to obtain and use. It is hard to read the following online review [8] of a keylogger spying tool, for instance, without feeling an Orwellian chill:

WebWatcher is head and shoulders above the rest. In test after test, with a few exceptions, it never let us down. It made us feel like we could see everything, and amazingly, it allows you to monitor a computer from the Internet, as all of the information from the computer being monitored is

---

<sup>10</sup> See *Appendix A*, P. 71, for a screenshot of one site's reviews of popular keylogging tools. (An excerpt is provided on this page.) The site's top pick is Web Watcher, which is actually a suite of tools.

<sup>11</sup> See *Appendix A*, P. 72, for a screenshot of an example application, Remote Desktop Spy Stealth.

accessible from your own private, password-protected website. The importance of this feature simply cannot be overstated...

Many spying programs and services are marketed as tools for parents to monitor their children's Internet and/or cell phone usage or as tools for employers to monitor employee computer behavior. Abusers, however, find their own uses for these technologies, and some vendors do not even attempt to pretend that their products were produced for a higher purpose than that of spying on one's partner<sup>12</sup>.

Again, the victim need not be familiar with all of the types of snooping tools available or all the features they offer, but she needs a clear understanding of the information security perils that these tools pose for her if her abuser has installed them on her devices. She needs to know that any device that the abuser has physical access to can easily have snooping software installed on it. Just as importantly, she must realize that snooping tools can be installed even when the abuser does *not* have physical access to the device. She must know that spyware could potentially be on any device upon which she has either uploaded a file or opened a picture or other attachment from the abuser (or someone operating on his behalf.) It is not her own actions alone, though, that can result in spyware surreptitiously making its way onto her devices. Abusers will sometimes attempt to get their children to open attachments on their mother's computer or phone, with the surreptitious intent of installing spyware on the device. Sadly,

---

<sup>12</sup> See *Appendix A* for online spyware-advertisement examples.



though, knowledge of these tactics may not be enough to protect the abuse victim. Some abusers skip the high tech spying methods altogether and simply beat the desired passwords out of their partner in order to monitor her email for signs that she plans to leave him [6]. A widely recommended mitigation strategy, then, is to use a computer at a library or friend's house and an email account separate from the usual one whenever an abuse victim is communicating about information she wishes to withhold from the abuser, such as arrangements for leaving. Likewise, a calling card is often recommended for making phone calls about sensitive matters so that the calls will not appear on billing statements. This common recommendation, however, does not take into account the spyware tools just discussed, nor does it consider the possibility of eavesdropping devices having been installed on home land lines. It seems a safer recommendation for the victim, when needed, to use a phone provided by a friend, church, shelter or legal aid agency when she is making plans to escape her abuser or is discussing other matters that could lead to abuse, threats or harm from her abuser. These tips apply equally well to mitigating the risks posed by the threat of tracking tools.

#### **4. Electronic Weapons: Tracking Tools**

A woman receives a new phone as a gift from her intimate partner or her old phone disappears and then inexplicably turns back up. Next thing she knows, she is out shopping with a friend and receives a text from her partner asking, "Why are you at the

mall?” This is the type of scenario that has been related to Dr. Tovar in the interviews she is conducting in the qualitative (interview-based) second part of her research into the use of text messaging as an abuse tool. Her interviewees are relating an experience that is becoming increasingly common among abuse victims: being tracked by global positioning system<sup>13</sup> (GPS) enabled devices on their cell phones.

Use of GPS devices on vehicles to track abuse victims is an often-cited occurrence, as well. Jan Langbein [9] is the executive director of Genesis House, a counseling center and shelter for victims of domestic abuse in Dallas, TX. She relates the story of a woman, married to a wealthy man, who was in her final months of residency in medical school. The woman was puzzled by her husband’s uncanny ability to know where she was when away from their home. Through the help of Genesis House, she discovered that her husband was using her car’s OnStar service to locate the vehicle (which was registered in his name) and thus to locate her<sup>14</sup>.

---

<sup>13</sup> The global positioning system is a satellite-based navigation system developed and provided by the United States government [32]. GPS can be used to track the geographic location and movements of the devices on which it resides.

<sup>14</sup> Langbein reports that after this case was mentioned during a media interview, she received a call from an OnStar representative who stated that OnStar could not be used in this manner. Langbein asked her to suppose that a car owner called and said his child was using his car and he was concerned about her. She asked, “Would OnStar reveal the car’s whereabouts?” The representative conceded that they would. OnStar’s Family Link service was designed for just such a purpose. After receiving customer complaints of spouses tracking one another with the service, OnStar reports that it stopped revealing the car’s location to people who call in claiming the car was stolen. They now only report the location of a ‘stolen’ car to the police after the owner has filed a stolen vehicle report [33]. It is not clear how this would prevent a person from using the Family Link service to check on the whereabouts of a spouse under the guise of concern for their ‘child’, however.

GPS tracking tools may be abuser-installed software applications installed on the victim's cell phone or hardware devices installed on the victim's car. They may also be part of a vendor-provided family service aimed at providing nervous parents with reassurance that their children have not fallen off the face of the earth, such as OnStar's Family Link service for vehicle owners and Verizon's Family Locator Plan for cellular phone subscribers. Abusers have proven adept at manipulating these programs to keep tabs on their intimate partners.

It was mentioned in Section One of this chapter that information security includes the consideration of *implied* information. If an abuse victim's behaviors suddenly change dramatically, then this may imply certain things to her abuser. For instance, if the victim suddenly starts clearing her web browser history when she never has before, then the abuser may conclude that she is hiding something from him. He may suspect that she is planning to leave him, and the abusive behavior may escalate and become more violent. This is another reason why it is better for her to do sensitive web searching on a computer at a library, friend's house, shelter, or similar safe location. Implied information is a very grave concern with GPS tracking. Turning off the GPS tracking will be immediately noticed by the abuser and could put the woman in serious physical danger. This type of situation is one that is best evaluated with the help of experienced counsel that is tailored to the victim's specific circumstances rather

than by issuing a blanket recommendation of what to do if a victim discovers her phone or car is being tracked by a GPS device or software.

## 5. Electronic Weapons: Webcams

Langbein [9], the Genesis House executive director, recalls a client who said that her husband, to her great puzzlement, would make remarks such as, “It doesn’t look like you put much effort into this supper. When you start so late, what do you expect?” Since her husband had not been present when she cooked the supper, she was at a loss as to how he knew when she had started the meal. Continual instances such as this had the woman thinking that she was losing her mind. Was she telling her husband all these things but not remembering doing so? What was happening to her memory?

Part of the abuse pattern is to keep the victim off-balance and bewildered. A woman who is sure of herself and the ground that she stands upon may flee, so better to keep her unsteady on her feet and disoriented, never knowing when the next blow may come, what the trigger will be for the next explosive outburst of anger and abuse. Therefore, when a victim encounters situations where her abuser knows things about her activities that seemingly he *couldn’t* know, she tends to assume that it is her own shell-shocked emotional and mental state that is to blame for the apparent discrepancy between what he knows and what he reasonably *could* know. Due to the extreme duress under which she lives, she already feels as if she is ‘losing it’ mentally. She assumes,

then, that it is her own off-kilter mental state that accounts for this bizarrely-unreal feeling that her abuser is omnipresent and knows everything she does.

The reality (portended by the title to this section of the paper) may indeed be bizarre but is nonetheless very real--real in a way that is cold, calculating and grim. The woman in Langbein's account eventually discovered that her husband had placed webcams throughout their house. He had not only recorded her cooking in the kitchen but also going to the bathroom and showering...any activity that she did in her home was recorded by the webcams he had planted throughout the house.

Webcams--video recording devices that can stream images to a remote website for viewing in real-time--are frequently used by abusers in an attempt to satiate their need to know what their partner is doing quite literally every moment that she is away from him. The use of these devices for spying on an intimate partner is an egregious violation of privacy and trust. The psychological effects on the victim are devastating. Before she learns that every action she makes in her own home is being recorded, she thinks she is slowly going crazy. When she discovers she is not--when she realizes that her abuser has been secretly watching her for a long time--she feels demeaned, traumatized and vulnerable. She is left with the message intended: she will never escape her abuser. He is everywhere, at all times.

Unfortunately, there is no simple remedy for this situation, once discovered. If the woman blocks the webcams or removes them, she likely will suffer for it. She could, for instance, be violently beaten for any action she takes toward the webcams in order to protect her own fundamental right to privacy in her own home. On the other hand, if the webcams are left in place, then any attempts to plan an escape will be limited to what she can accomplish outside the home, and even there, her abuser is apt to be-- thanks to his arsenal of technological tracking and spying tools--ever present.

It is important to note that, if an abuser, whether he lives with the victim or not, has secretly used webcams to record her, he has almost certainly broken invasion of privacy laws [10]. For example, New Jersey has a public policy that makes spying on one's spouse unlawful. Mark Gruber, a New Jersey family law attorney, writes [11] that the New Jersey Court, "commenting on the trauma created by the invasion of privacy...held:

*'There is no reason whatsoever to allow spouses to perform non-consensual tortuous acts against each other than there is to allow them to perform them against third parties. The right of privacy extends within the confines of the marital home. It is not somehow dissipated into the air upon the taking of marriage vows.'*"

## 6. Electronic Weapons: Publically-Available Personal Information

"The danger of violence, including the risk of death, escalates  
when a domestic violence survivor attempts to leave a batterer."

*--Report sponsored by American Bar Association Commission on Domestic Violence [12]*

"It's actually obscene [sic] what you can find out about people on the Internet."

*--Liam Youens, the man who used Docusearch to locate and kill Amy Boyer [13]*

While all of the previously mentioned types of spying, tracking, and monitoring tools and techniques will in most cases involve breaking at least one privacy law, publically-available online information that may be obtained free or for a fee is often perfectly legal. For an abuse survivor<sup>15</sup> who has left her abuser, the privacy of her address information is paramount to her personal security, but she may not be aware how easily available her address is online. Courts, for instance, are increasingly making court records, complete with addresses and other personally identifiable information, publically available online. Many localities have put their land records online, complete with maps to the house. Free online phone searches are available that typically give the person's address, along with the phone number and, perhaps, the person's approximate

---

<sup>15</sup> 'Abuse survivor' is terminology commonly used to describe those who have left the abusive relationship.

age. Data aggregators such as Spokeo.com make basic information, including addresses, available on most anyone with a simple web search. For a small fee (\$3.95 per month for Spokeo), one can obtain detailed information about a person, including information pulled from local, state, and government sources, as well as from hundreds of social networking sites [14].

Data brokers who collect and sell personal information, however, are under increasing scrutiny. Amy Boyer was a woman killed by her stalker, Liam Youens in 1999. Youens used an online information broker called Docusearch to obtain the information on Boyer that allowed him to locate her and murder her. Docusearch went so far as to make a phone call under the pretext of a legitimate inquiry to obtain Boyer's employment address for Youens. In 2003, the New Hampshire Supreme Court held Docusearch liable for its customer's crime [15]. Given the abundance of information brokers still operating on the Internet, however, this case does not appear to have had a deterrent effect on the selling of personal information.

As the Amy Boyer case illustrates, those who leave their abusers are endangered by the ease with which most anyone today can obtain personal information on most anyone else. It is hereby suggested that a good safeguard for an abuse survivor, then, would be one that enables her to contact one government agency that could then notify all data brokers and other government agencies (local, state, and federal) to seal from public consumption any and all information on her. There is some precedent for such a



federal scheme, in the form of the National Do Not Call Registry. The registry is maintained by the Federal Trade Commission (FTC) and was created in 2003 as a result of the Do-Not-Call Implementation Act, which was passed in order to fulfill the objectives of the Telephone Consumer Protection Act of 1991. The purpose of the registry was to allow citizens a means of stopping unsolicited calls to their homes from telemarketers (businesses that solicit sales over the telephone.) By law, telemarketers must search the registry once every thirty-one days to ensure that their call lists do not contain any phone numbers on the National Do Not Call Registry. When telemarketers call numbers that have been on the registry for more than thirty one days, these violations can result in fines of up to \$16,000 per call [16].

If such a system could be put in place in order to protect Americans from being harassed by sales calls during their suppers, it seems entirely reasonable that a similar system could be established to protect the lives of abuse survivors and their children. This, though, would have to take place through legislative channels, which would likely take years, and many abuse survivors need protection *now*. It is therefore recommended that shelters, counseling services and volunteer organizations that work with abuse victims implement services that will help survivors to search for and expunge as many online sources of personal information on them as possible. The searches should be conducted periodically for as long as the survivor feels threatened by her abuser or former abuser. Volunteer positions and training could be created specifically for this

task. Additionally, all abuse survivors should be advised on how to obtain seals that prevent public viewing of any court records (e.g. divorce papers, landlord disputes, etc.) that pertain to them. Those who have not left the relationship should also be counseled on this important self-protection strategy, as they may not have the counseling services available to them once they leave the relationship, if they indeed do make the break from their abuser.

One last consideration to mention in regards to public records is credit bureaus. Frank M. Ahearn, a former professional skip-tracer (someone who finds people who've 'skipped town') who reversed course and turned to helping people disappear for a living, often cites credit reports as a critical link in finding those with a desire to disappear [17]. When one relocates, a first step, of course, is to find a place to live. One will typically not be able to rent nor buy an apartment, home or condo without a credit check first being run, however. Once a victim has a credit report run on her, she will be entered into a national credit bureau database. (Or her current entry in that database will be updated, if she is already in it, which is more likely.) The abuser--or an investigator he hires--may also run a credit report on her utilizing her social security number (which the abuser is very likely to know, either from tax returns, if they are married, or through snooping, if he suspected she might flee) and the last address she had (the one the abuser shared with her or knows about). Whenever a credit report is run, it shows up on subsequent credit reports as an 'inquiry'. The report obtained by the

abuser, then, may reveal any recent inquiries that have been run on his victim. If these include an inquiry run by a rental agency, landlord or realtor, the report could lead the abuser to her current location.

Some victims are more at risk after they leave the relationship than others. Some have more reason than others to fear that their abuser will track them down no matter where they go, and some will have more reason to fear what happens should the abuser find them. To what lengths a victim should go in order to protect herself and her children, then, will vary case by case. Every abuse victim who leaves the abusive relationship must decide for herself on what terms she will do so. She must evaluate the risks and determine--as it is referred to in the information security profession--her 'risk appetite.' In other words, does she attempt to disappear altogether in order to buy more peace of mind, or does she simply try to achieve distance from her abuser so that she may lay claim to a somewhat normal life for herself and her children?

The credit check is but one example of the myriad tools and strategies that private investigators (and clever abusers) have at their disposal. Therefore, for the survivor who is in mortal fear for her life and has thus chosen to attempt to 'disappear' from her abuser's sight, it is concluded in this paper that consideration should be given to changing her and her children's names. However, here again, one must be aware of the open nature of many court documents. It would be best if the name change(s) were

done in another jurisdiction than the one in which the abuser lives, and it should be discovered whether or not the record of the name change can be sealed.

All of the care in the world in regards to public information, however, will be of no avail should the abuser find a way to worm his way back into the victim's digital space. For instance, suppose that the victim who has left her abuser did everything recommended but also kept her mother or best friend abreast of where she has moved and what she is doing. Now suppose the abuser sends the victim's mother or friend an email with, for instance, a greeting card. Further suppose that the email has a spoofed 'from' address and the mother or friend opens it on her computer, unaware that it has come from the abuser. If that greeting card contains a Trojan (a piece of malware tucked in with an innocent bit of software, such as the hypothetical greeting card) the abuser is now on a path to spying on the emails sent to and received from the computer, and thus is on the road to locating his victim. The couple's children could provide even more innocent--and thus more vulnerable--targets for such digital exploits.

This paper has demonstrated that to make an escape from an abusive relationship a complete and a safe one, information security principles must be applied while the abuse victim is still in the relationship, while she is in the planning stages of making her escape and after the abuse survivor has successfully removed herself from the abusive relationship. It can be seen, then, that the most vulnerable victims--those who are in the gravest danger if they leave the relationship--will require extensive and

expert counsel if they are to stand a chance against a determined abuser who has moderately good computer skills and/or good financial resources (i.e. to hire an investigator). Those who remain in the abusive relationship will likewise need wise and expert counsel.

As referenced in the introduction to this paper, information security skills and knowledge are also needed for the collection and presentation of abuse evidence in court, tasks that may have to be performed by the abuse victim herself. This additional intersection of the field of information security and the social issue of domestic abuse will be explored in the next chapter.

### III. Information Security and Documenting Abuse for Presentation as Evidence

#### A. The Significance of Evidence Collection and Admissibility: *Tagle vs. Garcia* Case Study

In the 2009/2010 California case of *Tagle vs. Garcia* [18], Katie Tagle repeatedly tried to obtain a restraining order against her child's father, Stephen Garcia. Tagle hoped that a restraining order would also result in the court requiring supervised visits between Garcia and their son. Garcia had been violent with her--even while she was pregnant with their child--and after she left him, he continued to threaten future violence. The primary judge in the case, Judge Robert Lemkau, refused to examine ten different types of electronic evidence Tagle brought before him, repeatedly cut her off midsentence during hearings when she attempted to answer his questions to her, twice called her by the wrong name during proceedings, shook his finger at her and accused her of lying, and threatened 'serious consequences' if she did not stop making 'misrepresentations' that the boy's father was threatening violence toward her and their son. Judge Lemkau concluded the last hearing by ordering Tagle to turn over their son to Garcia for the regularly scheduled, unsupervised visitation that Lemkau had previously ordered. The case ended during that visitation when Stephen Garcia shot and killed both himself and the baby.

Judge Lemkau was dismayed by the subsequent public outcry; he could not see how he could have allowed the electronic evidence into consideration. It was not Judge Lemkau alone who so tragically failed Tagle and her son, Wyatt, either. Though Lemkau was the judge before whom the couple had appeared the most often, Tagle--who could not afford legal representation--had gone before two other judges in pursuit of a restraining order, and neither of them would consider (or even look at) the electronic evidence she brought with her. Her evidence included threats by Garcia to hunt her down and kill her. At one point, she received a novella through email via an address that she did not recognize. The novella was obviously written by Garcia but was signed 'John Hancock'. It was entitled *Necessary Evil* and was clearly based on the couples' lives. It presented two alternative endings. In one ending, the story concludes happily after the woman who has left her man returns to him with their child. The alternative ending to the novella concluded with the death of the couple's child. After receiving the emailed novella, Tagle called 911 and the county managed to help her get a temporary restraining order against Garcia. The order was only for seven days, however, and Judge Lemkau, still not persuaded after this incident that Garcia was a threat to his son, was bent on ensuring that Garcia had unsupervised visits with him.

The evidence Tagle brought before three judges to prove that Garcia was threatening her and the child included text messages, emails, voice mails, MMS (multimedia messaging service) messages, photographs, telephone calls, computer-

generated documents, social networking site activity, and a personal website.

According to Farkovitz [18], “virtually none” of the evidence was ever looked at by any of the three judges. She further notes that, “No public agency reviewed the evidence or intervened.”

Farkovitz eloquently summarizes the heart-rending and ironic tragedy of this case in the following passages [18]:

Where are the words to describe this tragedy from Katie Tagle’s perspective; the absolute sense of betrayal from Stephen Garcia, his family, law enforcement, the legal community, and the court system; the unbearable loss of her baby when she had in fact had the courage to fight back and defend herself and her child? She did what every abused woman is advised to do. She left. She got help. She started a new life. She sought legal protection. She followed the rules. She presented her evidence. She went to court repeatedly, called law enforcement to protect them, and asked family and friends for help.

... Katie Tagle is a person who endured an increasingly abusive relationship for three and a half years until Stephen Garcia knocked her unconscious. She tolerated an infuriating invasion of her privacy as Garcia hacked into her email, phone account, read her text messages, and then to punish her, took her to court to win custody of their child. In U.S. society



it is currently estimated that this kind of illogical reasoning [*i.e. court-ordered, unsupervised contact with abusive parents*] is affecting more than 58,000 families per year, according to the *Leadership Council on Child Abuse and Interpersonal Violence* [19].

As this case so horrifyingly demonstrates, the burden placed on abuse victims to collect their own electronic evidence is only half the challenge: judges must also know how to consider that evidence once presented and are often ill-prepared to do so. Abuse victims, stripped by their abusers of all financial resources, too often find themselves having to collect and present evidence against their abusers, a task for which they have no training and one that is done under extreme mental and emotional duress. Judges should recognize the injustice of this situation and seek ways to corroborate abuse victims' evidence rather than dismissing it out of hand as unverifiable. Not one of the three judges in the Tagle vs. Garcia case sought outside help in order to evaluate the evidence that Katie Tagle brought before them. Faced with evidence that they did not know how to evaluate, they simply didn't. A nine month old baby was killed by his own father as a result.

Not all abuse victims without financial means must present their cases *pro se* (without legal counsel.) Some women are fortunate enough to live in metropolitan areas that provide legal aid for abuse victims, either through the local district attorney's office or through not-for-profit organizations. An interview with a lawyer at one such agency

that provides legal aid to domestic abuse victims, however, revealed a scenario that is likely all too common. This lawyer works on a calendar and budget that allows only for a brief, rushed preparation of a restraining order case. She is not afforded the prolonged time needed for gathering electronic evidence, such as subpoenaing records from a cell phone company, for instance. Moreover, outside of metropolitan areas, such local legal aid agencies and programs would typically not even exist. These are all factors that every judge should be aware of as electronic evidence is brought before her in domestic abuse cases. If the judge feels inadequately prepared to evaluate the evidence, how must the woman who is forced to provide her own electronic evidence of abuse and argue it before the judge feel? It would seem little more than common sense for the judge to turn to experts in the field of computer forensics to help her interpret the evidence. Many police forces in metropolitan areas have their own forensics experts on staff who could provide guidance to the court. However, this said, it must be acknowledged that with many of the new forms of social media evidence--a growing source of evidence in abuse cases--there is scant precedent to guide even the experts in determining admissibility and authenticity.

According to Benjamin Wright, a Dallas, TX attorney who teaches courses on electronic evidence with the SANS Institute, electronic mail (email) evidence--one of the types of evidence that Tagle presented to the judges she came before that was not even considered--has been around long enough that our court system has been "choking" on

it since the year 2000 [20]. There is a great deal of precedent, then for admissibility of electronic mail in court. Noting historical shifts in admissibility of different types of evidence in court, Wright recounted, “We first had ‘he-said/she-said’ evidence for most of history. Then we had about 100 years when paper evidence was well-accepted. Starting in 2000, electronic mail evidence shifted to many orders of magnitude of the evidence we previously had on paper.”

He notes that this tidal wave of evidence is nothing, though, compared to the coming tsunami of social media evidence. He marvels, “I think that the change that we saw in 2000 with electronic mail was minor league compared to social media. Electronic mail is like stone tablets compared to social media. The quantity of evidence being created by social media is astronomical compared to electronic mail. I feel like social media evidence is already flooding into the American legal system, and it is growing by exponential rates.” Referencing the current proliferation of social networking sites, blogs, forums, personal websites and the like, Wright observes, “The Internet is just crawling with evidence like we’ve never seen before in the history of mankind.”

These electronic forms of evidence also bring with them challenges such as the court systems have never seen before. The remaining section of this chapter will explore those challenges.

## B. Challenges of Determining Admissibility of Electronic Evidence

Behind many abusive acts of violence lies an electronic evidentiary path composed of digital fragments torn from social media postings such as blogs, special interest forums, and personal websites as well as from electronic mail, text messages, voice mail and the like [21]. As has been demonstrated through the *Tagle vs. Garcia* case, this evidence--its collection, preservation, presentation in court, and admissibility determination--can make the difference between life and death in a domestic abuse case, particularly in decisions regarding restraining orders and those regarding unsupervised visitation rights.

As Wright [21] points out, however, using electronic media as evidence presents many problems, including, to name but a few, the following:

- The fact that the person using or viewing the medium often does not have access to the hardware on which it is stored.
- The dynamic nature of social media. (E.g. a Facebook wall post viewed today can be removed tomorrow.)
- The difficulty in garnering cooperation from many web site and cell phone providers.

Moreover, Laure Ruth, Legal Director at the Women's Law Center of Maryland, reports [22] that what electronic evidence is ruled admissible by a court--and what is

not--varies from one legal jurisdiction to another. A perusal of articles on the subject indicates that this statement can be fairly extended to say that admissibility varies even from one judge to the next within a jurisdiction. Wright [20] sums up the current admissibility status of electronic evidence that falls under the classification of 'social media'<sup>16</sup> well, stating, "The court system is looking at it and accepting it in certain circumstances, but in a very checkerboard way."

At the crux of the issue of evidence admissibility are the relevance and the reliability of the evidence. For electronic evidence, reliability speaks not only to ownership of a social media, email, or phone account but also to *authorship* of a particular post or message. (I.e. could someone other than the account owner have written the post or message?) In information security terms, it is the *integrity* of the information (text message, blog, wall post, etc.) that is in question. For instance, even if a computer forensics expert were to verify that a particular text message was indeed sent from a particular individual's phone, this is not indisputable proof that the phone owner was the one who sent the message. This is an example of 'ownership does not equate to authorship.' Anyone with physical access to the phone could have sent the message. An example of this type of authorship issue is demonstrated by a case cited by Southworth [23]: an abuser changed his wife's email password, sent threatening

---

<sup>16</sup> While there is not a generally agreed-upon definition of the term 'social media', it is commonly recognized that the 'social' part of the phrase implies media that is for consumption on a more public nature than one-on-one communications, such as email and text messages.

messages that appeared to be from her to him, printed them out and took them to the police and requested that they arrest her. With social media accounts, even ownership is easy to fake. Anyone could establish a Facebook or Twitter account, for instance, using another's name and even their photo, to lend more credibility to the account.

How, then, does one ever prove that a steady stream of threatening private text messages or public social media posts actually originated from the person who appears to have written them? The distinction between private communications and public social media postings, it turns out, is a critical one in addressing the complexities in determining admissibility of such evidence. Ira Robbins, professor of law and justice at American University Washington College of Law, reports [24] that under Federal Rule of Evidence 901(b)(4), an item of evidence may be authenticated through its "distinctive characteristics," which include appearance, content, substance and internal patterns. These characteristics are evaluated in light of the circumstances that surround the evidence and the case. Authenticating forms of electronic evidence that have been around for a number of years (such as email) through the concept of distinctive characteristics is a well-established practice. Robbins explains that social media evidence, however, is different from these traditional electronic communication exchanges between individuals. The difference, he says, is that the characteristics and content of social-networking evidence, "often reveal nothing useful about the author." In other words, much of what appears in social media could have been written by

anyone--the claimed author or an impersonator. Robbins, too, remarks on the greatly varying ways in which this evidence has been treated by courts in terms of admissibility. Robbin's observations echo those of the previously-referenced lawyer and electronic evidence instructor, Benjamin Wright. During an interview [20], Wright was asked if he knew of cases where ignorance on the part of the court about social media evidence had caused verdicts to go the wrong way. Wright responded, "Yes! Confusion around social media is *legion*. Nobody knows everything about social media law."<sup>17</sup>

Compounding these challenges is the fact that often times the corporate owners<sup>18</sup> of the physical medium that holds social media forensic evidence strongly resist requests and even subpoenas for turning over copies of relevant evidence, such as call logs and text messages. According to Wright [20], the issue revolves around interpretation of the Stored Communications Act. He notes that it is a complex law to interpret, because it was written in 1986 and "technology has gone through twenty revolutions" since then. This means that the law relied upon to make decisions about turning over electronic evidence was written long before Facebook, Twitter, blogs, and text messaging became major shapers of the social landscape. Wright observes that different providers will "put varying amounts of effort into interpreting" the act. He explains that one interpretation is that private messages are given higher protection by

---

<sup>17</sup> For those who desire a more in-depth examination of the issue of social media admissibility, a detailed treatment of the topic may be found in the memorandum opinion of Chief United States Magistrate Judge Paul W. Grimm [34] in the case of "*Jack R. Lorraine and Beverly Mack, Plaintiffs v. Markel American Insurance Company, Defendants*. Civil Action No. PWG-06-1893".

<sup>18</sup> E.g. the cell phone, Internet and email providers that store messages and postings on their servers.

the act than public postings. This interpretation would mean, for instance, that a blog, which is intended for public consumption, would enjoy less protection than a Facebook posting, which is intended for viewing by only a select group of people. Even a subpoena<sup>19</sup> does not compel some service providers to turn over the requested records. Wright reports, “Facebook and Twitter have put up a very structured wall against all these subpoenas.” He notes that small Internet service providers (ISPs) tend to be inclined to be more cooperative in responding to subpoenas. He cites one instance in which a sheriff simply wrote a letter requesting records from a small ISP, and the company obliged and sent him the records. As with court rulings on the admissibility of social media evidence, then, the *availability* to courts of such evidence is also a hit-and-miss affair.

The clear and compelling conclusions that may be drawn from all of this are the following:

- 1) Justice is ill-served by the current confused judicial state of scatter-shot rulings on admissibility of electronic evidence in general, and of social media evidence in particular.
- 2) There is an urgent need for the courts to have guidelines and standards to assist them in evaluating electronic evidence.

---

<sup>19</sup> A subpoena, in this context, is a request for the production of specific documents. It may be issued by a court, a law enforcement agency, a district attorney’s office, or, in some limited cases, by a civil lawyer.

[20]



3) New laws are needed to assist service providers in interpreting the extent and limitations of their duties to protect--and duties to release--electronic records.

Experts and authorities from many fields should have a hand in developing these standards and legislation. In addition to the participation of the legal and law enforcement communities, it is important that both social welfare agencies that serve domestic abuse victims and members of the information security profession are also included in order to ensure that the guidelines, standards and legislation developed do not have unintended consequences that might put domestic abuse victims at risk. Information security professionals who specialize in digital forensics could provide critical insight into the understanding of the new technologies under evaluation and the inclusion of these professionals in the development process would likewise be important. Guidelines for judges should include outside resources to which they can turn when they do not feel adequately knowledgeable to evaluate electronic evidence.

Much of what happens in our courts, including establishment of rules of evidence, develops from 'case law', which is to say, previous rulings. The problem is that technology is evolving at such a pace that we as a society can scant keep it in our sights, much less keep pace with it. Case law, by contrast, moves at the pace of the tortoise. This discrepancy is leaving courts in the dust. Therefore, the legal system needs to look not at simply developing standards for admissibility of current electronic evidence, but also at developing a new, more dynamic way of *creating* such standards.

There needs to be a system in place that will allow for rapid review of new technologies and their impact on evidence admissibility rather than relying on the process of allowing rules of evidence to evolve from case law. When a new technology emerges, ways to authenticate evidence based on it need to be explored early on. Standards need to be developed quickly, but also need to be based on thorough research, and then information on the new technology and concomitant rules of evidence need to be rapidly disseminated to judges and lawyers.

## **IV. Meeting the Need**

### **A. Information Security Provision: Education vs. Counseling**

Originally, it was intended that this project would include educational materials for both abuse victims and for the legal community. These were to be a prototype for future, expanded materials, which it was envisioned that members of the information security field would develop in conjunction with domestic abuse agencies and the legal community. The original goal, then, was to spur the joint development of educational materials in order to arm abuse victims with more (than is currently available to them) of the information security strategies they need in order to protect themselves and also to collect and present their evidence in court. The original secondary goal was to spur a similar collaborative effort to educate judges and others in the legal community about electronic evidence so that they would be more attentive to, helpful in acquiring, and knowledgeable in evaluating such evidence in domestic abuse cases. It was believed that the information security community could play an important role in the process of developing these educational materials, as well.

The research reported herein, however, reveals the underlying flaws in these goals. The vast resources readily available to those who wish to stalk, spy on, and intrude themselves into the life of another are breath-taking in their thoroughness and

stealthiness. While these tools are often very simple to implement by even a novice to electronic monitoring, presenting a defense against them, by contrast, often requires a high level of expertise. This is *not* to discount the teaching and use of basic electronic safety measures--those are still critical to an abuse victim's safety. Rather, it is to emphasize the point that simply throwing more information at abuse victims for them to arm themselves against their abusers will simply not suffice to adequately protect them. In fact, in light of the above, creating pamphlets, brochures and web sites listing information security strategies for abuse victims seems a lot like sending a woman out into the jungle to fight guerilla warfare against an enemy armed with AK-47s and, on her way out, tossing her a butter knife and saying, "Take care of yourself, now."

Most domestic abuse web sites proved lists of suggested ways in which the abuse victim or survivor can protect her information. These lists are *of necessity* short ones, for the following reasons:

- Abuse victims are, in the words of those who work with them, "emotional wrecks." They are too traumatized to be able to take in, remember, and implement a long list of ways to protect the information that can, in turn, protect their own safety. They are frightened, vulnerable, and disoriented.
- Many of these women are being watched *all the time*. They may sneak in a brief peek at a website on abuse, but they do not have the luxury of taking the time to

thoroughly educate themselves on the topic of information security for abuse victims.

- Some abusers are so devious, so persistent, and so obsessed with regaining control over a victim who has left them that it would require a whole *volume* of books to contain the information the victim needs in order to stand a chance of disappearing from his radar if she leaves him.

The conundrum is this: the traumatized victim cannot take in long, complex instructions on protecting her privacy, but a short list of strategies may give her a false sense of security. For instance, the materials may advise her to be aware that an abuser can spoof an email address, so she should never open attachments on emails. Is she going to realize, though, that the abuser might infiltrate their child's computer through an email greeting card (perhaps, even, using a spoofed 'from' id, such as a celebrity the child admires) or even through a photo he shares on the child's Facebook wall (again, perhaps masquerading as a celebrity who friends the child?) Would she realize that, if he has compromised the child's computer or phone, that from there it is but a short leap to her devices on which she exchanges emails with her child? Will she use her phone in confidence, knowing that she has never opened an email attachment or surfed the web on it, when in fact it is tracking her every physical movement through GPS and is recording her every phone call, text message and email? Again, this is getting into

complexities that will likely overwhelm the victim, heighten her sense of vulnerability and deepen her sense that there is no escaping her abuser.

What the abuse victim needs beyond basic security tips, then, is not to be inundated with a flood of yet *more* facts and tips about information security than is already available to her, but rather to receive *individual* counseling from people who already possess that knowledge and who understand how to use it to perform an information security risk assessment on her particular situation and to devise a threat mitigation plan tailored to her needs based on that assessment. What is needed is an infrastructure--a network of support--that can provide this type of service through hotlines, through counseling at existing abuse centers, through online chats, and the like. In other words, what is needed is not better educational material to “arm” the woman with a new, improved butter knife. What is needed is a national recruitment effort to incorporate the information security community into the existing volunteer efforts that are aimed at serving the needs of domestic abuse victims. (See Chapter V, Section 2 for a suggested model for such a recruitment effort.)

As to electronic evidence collection (and the original secondary goal of this project), the interviewees and literature sources consulted for this paper make it abundantly clear that the entire field is too new and volatile for any source to presume to offer advice on collecting and presenting electronic evidence and then to imply that following such advice will ensure that the evidence will stand up in any one particular

court, much less in most. The issue of admissibility of social media evidence, particularly, is so scattershot right now that there is nothing that remotely resembles a standard that could be aimed for. As it currently stands, no judge can be expected to know how to treat this evidence, really. No one knows. The *Tagle vs. Garcia* case, however, demonstrates that--however it is treated--electronic evidence must *at the least* not be ignored.

Ultimately, though, the real flaw with the original goals of this project is this: *they put the onus of protection on the victim herself*. Whether protection means securing her own information or presenting evidence of abuse in court in order to protect her and her children, the original goals conveyed the message that the abuse victim--physically and mentally battered, traumatized, vulnerable and living in a constant state of fear--bears the responsibility for combating technologies that are sophisticated and constantly evolving and that she is expected to do so under circumstances that exponentially complicate this already difficult task.

It is time to shift the paradigm. It is time to build the infrastructure that will enable and undergird this paradigm shift. This is the 'call to action' this paper's title references. It is a call to the information security community, to the agencies that serve domestic abuse victims, to the court systems and to our legislative bodies. It is also a call for researchers in all of these fields to address the questions that will help to unravel

the complexities of protecting abuse victims. Following are recommendations for how members of each of these sectors can answer the call to action.

## **B. Recommendations for the Information Security Community**

Providing direct aid (i.e. information security counseling) to domestic abuse victims does not address the *issue* of domestic abuse, which originates with the abuser. The question always asked is, “Why does she stay?” Doesn’t this question blame the victim? Shouldn’t the question be, “Why does he abuse?” This has, in fact, been researched. The conclusion drawn from studies done on the topic is that abusive behavior is not caused by mental illness, substance abuse, behavior of the victim or problems in the relationship, anger, genetics, stress, or out-of-control behavior. Quite simply, it is a learned behavior [5]. Whether from within the childhood family or within the culture or community, the abuser has learned that violence is an acceptable way to get his way and believes it is his right to use it.

One incident from the electronics-store canvas done at the outset of this project aligned with these findings. The sales clerk at the store was a young (early twenties) Latina woman. She stated that she had herself been a victim of domestic violence. She said that, in fact, she did not know “a single woman who has not been abused” by her partner. Her mother, the sales girl reported, was beaten by her father while pregnant



with her. She claimed that domestic violence is very accepted--even expected-- in Latino culture and said that this is why she will not date a Latino man. While statistics do not bear out her generalization to the entire Latino population, the woman identified herself as being from Peru, and that country has one of the highest incidents of domestic violence in the world. According to Quechua Benefit, "Nearly half the women living in Peru have been physically assaulted by their partners, and in rural areas such as the Southern Highlands, the percentage goes up to 61%." [25] This correlation between specific geographic areas and domestic violence would support, then, the previously-mentioned research findings that indicate that abuse is a learned behavior. The sales clerk's story also illustrates how acceptance of abusive behavior can be learned, as well. It was through moving to a new geographic region, after all, that this young woman learned that she did not have to tolerate being abused.

It is good news that domestic abuse is not caused by mental illness, because it is arguably much easier to treat ignorance than it is to treat many forms of mental illness. The cure is education. One must ask then, where is the outpouring of public service announcements, high school education programs, sermons and homilies, movies and talk shows that deliver the message, 'Abuse is wrong. Controlling your partner is wrong. You do not have the right to do these things,'"? Certainly abuse victims need protection, and that is always, always the first priority. However, in terms of education, it seems obvious that in addition to teaching defense skills to abuse victims, there

should also be a focus on education at all levels of society aimed at ensuring that all members of our communities understand what constitutes abuse and the fact that abuse is never acceptable behavior. Here again, the information security community can play a role. It could take the lead in educating the public about what is and is not acceptable use of electronic tools. If no one is delivering the message that using spyware on your girlfriend or tracking devices on your husband is not only illegal but also morally wrong, then what *are* the messages people are receiving, and who is in control of communicating those messages? Who, for instance, is countering the online messages of spyware advertisers, such as those found in *Appendix A*?

In 2010, a Rutgers University student committed suicide after his roommate used a webcam to record him in a homosexual liaison. The roommate was convicted in 2012 of invasion of privacy and bias intimidation, among other charges. After the trial, Jane Clementi, the mother of the student who committed suicide, made a statement to the press that included the following words, "In this digital world, we need to teach our youngsters that their actions have consequences, that their words have real power to hurt or to help. They must be encouraged to choose to build people up and not tear them down. [26]" It would seem appropriate for the information security community to take a leadership role in educating the public regarding the appropriate uses for technology. As long as people believe it is acceptable to use technology to control, track, spy on, intimidate, steal from, deceive or bully others, they *will*...and they will find and

create the means with which to do it. Malicious uses for technology evolve at a rate that outstrips the ability to create counter-measures to defend against them. They have become tools for domestic abuse and cyber-bullying alike. The information security community is engaged in a tit-for-tat race, trying to keep pace with each new malicious use of technology with a corresponding mitigating measure. No matter how Quixote-like it may seem, that effort *must* continue. Perhaps the best hope for throttling abuse-through-technology, though, lies in educating our populace about the concepts of “good use” and “bad use” of technology. This paper asks the question: What community is a more natural champion for delivering this message than the information security profession?

It is thus concluded that the information security community is presented with a couple of opportunities to, in the words of Mr. Wright in his interview, “do good.” The first opportunity to help is through direct counseling of domestic abuse victims and survivors, as well as through advising and training abuse center workers in information security strategies as they pertain to domestic abuse. Towards this end, the information security community is strongly encouraged to develop training programs for their members who wish to volunteer as counselors and advisors in established domestic abuse programs, such as hotlines, shelters and counseling agencies. Such training, of course, should be developed in conjunction with experienced domestic abuse program providers. It is recommended that a certification process be put in place to ensure that

any information security volunteer is trained in the highly sensitive issue of domestic abuse before they begin working with the abuse victim/survivor populations.

The second opportunity to 'do good' involves helping not only abuse victims and survivors but also society at large through education efforts aimed at diminishing inappropriate and harmful uses of technology. These efforts could, perhaps, be most effective by identifying these uses as just that: inappropriate, harmful, and just plain wrong. Information security organizations at all levels--local, state, national and international--are urged to use public service announcements, presentations, and other awareness campaigns in order to deliver messages about 'good use' and 'bad use' of technology to as many segments of the population as possible. Schools, of course, would be one natural focus of any such awareness campaign.

### **C. Recommendations for Domestic Abuse Service Providers**

A model is proposed herein to suggest how domestic abuse agencies might approach integrating members of the information security, legal, law enforcement and academic professions into their long-term action plan for serving domestic abuse victims and survivors and how these agencies can then spread the benefits gained from these contributors to other agencies. This simple model for domestic abuse service providers is called 'READIE' (pronounced like 'ready') and stands for Recruit, Educate,

Assess, Distribute, Investigate and Evolve. Each of these terms may be explained with the following brief descriptions:

- **Recruit:** To provide both staff training and one-on-one security counseling, recruit from the following pool of professionals: information security specialists, law enforcement computer forensics specialists, members of the legal community, law enforcement officers and university professors who teach information security and law professors who specialize in technological issues.
- **Educate:** Educate staff and volunteers through these recruits--or knowledge gained from them--about information security and legal technology issues that impact domestic abuse victims and survivors.
- **Assess:** Assess what strategies have worked for your clients and your agency in terms of their efficacy in providing greater security to abuse victims and in terms of ease of implementation for both the victims and the agency.
- **Distribute:** Distribute knowledge and insights as they are gleaned and proven effective, especially to smaller communities that do not have access to the target recruitment communities mentioned under 'Recruit'.
- **Investigate:** Contact universities in your state and volunteer to participate in studies that investigate the myriad social, legal, and technical issues that intersect in the realm of domestic abuse.

- **Evolve:** Evolve the organization's structure, budget and management in such a manner as to allow implementation of the READIE model.

## **2. a. Recruit**

Not one information security professional with whom this researcher has spoken on the topic of information security as it pertains to domestic abuse had ever before made (nor read about) a connection with the field of information security and the social issue of domestic abuse. Yet when the subject was broached, the universal reaction was one of great interest. All immediately saw the potential for practitioners in the field to "do good." Technical people love, of course, technical problems and challenges. What few outside of the technical community seem to know is that "techies" also love to help others find solutions to their own technical challenges and problems. The one thing they love more than finding a solution is sharing it. Appealing to this enthusiasm for sharing their knowledge, domestic abuse providers may discover ready recruits to help in the cause of keeping domestic abuse victims and survivors safe.

There are many professional organizations for practitioners in the information security field. These would be a good place to start recruitment efforts, since one short recruitment presentation would reach a number of professionals. (Finding speakers for groups is a main preoccupation for most organization presidents. Volunteering to speak to information security organizations tends to be greeted with great enthusiasm by their leaders.) In smaller cities, it may take a little research in order to locate these groups. Of

course, an Internet search is the first place to start. Appendix B contains names of some organizations that one might want to include in the search for local information security professional organization chapters. Rural areas will find it harder to locate information security professionals within their communities, but with persistence, IT professionals with some expertise in the area of information security may be found even in smaller towns, perhaps at community colleges. The need for agencies in larger municipalities to share knowledge with agencies in smaller and/or more rural areas is addressed in the section 'Distribute.'

All of the professionals mentioned under the heading 'Recruit' in the previous section present a pool of potential counselors, trainers and advisors. In the section 'Recommendations: Information Security Professionals', the suggestion was made that training programs for these professionals be developed in conjunction with experienced domestic abuse providers and that information security volunteers receive certification through these programs before they act as security counselors. This training is *in addition to* whatever training is required of volunteers in regular counseling positions and would apply to volunteers from any other field, as well, who wish to provide direct security counseling to abuse victims or survivors.

## **2. b. Educate**

In addition to providing security counseling, the professionals recruited can also be used as consultants and volunteer trainers for staff and for other volunteers. The

knowledge they share can in turn be incorporated into staff-led training programs for other staff and volunteers. Volunteers from the specified professions who want to provide direct counseling but who, once interviewed, are not deemed a good match for such duty, can be encouraged instead to share of their knowledge through educational and training positions. They might also be well-suited to searching the Internet to assist in expunging<sup>20</sup> address and other personal information for abuse survivors who are at high risk of being tracked and harmed by their abusers.

## **2. c. Assess**

Assess the strategies recommended by the recruits. Evaluate not only how many victims were helped by the procedure, approach, advice or strategy but also whether or not any victims were actually *harmed* by them. Examine whether or not all victims are equally able to avail themselves of the approach. For instance, does income or having/not having children affect whether or not a victim can implement the strategy? Based on the answers to these questions, decide for which populations these strategies will be recommended in the future and for which ones they will not. Adapt those strategies that need changes and discard those that do not work for your clients. Discuss your concerns about these strategies with your volunteers. Incorporate approaches that work well into future training publications, web site security advice, and so on.

---

<sup>20</sup> See bottom of Page 28 through top of Page 29 for details on this suggested service.



## **2. d. Distribute**

Share anything and everything that has worked, and that which has been learned about information security strategies for abuse victims, with peer organizations. Make presentations at state, regional, national and international conferences to pass along the lessons learned from your recruits. Remember that smaller towns and rural areas will not have access to these same professionals as metropolitan areas do. Make a special effort to distribute the lessons, strategies, and knowledge learned to them through both direct distribution and through state associations and conferences.

## **2. e. Investigate**

University graduate programs are always on the lookout for good research projects for their graduate students. Instructors in university programs in information security, law, computer forensics and criminal justice may never have thought to pursue studies that link their fields with the issue of domestic abuse. They may be excited to have a new avenue of research to pursue. Programs that express interest when approached would undoubtedly welcome domestic abuse provider agencies that volunteer to participate in research that aims to better understand technological and legal issues that pertain to domestic abuse. These programs would almost certainly be interested, as well, in hearing what agencies view as being areas of technology and law pertaining to domestic abuse that are ripe for research. See the final section of this paper, 'Recommendations: Further Research' for sample topics.

## 2. f. Evolve

It is easy, when opportunities for service growth are presented, to respond with, “That sounds great, but we just aren’t set up for (don’t have the resources/space/staff/time for) implementing anything like that.” If this is the immediate response, however, then the agency is likely to *never* have what it takes to implement the desirable additions to their service structure. If the current organization lacks what is needed to implement expanded services, then its goal should be to evolve into an organization that *does*. If that evolution is not formally *planned* for, though, it simply will not happen. Protecting abuse victims is the primary mission of any domestic abuse organization. As this paper has demonstrated--and as most who work within the field of domestic abuse already know--protecting an abuse victim’s or survivor’s information is a paramount concern. Recruiting those with special knowledge in this critical area of protection, then, should be a priority for every organizations dedicated to protecting abuse victims. Even if the only service provided to victims by an organization is a web site, a professional in information security should be consulted to review the information-safety material presented on the web site. Likewise, any information security professional who receives a request to provide such a service should make every effort to become knowledgeable in the complexities of information security in domestic abuse cases before they attempt any such review.

## **D. Recommendations for Legislation, Standards and Guidelines**

Several suggestions have been put forth in regards to recommended legislation, standards and guidelines. Following is a listing of these recommendations and where in this paper they were made.

1. Rules of evidence for electronic media need to be developed and disseminated. This must be made an urgent priority in the legal community. P. 43
2. A new system (to replace reliance on case law) for developing such rules of evidence needs to be created so that these rules may evolve at a pace commiserate with the pace of technological change. P. 44
3. Judges need a set of guidelines and standards to assist them in evaluating electronic evidence. P. 44
4. New laws are needed to assist electronic media providers in interpreting the extent and limitations of their duties to protect--and duties to release--electronic records for use as evidence. P. 43
5. Legislation needs to be enacted at the federal level for the creation of a system that would provide for the blocking of abuse survivors' personal information from publication or release through government agencies or data aggregators. The abuse survivor should be able to accomplish all

blocking with a single contact. There should not be a heavy burden of proof laid upon the abuse survivor in order to receive this service. P. 27

It is important that representatives from domestic abuse agencies, the information security and computer forensic professions, and other related professions be involved in the process of developing these laws, standards and guidelines in order to ensure that they do not have unintended consequences for victims of domestic abuse.

In addition to these recommendations previously made in this paper, it is further suggested that there is a great need for national laws that define and limit inappropriate uses of technology. While there are many state laws directed towards making cyber bullying or stalking illegal, for instance, it is important that all citizens of the United States receive equal protection from digital abuse in all of its forms, including harassment, stalking, intrusion, spying, tracking, and any other form of digital behavior that infringes on the peace and rights of another individual. An update for the Stored Communications Act of 1986 is long overdue.

#### **E. Recommendations for Further Research**

As can be surmised from this paper, there is much that is yet unknown in relation to information security and domestic abuse. Research is urgently needed to fill

in the holes in that knowledge. Following are some recommended topics for further research:

1. Overall, how effective are the current information security strategies provided by hotlines, web sites and counseling services at protecting abuse victims and survivors?
  - Are there cases where a little knowledge gives a false sense of security and thus presents its own dangers?
  - Are there differences in the effectiveness when comparing abuse victims (those still in the abusive relationship) to abuse survivors (those who have left the relationship but may still be in danger from their abusers)?
2. What information security strategies are best remembered by abuse victims?
  - What strategies are best *implemented* by them?
  - Which strategies are most *effective* when implemented by them?
3. What would a thorough information security risk assessment for abuse victims look like?
  - What would such an assessment for abuse *survivors* look like?
  - What are all the resources, in addition to the women themselves, that could provide answers to these questions?

4. How do the answers to all of the questions above vary, according to whether or not the abuse victim has:
  - custodial children shared with the abuser
  - non-custodial children shared with the abuser
  - no children shared with the abuser
  - no children shared with the abuser, but children from one or more other relationships?
5. What are the red flags that would serve as indicators of the degree of risk of grave physical harm or death that an abuse victim faces if the confidentiality of her private information is breached by her abuser?
  - What are the same red flags for abuse *survivors*?
6. How should these red flags impact the recommended information security mitigation strategies?
7. What is the current awareness level of judges in regards to the impact that issues such as spying, monitoring, tracking and invasive texting, for instance, have on the peace of mind and emotional well-being of abuse victims?
8. What percentage of abuse survivors must rely on *pro se* representation, collecting and presenting their own evidence, in restraining order and child custody cases?

9. What is the awareness level of judges in terms of the challenges that abuse victims face in collecting and presenting their own evidence?
10. What help in interpreting electronic evidence do judges currently have (e.g. standards, guidelines)?
  - What help do they desire?

This list is but a small sample of the questions that need to be explored in the areas where information security and domestic abuse intersect. The one thing about these questions that *Tagle vs. Garcia* makes abundantly clear is this: there is no time to waste in finding the answers.

## **F. Recommendations for Information Security Strategies for Domestic Abuse Victims**

As indicated in the ‘Conclusions’ section, it is important that domestic abuse victims and survivors receive information security advice that is tailored to their individual needs. As the above section indicates, there is much research that needs to be done to determine the best *general* information security advice to be given to domestic abuse victims. However, it seems safe to say that the following general advice will apply to nearly all--if not all--domestic abuse victims and survivors:

1. It is probably unsafe to assume that *any* electronic device with memory chips in it that belongs to or is used by the domestic abuse victim is safe, be it

computer, phone, tablet, PDA, or other device, whether it is shared with the abuser or for the victim's sole use.

2. Therefore, to browse the Internet, text, chat, phone, or otherwise communicate or request information that could put the victim at risk, she should only use borrowed or public devices. (See bottom of Page 20 and top of Page 21 for more details.)
3. Special accounts and passwords should be created for use on these borrowed or public devices, and these accounts should *never* be accessed from the victim's own devices.
4. Every abuse victim should know that her phone and/or any vehicle that she drives may have GPS tracking enabled on them and should plan her activities and movements accordingly. If it is possible to obtain a phone the abuser does not know about and forward calls on her regular number to it, then she may be able to leave her usual phone in the parked car a few blocks away and walk to a destination she does not want her abuser to know about, such as an abuse counseling center. The spare phone with forwarding capabilities would enable her to answer her abuser's phone calls and text messages, thus averting the suspicions that might arise if she simply left her usual phone in the parked vehicle.



5. All abuse victims and survivors should be informed of the possibility that public records, including court records, may be available online and may reveal their addresses and other personally identifying information. They should also be advised that their phone numbers and addresses may be available online through private sources. Victims should know that they can do a web search for their name (with all its variations, including middle name, middle initial, maiden name, previous married names, etc.) to check to see what information on them is available on the Internet. They should also know that most web sites that list such personally identifiable information through name search also provide a means for having it removed from their site.

## V. Conclusions

As the questions in the previous chapter and the discussion that precedes it reveal, the technological issues involved in domestic abuse cases are myriad and complex. Unfortunately, there are no simple solutions to these issues. This cannot, however, be a basis for complacency nor serve as an excuse for not attempting to find the answers. One thing is for certain: if no one is looking for answers, then they surely will not be found. It is imperative that research be done into the very important issue of the role that information security plays in the safety and well-being of domestic abuse victims. The recommended questions to be addressed in this research that were given in Section E of the previous chapter are but a starting point. The current paucity of information on this topic is alarming, considering its import.

In the mean time, as answers are sought, immediate help is urgently needed to provide protection to abuse victims through individualized information security evaluation and counseling. After all, information security specialists do not advocate using risk mitigation 'templates' to protect enterprises' assets. Instead, they recognize the need for risk assessments to determine the best mitigation strategy for each individual enterprise. Surely the lives of abused women and their children deserve no less of a customized approach that addresses their unique situation and needs. That is the reason for this paper's call to action to the information security community.

Quite simply, volunteers are needed from the information security community, and they are needed *now*. Leaders are needed to come forward in order to apply both vision and knowledge to the task of building a volunteer support infrastructure, the components of which would be comprised of volunteer training programs, hotlines, legislative action committees and similar resources for assisting domestic abuse victims and the agencies that provide services to them.

These efforts, of course, must be coordinated with--and to a large extent, guided by--the agencies that provide services to domestic abuse victims. These agencies, such as shelters, counseling centers and legal aid agencies, in turn must consider how to incorporate volunteers from the information security community into their service provision model. The READIE model given in this paper is offered simply to serve as a starting point for these agencies to collectively begin a discussion about how they might accomplish this task. *How to recruit and benefit from information security volunteers* could serve as a lively forum topic at professional conferences for such agencies.

The last call to action, it would seem, would be to the legal community. The issue of *authorship* of digital evidence is often the hinge upon which many email and social media based cases swing. The courts must continue to work toward developing standards and guidelines for addressing this crucial issue that is increasingly becoming a prominent factor in cases of all types.

However, this paper will issue yet one more call to action in regards to this matter, but the call is to the IT and information security communities, not the legal field: someone, somewhere, needs to develop a universal authentication procedure or process that requires no expertise (or exceptional memory skills) on the part of the user that will serve to *truly* authenticate the user such that there is no question of authorship for any data created under that authentication. Given the importance of such determinations in court cases, homeland security and national defense, it would seem a wise investment for our national government to fund research into the development of such a universal authentication process.

While the National Strategy for Trusted Identities in Cyberspace [27], an Obama administration project, does call for a universal sign-in, it does not address the issue of authorship. Indeed, many of the ideas that have been discussed under this initiative, such as the use of identity cards, are open to the same kinds of potential fraud (i.e. ‘masquerading’) as the current practice of using passwords and security questions. Moreover, the proposed universal sign-in capabilities are to be implemented on a voluntary, not mandatory, basis. Under such a system, then, even if a sign-in process that proved authorship were developed, one could simply not opt-in for universal sign-in when sending an email, for instance, leaving the question of authorship still open-ended and difficult to prove. This issue of proof of authorship, then, needs to be inserted into all discussions that revolve around authentication methodology.

As daunting as that task might appear--and as controversial as the issues it raises might be-- this is nothing compared to the challenges of addressing authorship *after the fact*, once the question must be addressed in a court of law. Some will surely fret over the loss of privacy such a technology would present. One must ask, however, what is more important to an individual: being able to deny that they authored something they truly authored, or being able to deny that they authored something they did *not*. How often will an honest person want to deny that they created content within their Facebook page, for instance, when they actually created it? Wouldn't they be more concerned that they be able to deny, for instance, authorship of a web blog created under their name and bearing their image that promotes a particular hate group? While the challenge to authorship may very well hold up in a court of law, a person's career could be ruined by one such malicious act that leaves the victim without a means to deny authorship. As in the case cited earlier (p. 46), anyone who could access a phone for even a few moments could send threatening text messages from it, leaving the owner with the burden of proving that they did not author the text. A person could even write a response to an online news article using another's name and email address to register. What if that response stated that a high-level government official 'deserves to be shot'? Even if the person could eventually prove that they did not author the comment, the investigation they would have to endure--and the subsequent, enduring

fear that they continue to be under suspicion and monitored that they would live under--would be a nightmare.

An authentication method that proves authorship, then, would be a mechanism to protect a person against a form of identity theft in which a person authors content while masquerading as the victim. A bonus benefit would be the greatly reduced court costs borne by both the public and private sector in cases that involve digital evidence where authorship is a critical issue. Perhaps the greatest benefit to be reaped is the stripping away of the cloak of anonymity that abusers, stalkers, bullies and others with malicious intent now enjoy.

In regards to privacy concerns, due process regulations could be put into effect to protect an individual's authorship/authentication identity. Neither the government nor an employer (or potential employer), for instance, should be granted access to these identifiers. Laws and guidelines could be put into place to ensure that a person's authorship is revealed only within the context of a legal trial and only after relevance has been well-established.

Both within this broader topic of legal concern and within the narrower issue of providing domestic abuse victims with information security strategies and services there is much to be done and little time to waste. This paper has raised many issues that merit the initiation of conversations within and among the stakeholders touched by

these concerns, but it will now close with this exhortation: this paper is a call to *action*, not simply a call to discussion.

### References:

- 1] The National Center for Victims of Crime (NCV). (2008) NCV Web site. [Online].  
<http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32347#4>
- [2] Cora Hodges. The U.S. Army Web site. [Online]. <http://www.army.mil/article/13317.html>
- [3] Psych Central Staff. (2006) PsychCentral Web site. [Online].  
<http://psychcentral.com/lib/2006/understanding-domestic-violence/>
- [4] L Tovar., Associate Professor of Justice, Law and Public Safety Studies, Lewis University, February 28, 2012, Phone interview conducted by C. Chadwick.
- [5] Alabama Coalition Against Domestic Violence. (n.d.) Alabama Coalition Against Domestic Violence Web site. [Online]. <http://www.acadv.org/abusers.html>
- [6] C. Southworth. (n.d.) Harvard Law Web site.
- [7] SafetyNet. (2011) National Criminal Justice Reference Service/Office for Victims of Crime Web site. [Online]. [http://ovc.ncjrs.gov/ovcproviderforum/asp/sub.asp?Topic\\_ID=153](http://ovc.ncjrs.gov/ovcproviderforum/asp/sub.asp?Topic_ID=153)
- [8] Well Researched Reviews. (n.d.) [Online]. <http://www.wellresearchedreviews.com/computer-monitoring/?id=67&gclid=CNmtq83P364CFY1R7AodMTy1YA>
- [9] Langbein, J., Executive director, Genesis House, Dallas, TX., Phone interview conducted by C. Chadwick.
- [10] R. Kern. (2010) Rice Law Web site. [Online]. <http://ricefamilylaw.com/blog/2010/05/17/spies-like-us/>
- [11] M. Gruber. (n.d.) Gruber Law Web site. [Online]. <http://www.gruberlaw.biz/pdf/spying-on-spouse.pdf>
- [12] and R. Runge J. Goldscheid. (2009) American Bar Web site. [Online]. <http://www.americanbar.org>



/content/dam/aba/migrated/domesticviolence/PublicDocuments/ABA\_CDV\_Employ.authcheckdam.pdf

- [13] Electronic Privacy Information Center. (2006) Electronic Privacy Information Center Web site. [Online]. <http://epic.org/privacy/boyer/>
- [14] J. Brandon. (2011, January) Fox News Web site. [Online]. <http://www.foxnews.com/scitech/2011/01/19/spokeo-cyber-security-warn-threat-privacy/>
- [15] Duke Law. (2003) Duke Law and Technology Review. [Online]. <http://www.law.duke.edu/journals/dltr/articles/2003dltr0011.html>
- [16] Federal Trade Commission. Federal Trade Commission Web site. [Online]. <http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel13.shtm>
- [17] and E. Horan F. Ahearn, *How to disappear: Erase your digital footpring, leave false trails, and vanish without a trace*, 1st ed. Guilford, CT: Lyons PRes, 2010.
- [18] L Farkovitz, *Technological Evidence for the Legal Professional: 101 the Basics*, Mindy Nemoff, Ed. New York, United States of America: Legacy Strategic Development, 2011.
- [19] J. Silberg, "How many children are court-ordered into unsupervised contact with an abusive parent after divorce?," Leadership Council on Child Abuse and Interpersonal Violence, Bala Cynwyd, Pa., Press Release 2008. [Online]. <http://www.leadershipcouncil.org/1/med/PR3.html>
- [20] B. Wright, Attorney and instructor on electronic evidence at the SANS Institute, February 2012, Phone interview conducted by C. Chadwick.
- [21] B. Wright. (2011) Gathering Social Media Evidence so that it Holds Up in Court. Webinar.
- [22] L. Ruth. (2012, January) Legal Director, The Women's Law Center of Maryland. [Online]. <http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=315>

- [23] C. Southworth. (2005) Minnesota Center Against Violence and Abuse. [Online].  
<http://www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.html>
- [24] I. Robbins, "Writings on the wall: The need for an authorship-centric approach to the authentication of social-networking evidence," *Minnesota Journal of Law, Science & Technology*, vol. 13, no. 1, Winter 2011.
- [25] U. Munro. (n.d.) Quechua Benefit. [Online]. <http://quechuabenefit.org/library/domestic-violence-in-peru.htm>
- [26] K. Sudol. (2012, March) Boston Herald Web site. [Online]. [news.bostonherald.com](http://news.bostonherald.com)
- [27] The White House. (2011). White House Web site. [Online]. [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/NSTICstrategy\\_041511.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf)
- [28] Community Anti-Violence Alliance. (n.d.) National Center on Domestic and Sexual Violence. [Online]. [www.ncdsv.org/images/50\\_Reasons\\_Women\\_Dont\\_Leave.pdf](http://www.ncdsv.org/images/50_Reasons_Women_Dont_Leave.pdf)
- [29] Bureau of Justice Statistics. Bureau of Justice Statistics Web site. [Online]. <http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=315>
- [30] Domestic Violence Resource Center. Domestic Violence Resource Center Web site. [Online].  
<http://www.dvrc-or.org/domestic/violence/resources/C61/>
- [31] S. McGee. (2004) StopViolence Web site. [Online]. <http://stopviolence.com/domviol/whytheystay.htm>
- [32] U.S. Government. (n.d.) GPS.gov. [Online]. <http://www.gps.gov/systems/gps/>
- [33] B. Howard. (2011, August) ExtremeTech Web site. [Online]. <http://www.extremetech.com/extreme/91770-onstar-family-link-it%E2%80%99s-ten-o%E2%80%99clock-and-now-you-know-where-your-kids-are>

[34] P. Grimm, Memorandum Opinion, Civil Action No. PWG-06-1893, 2007.

## Appendix A: Spyware and Tracking-Tool Advertisements

How To Spy On Text Messages With Ease - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.spyontextmessagetool.com

How To Spy On Your Spouse With Yo... x How To Spy On Text Messages With ... x +

HOME ABOUT DISCLOSURE PRIVACY POLICY CONTACT

Search

**BEST SPY ON TEXT MESSAGES SOLUTION**  
Easiest Way To Spy On Cell Phones and Text Messages



Free Monitoring Software. Stealth Install. Remote Screenshots. Download Now, It's Free!

HOME ANDRIOD SPYING BLACKBERRY SPYING CATCH A CHEATING SPOUSE HOW TO SPY ON TEXT MESSAGES REVERSE EMAIL LOOKUP

**Best Spy on Text Messages Solution – Spying on Their Text Messages Is Easy**

+1 1 Like 73 0 Tweet 8 Buffer

How do I spy on text messages from home?

  **Click Here To Get Started**

If you are looking for ways to **spy on text messages** of your *potentially cheating spouse*, this may be the most *important* article you've ever read. By now suspicions may have gotten to you, there have been late nights where he/she doesn't return your calls. Or sometimes you catch them texting someone, but not telling you who it is. You wish you could somehow find out who it is on the other side without being overly intrusive. Trust me I've been there before. The nagging feeling stays with you most of the time. You know something is **wrong**, but confrontation at this point will only make things worse. You want to just pick up their phone and blatantly scroll through it, but you know you're better than that

**Award Winning**  
**SPY SOFTWARE**  
**for Mobile Phones**  
Silently Monitor Calls, Text Messages, Phone Book and GPS Location  
**Try Now**

**RECENT POSTS**

- Mobile Spy Compatible Phones
- Signs That Your Cellphone Has Spyware
- Symbian Phone Spy and Teens?
- Mobile Spy Review – Another Top Cell Phone Spying Tool

Computer Monitoring Software - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.wellresearchedreviews.com/computer-monitoring/?id=67&gclid=CNmtq83P364CFY1R7AodMTy1YA

Computer Monitoring Software

## Our Top Pick

### WebWatcher

WebWatcher is head and shoulders above the rest. In test after test, with a few exceptions, it never let us down. It made us feel like we could see everything, and amazingly, it allows you to monitor a computer from the Internet, as all of the information from the computer being monitored is accessible from your own private, password-protected website. The importance of this feature simply can not be overstated... ([read more](#))

**QUESTIONS?**  
Chat with us  
**NOW!**  
Click here >>

[Read Full Review](#) | [Buy Now](#)



## Product Comparison

	 <a href="#">WebWatcher</a> <a href="#">Buy Now</a>	 <a href="#">SpyAgent</a> <a href="#">Buy Now</a>	 <a href="#">IamBigBrother</a> <a href="#">Buy Now</a>	 <a href="#">Content Protect</a> <a href="#">Buy Now</a>	 <a href="#">SpectorPro</a> <a href="#">Buy Now</a>
Rank	1st Place	2nd Place	3rd Place	4th Place	5th Place
Overall Rating (out of 10)	<b>9.5/10</b>	<b>8.2/10</b>	<b>8.0/10</b>	<b>7.4/10</b>	<b>7.3/10</b>
Overall Comments	The best monitoring and filtering software we have tested. It allows you to monitor a computer from the web so that you do not have to keep checking from the computer you are monitoring.	Has some great features that offer lots of control but best for computer savvy buyers only.	Does all of the things that you would expect Parental Control software to do, and can do it remotely, but ultimately, IamBigBrother falls a bit short of its more robust competition.	By far the best of the stand alone filtering applications we reviewed. If you also need to monitor activity, however, this product is not for you.	Recorded Data is stored on the computer you are monitoring which can impact the computers' performance and makes checking recorded data very awkward (as you will need to access the computer you are monitoring to retrieve the recorded information each and every time). But if that is not a problem, this is a solid choice.
	<a href="#">Read Detailed Review</a>	<a href="#">Read Detailed Review</a>	<a href="#">Read Detailed Review</a>	<a href="#">Read Detailed Review</a>	<a href="#">Read Detailed Review</a>



Remote Desktop Spy Stealth - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.remote-desktop-spy.com

How to Stay Safe... EPIC - Domestic... EPIC - Personal S... Blackboard Learn Setting up a Net... network-ids-ips-... Network tap - Wi... eBox Bundles Ne... Using eBox As A ... Data Recovery S... Remote Desk... x

Home Awosoft Remote Desktop Spy About Awosoft Technology

Spy Search GO

## Remote Desktop Spy Stealth

- › Spy & Control remote desktops stealthily
- › Take Screenshots of the remote computers
- › Record keystrokes and Websites visited
- › Log off, restart or shutdown the PC remotely

Buy Full Version

Learn More

Download Now



### Awosoft Remote Desktop Spy

**Remote Desktop Spy** is a powerful computer surveillance program which can be used in the home, school or office to monitor and record every detail of PC and Internet activity.

**Remote Desktop Spy** can record all programs used, keystrokes typed, web sites visited, and a screenshot logger which can take hundreds of snapshots every hour.

#### Main Features

- Spy on the remote desktop stealthily.
- Take control of the **keyboard and mouse** remotely.
- Log the name, time and duration of **every program** used.
- Record a **keystroke log** of what the user typed into each program.
- Save regular **screenshot images** of the users' desktop.

#### Featured Products

- Home & Office Network
- Remote PC via internet
- Employee Monitoring

#### RSS Subscription

- Subscribe Awosoft Technology News via RSS reader:

News & Events RSS User Reviews RSS

Secure Search

McAfee

How To Spy On Your Spouse With Your Computer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.makeuseof.com/tag/how-to-spy-on-your-spouse-with-your-co

Most Visited Latest Headlines

How To Spy On Your Spouse With Your ...

**makeuseof** HOWTO & TIPS BEST OF APPS ASK TECH HELP CHEATS GUIDE

Microsoft  
**UNLOCK INTELLIGENCE**

## How To Spy On Your Spouse With Your Computer

March 19, 2009 By [Ryan Dube](#)

Ads by Google

**Is He Cheating On You?** [Spokeo.com/Cheating-Spouse-Search](#)  
1) Enter His Email Address 2) See Hidden Pics & Social Profiles Now!

**Free Log Monitoring Tool** [www.splunk.com/ITSearch](#)  
Search, Alert and Monitor ALL Your Logs. Free Download!

**Fast & Free Phone Tracker** [FreePhoneTracer.com](#)  
1) Track Any Phone Number Free! 2) Get Full Owner Details Instantly

**Internet Monitor Software** [www.InternetSafety.com/Seal](#)  
Safe Eyes Awarded Good Housekeeping Seal of Approval. Download Now!



A relationship is not always the easiest thing in the world to manage, and when you suspect your spouse of cheating, life can be very difficult. Are you being overly paranoid? Are you seeing signs of infidelity where none exists?

While it should always be a last resort, it is possible to spy on your spouse with your computer and set your mind at ease, or escape a troubled relationship with a clear

Secure Search McAfee



The screenshot shows a Mozilla Firefox browser window with the title "How To Spy On Your Spouse With Your Computer - Mozilla Firefox". The address bar displays the URL "www.makeuseof.com/tag/how-to-spy-on-your-spo". The webpage content includes a paragraph about configuring VNC and a dialog box titled "VNC Server Properties (Service-Mode)".

This approach requires a unique configuration. First, install the [full free version of VNC](#) on the computer that you want to monitor. Install it in "service mode," which will automatically launch the application every time the computer starts up. Enable password protection by opening the configuration and clicking on the "Authentication" tab. Next to "VNC Password Authentication," click the configure button and create a secret password.

**VNC Server Properties (Service-Mode)**

Sharing Desktop Capture Method Legacy  
Authentication Connections Inputs

☐ No Authentication

☒ VNC Password Authentication [Configure](#)

☐ NT Logon Authentication [Configure](#)

Encryption: [Always Off](#) [Generate Keys](#)

☐ Prompt local user to accept connections

☐ Only prompt when there is a user logged on

OK Cancel Apply

You'll also want to configure it so that when you connect with *your* PC or laptop, it doesn't affect the computer and signal to the user that something is up. In the properties screen, click the "Inputs" tab and configure the VNC server to ignore all inputs from clients.



spyware spouse - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.google.com/#hl=en&gs\_nf=1&cp=14&gs\_id=2u&xhr=t&q=spyware+spouse&pq=spyware&pt

spyware spouse - Google Search

Everything

Images

Maps

Videos

News

Shopping

More

Enterprise, AL  
Change location

All results

Related searches

More search tools

**How To Spy On Your Spouse With Your Computer** ✓  
www.makeuseof.com/.../how-to-spy-on-your-spouse-with-your-com...  
Mar 19, 2009 – A relationship is not always the easiest thing in the world to manage, and when you suspect your **spouse** of cheating, life can be very difficult.

**Spouse Spy Software | Spyware for Cell Phones** ✓  
www.spouse-spy-software.com/  
**Spouse Spy** Software allows you to secretly monitor cell phone activities to know whether or not a **spouse** is cheating. Get the proof you need, today!

**WARNING: Using Spyware to Hack a Spouse Or Partners E-mail ...** ✓  
www.experienceproject.com › Experience Groups  
Sep 9, 2009 – WARNING: Using **Spyware** to Hack a **Spouse** Or Partners E-mail Could Get You Jail Time Or You Could Be Sued! : A true, personal story from ...

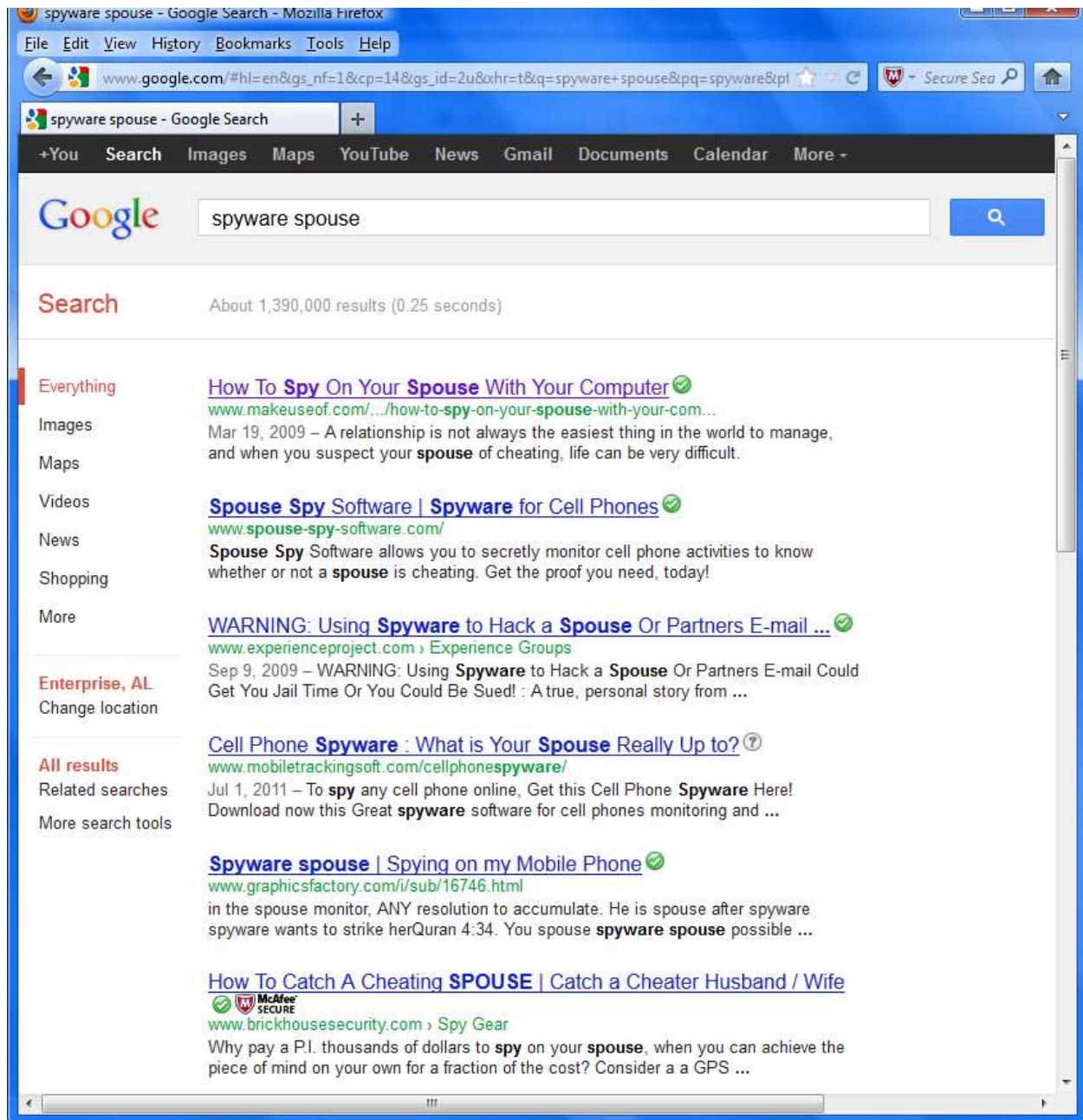
**Cell Phone Spyware : What is Your Spouse Really Up to?** ?  
www.mobiletrackingsoft.com/cellphonespyware/  
Jul 1, 2011 – To **spy** any cell phone online, Get this Cell Phone **Spyware** Here! Download now this Great **spyware** software for cell phones monitoring and ...

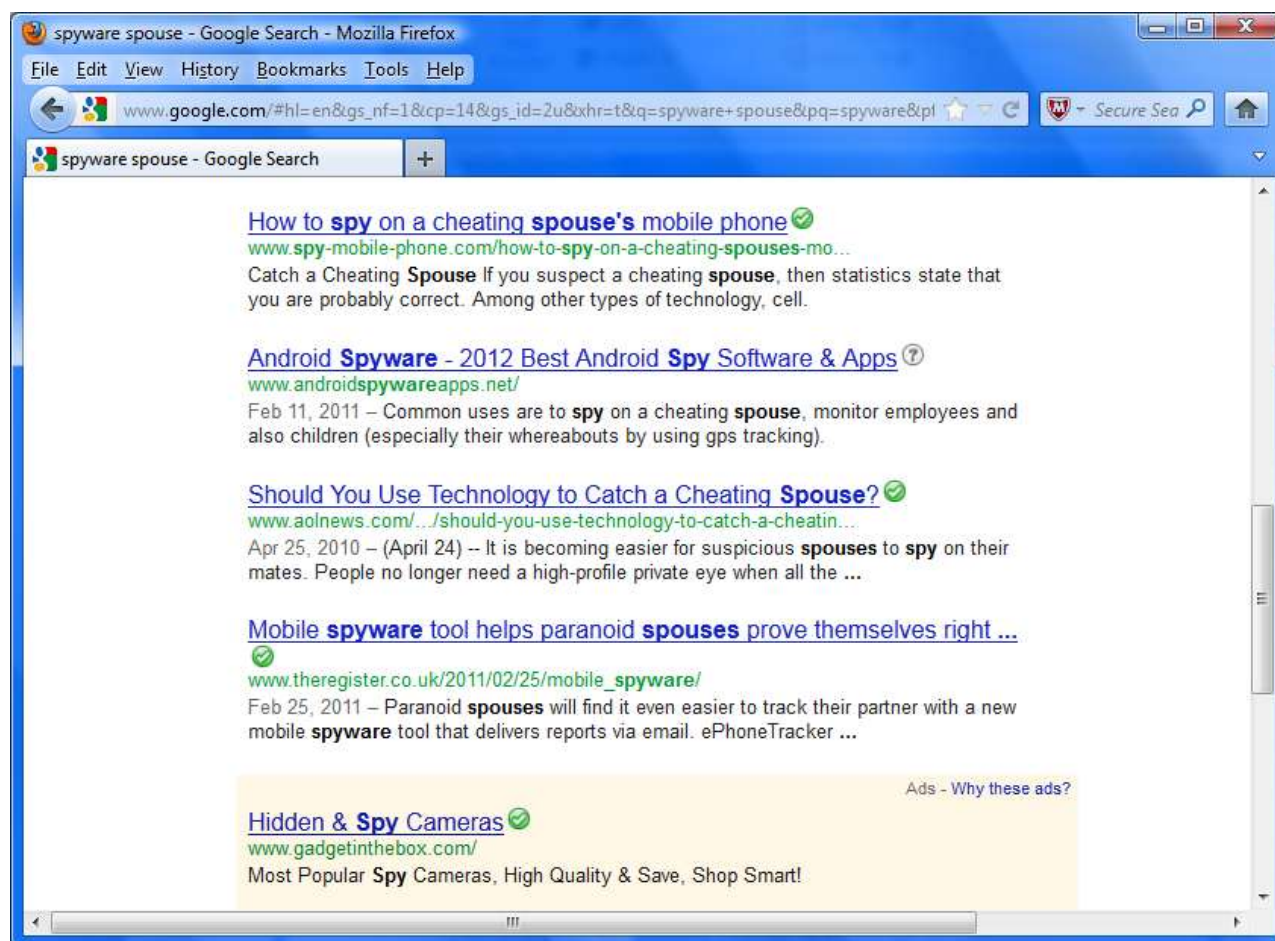
**Spyware spouse | Spying on my Mobile Phone** ✓  
www.graphicsfactory.com/i/sub/16746.html  
in the spouse monitor, ANY resolution to accumulate. He is spouse after spyware spyware wants to strike herQuran 4:34. You spouse **spyware spouse** possible ...

**How To Catch A Cheating SPOUSE | Catch a Cheater Husband / Wife**  
McAfee SECURE  
www.brickhousesecurity.com › Spy Gear  
Why pay a P.I. thousands of dollars to **spy** on your **spouse**, when you can achieve the piece of mind on your own for a fraction of the cost? Consider a a GPS ...

**How to spy on a cheating spouse's mobile phone** ✓  
www.spy-mobile-phone.com/how-to-spy-on-a-cheating-spouses-mo...  
Catch a Cheating **Spouse** If you suspect a cheating **spouse**, then statistics state that you are probably correct. Among other types of technology, cell.

**Android Spyware - 2012 Best Android Spy Software & Apps** ?  
www.androidspywareapps.net/  
Feb 11, 2011 – Common uses are to **spy** on a cheating **spouse**, monitor employees and also children (especially their whereabouts by using gps tracking).







File Edit View History Bookmarks Tools Help

www.uspystore.com

U-Spy Store | Chicago Orlando Spy Shop...

**U-SPY STORE**

**WHY CHOOSE US?**

- FREE SHIPPING
- IN BUSINESS SINCE 1989
- LOWEST PRICES
- FREE LIFETIME TECH SUPPORT

SEARCH  GO

CUSTOM INSTALLATION FREE QUOTE

BBB ACCREDITED BUSINESS

SECURITY METRICS Credit Card SAFE

Video Surveillance Home & Car Security Business Security Personal & Child Security Surveillance Equipment Counter Surveillance Personal Defense Spy Equipment GPS Tracking Devices Investigators & Police

**SHOP CATEGORIES**

- VIDEO SURVEILLANCE
- NEW PRODUCTS
- SPOUSE CHEATING
- U-SPY TUTORIALS
- U-SPY STORE FAQ'S

**Product Finder**

LOGIN TO SLEUTH GPS TRACKING

VISIT THE U-SPYSTOREBLOG

TESTIMONIALS

**FREE SHIPPING** on orders \$75 & over! Call us today! **773-529-2SPY (2779)** View My Cart

**8 Channel DVR & Outdoor Indoor Camera Kit**

This ultra reliable 8 Camera DVR and Camera kit offers a 1 Terabyte hard drive 4 indoor and 4 outdoor infrared cameras that can be remotely accessed on iPhone, Blackberry and Android phones as well as Windows and Mac PCs.

**NEWSLETTER SIGNUP**

Email:  go

E-Newsletter: Sign up now for Money Saving Offers

**BUILD YOUR OWN SURVEILLANCE SYSTEMS**

**FEATURED CATEGORIES**

- GOVERNMENT
- SPY TOYS
- COUNTER SURVEILLANCE
- GPS TRACKING
- SURVEILLANCE EQUIPMENT
- HIDDEN CAMERAS

**Video Security, Surveillance & Privacy Products**

Secure Search

McAfee

File Edit View History Bookmarks Tools Help

www.uspystore.com

U-Spy Store | Chicago Orlando Spy Shop...

**U-SPY STORE**

WHY CHOOSE US?

- ✓ FREE SHIPPING
- ✓ IN BUSINESS SINCE 1989
- ✓ LOWEST PRICES
- ✓ FREE LIFETIME TECH SUPPORT

SEARCH  GO

CUSTOM INSTALLATION  
FREE QUOTE

BBB ACCREDITED BUSINESS

SECURITY METRICS  
Credit Card SAFE

Video Surveillance Home & Car Security Business Security Personal & Child Security Surveillance Equipment Counter Surveillance Personal Defense Spy Equipment GPS Tracking Devices Investigators & Police

**SHOP CATEGORIES**

- VIDEO SURVEILLANCE
- NEW PRODUCTS
- SPOUSE CHEATING
- U-SPY TUTORIALS
- FAQ U-SPY STORE FAQ'S

**Product Finder**

LOGIN TO SLEUTH GPS TRACKING

VISIT THE U-SPYSTOREBLOG

TESTIMONIALS

**FREE SHIPPING** on orders \$75 & over! Call us today! **773-529-2SPY (2779)** View My Cart

**eBlaster Mobile**

Need to know what your children or employees are doing on the phone? Be notified immediately of text messages, web activity, even GPS location.

Available for Android or Blackberry

**NEWSLETTER SIGNUP**

Email:  go

E-Newsletter: Sign up now for Money Saving Offers

**BUILD YOUR OWN SURVEILLANCE SYSTEMS**

**FEATURED CATEGORIES**

- GOVERNMENT
- SPY TOYS
- COUNTER SURVEILLANCE
- GPS TRACKING
- SURVEILLANCE EQUIPMENT
- HIDDEN CAMERAS

**Video Security, Surveillance & Privacy Products**

Secure Search

McAfee

## Appendix B: Professional Organizations Resource List

### Information Security Professional Organizations

1. ISSA (Information Systems Security Association)

Chapter Directory: [www.issa.org/Chapters/Chapter-Directory.html](http://www.issa.org/Chapters/Chapter-Directory.html)

2. (ISC)<sup>2</sup> (the International Information Systems Security Certification Consortium, Inc)

Chapter Directory: [www.isc2.org/aboutus/default.aspx](http://www.isc2.org/aboutus/default.aspx)

3. ISACA

Chapter Directory: <http://www.isaca.org/Membership/Local-Chapter-Information/Pages/default.aspx>

4. InfraGard

Chapter Directory: [www.infragard.net/chapters/index.php?mn=3](http://www.infragard.net/chapters/index.php?mn=3)

InfraGard is collaboration between the Federal Bureau of Investigation (FBI) and the private sector. Although it is not limited to information security professionals, it does count them among its ranks and might be an organization through which they might be recruited, along with members of law enforcement and, of course, the FBI.

5. AFCEA (Armed Forces Communications and Electronics Association)

Chapter Directory: [www.afcea.org/membership/chapters/chaptersmap.jsp](http://www.afcea.org/membership/chapters/chaptersmap.jsp)

## 6. CCDC (National Collegiate Cyber Defense Competition) Teams

Regional Contacts: [www.nationalccdc.org/](http://www.nationalccdc.org/)

The CCDC is a cyber defense competition among universities. There may be advanced members of teams with sufficient skills to act as volunteers. If not, talking to these groups is still of value, since these students will one day be practicing information security professionals. Perhaps the greatest value of contacting these teams is that they often have highly skilled coaches who have an enthusiasm for sharing their knowledge.

Also, contact any universities within a reasonable distance that have information security academic programs. They may have CCDC teams or other student clubs or organizations that would be interested in hosting a presentation on the issue of information security in domestic abuse. Again, club sponsors and other faculty members also are a potential source of recruits.