Read more at www.lynchowens.com/blog

The Growing Problem of Digital Spying in Divorce Cases

By Carmela M. Miraglia | May 15, 2018

Criminal Law Family Law Divorce

Carmela M. Miraglia explores the growing trend of cyber spying and other forms of digital harassment in divorce cases.

Distrustful spouses have always spied on each other. In the modern era, however, it is no longer necessary to hire a private eye for to spouse to track his or her better half. In the era of social media, spouses and former spouses often engage in digital "self-help", tracking each other's movements through GPS, intercepting emails and text messages with one other's passwords, or simply searching the other's iPhone.

In Massachusetts, spying on spouses – or anyone else, for that matter – is typically illegal. However, the laws in Massachusetts that deal with eavesdropping and other forms of digital spying are often ineffective or poorly enforced.

It goes without saying that filing for divorce is an emotionally trying event. Some spouses, wanting to get the "upper hand," resort to worrisome or chilling tactics out of fear, jealousy, or anger. Some may even take part in the growing trend of digitally spying on spouses or ex-spouses, which has grown more frequent as technology has developed and helped to facilitate online monitoring of every kind.

The Growing Problem of Spouses Spying on Spouses

The issue of spouse-on-spouse spying was recently a topic in an interesting article for *National Public Radio*. In the story, a former wife was worried that her ex-husband was stalking her, based on his detailed knowledge of her exact whereabouts at any given time. He also had the details of private conversations she had with her close friends via text message.

When the wife took the car to the mechanic for a routine check-up, she asked him to look for a GPS device. The mechanic found a GPS device hidden in one of the wheel wells. Based on the battery life, the amount of battery power remaining on the device, and the length of time since the couple divorced, it seemed clear that the husband not only placed the device on the wife's car but had also replaced the device numerous times when the battery wore out.

When asked about the GPS device, the husband admitted to installing it on his ex-wife's car. When the wife's attorney brought this up to the court during a hearing for a restraining order, the court focused on husband's threatening behavior dismissing wife's concerns about the GPS device. The police also dismissed the wife's complaint about the GPS and closed the investigation after learning the vehicle was registered to both parties; as a joint owner of the vehicle, the husband could legally install the GPS to track its whereabouts.

The situation is not unique: lawyers and judges in divorce court are constantly dealing with evidence that was obtained through spying or stalking. According to the Department of Justice, 14 out of every 1,000 persons over the age of 18 in the U.S. are victimized by stalking every year. This figure jumps to 34 out of 1,000 when the victim is divorced or separated.

How Divorce Law Invites Spying Cases

Perhaps unsurprisingly, divorce often encourages digital spying. In Massachusetts, when a judge has to decide an alimony issue, he or she is only allowed to consider the factors set forth in M.G.L. c. 208, § 34. Some of these factors – like the conduct of the parties during the marriage or each party's sources of income – essentially reward one spouse's independent detective work. When this detective work is done by an attorney, using legal methods, it is called discovery. When spouses take the law into their own hands, illegal eavesdropping is often the result.

The incentives for spying are clear. Marital misconduct can affect how much, or even whether, alimony gets awarded. In many spouse's minds, the cost of spying on a spouse pays for itself if the judge finds the conduct uncovered through

spying warrants a reduction in alimony or child support, a change in the division of assets or an important child custody decision.

The disincentives for spying are often murkier. As discussed below, illegal eavesdropping by private citizens is a felony in Massachusetts. However, the crime often becomes harder to prove when spouses who live together have shared their digital lives over a lengthy period of time. A spouse breaking into the other's email account might claim he or she always had access to the other's password. Or, like the wife in the NPR story, police may be hesitant to prosecute when the spying mechanism involves jointly owned property, like a family car or computer.

Americans understand that government agencies like the NSA and FBI have vast forensic resources that allow agents to sift through mountains of digital data. What is less understood is how limited the training and resources are for many local law enforcement agencies attempting to address digital crimes like identify theft, cyberbullying and online harassment. Local police departments often lack the tools and personnel to investigate cyber-crime, much less prosecute cases.

Developing Technology Exacerbates Divorce Cyber Spying

Today's technology plays a prominent role in the upsurge of spousal snooping. With smartphones, apps, and the increasingly prevalent interest in "big data," spying on other people has never been easier. GPS tracking devices are readily available online for less than $30, and show exactly where the device, and thereby the person, is or has recently been. When combined with credit and debit card records – which offer their own form of geographic tracking each time an individual swipes his or her card – GPS data can provide a remarkably granular picture of an individuals' movements.

Good old-fashioned cell phone bills – which provide the date, time and phone numbers of all calls made, as well as the date and time of incoming and outgoing text messages – also add to the picture. Several factors contribute to vulnerability with cell phone bills. First, many families now pay for cell phone services on "family plans", in which a single family member pays for the cell phone service of each family member. Spouses often forget that his or her ex continues to receive the cell phone bill – and all of the usage data for phones under the plan – for as long as that spouse pays for the bill. Adding to the confusion, many individuals have "gone paperless", meaning that bills no longer show up in the mailbox, reminding each spouse of the sensitive data within. (Of course, the data is still available in digital form.)

Finally, encrypted messaging apps, such as iMessage and WhatsApp have contributed to a false sense of security with respect to cell phone billing records. Messages exchanged on iMessage or WhatsApp typically do not appear in cell phone billing records, causing users to assume their communications are private. However, few users recognize how many traditional text messages they actually exchange each month outside of these applications. For many wireless carriers, the dates, times and phone number of all traditional text messages appear on the billing statement.

PC Trackers: Tools to Monitor Children, Teens and Employees

Ironically, some of the most common digital spying tools were designed to help parents track the online activities of their children and teenagers in an increasingly complex online world. Companies like childguard.com offer a suite of products like WebWatcher and Net Nanny, that enable parents to monitor web surfing and social media activity by their children. Sophisticated new programs include “keyloggers” (which track everything typed on the computer) and provide detailed reports of when, how long, and how an individual used the computer each day.

In addition to protecting kids and teens, many employers now deploy sophisticated tracking software to monitor how employees are using computers and the internet. While using keylogging and other digital monitoring platforms to monitor children and employees is generally legal, few states (or courts) have defined the privacy rights of these groups, where the expectation of privacy for children (vis a vi their parents) and employees (vis a vi their employers) are lower than those of private adults.

The bottom line is that the legitimate need for tracking online behavior has spawned a large number of affordable and effective software tracking platforms that spouses can use on each other as easily as their children. And while many computer-based platforms can be detected and removed by users who know how to look, many Americans never bother to take even routine safety measures to ensure their online activities are not being monitored. In other words, when it comes to divorce, keyloggers and other forms of computer-monitoring are often hiding in plain sight.

Social Media: A Way to Connect or an Engine for Infidelity?

We've all heard the story. A middle-aged married man opens his Facebook account. He quickly finds friends from high school or college he thought he'd never see again. He also finds his old high school sweetheart, who is divorced and single. They start exchanging messages and find some of the old sparks remain…

Any social media company will tell you that a major goal for their platform is connecting people. This includes lonely people, individuals who are unhappy in their marriage, and online voyeurs who enjoy viewing the pictures and online behavior of others.

Any divorce attorney who has practiced over the last decade will tell you that social media is a driving source behind marital infidelity. Given the reality of social media a driver of affairs, it probably isn't surprising that suspicious spouses often track each other's social media activity with enthusiasm. For spouses with poor passwords (or security questions), or those being monitored by spyware or keyloggers, social media accounts are often a major target.

The Elephant in the Room: Your Smart Phone

Of course, the single biggest privacy risk that all of us carry is the smartphone we carry around in our pockets. As an attorney who has subpoenaed cell phone records from AT&T, Verizon and Apple, I can tell you from experience that the little computer in your pocket is tracking your every move, every second of the day. Your iPhone is constantly bouncing signals off of the closest cell phone tower, monitoring your general location even when GPS is not turned on. Every app you use, webpage you visit and swipe you make is tracked by your smartphone. It sees all.

Unsurprisingly, spyware for smartphones is invasive and pervasive. For a subscription price of less than $20 per month, a suspicious spouse can install a smartphone app on their spouse's phone that records everything the phone does from calls to texts to internet use to keystrokes. Like PC tracking software, many of the best smartphone trackers are built for parents who are seeking to monitor their children's behavior. While iPhones pose some special challenges for truly comprehensive spyware, Android phone represent the wild, wild west of digital spying. Almost anything goes.

Smartphone spying apps can be downloaded and installed in seconds, giving the spying spouse access into the other person's life even if they only briefly have control of the phone, while the other spouse has no knowledge that their device has been compromised. As was the case in the previously mentioned NPR article, the husband had installed software on the wife's phone and had access to

her text messages and emails. The wife only learned of the access when the husband sent her snippets of her own conversations with the husband. Other data includes recording of all photos, audio and digital use of the phone, real-time GPS and/or geolocation tracking, and keylogging of passwords and other sensitive information typed in text.

Digital Spying Laws Struggle to Keep Up in Massachusetts: The Eavesdropping Statute

To the dismay and surprise of many spouses, spying between private citizens does not implicate Fourth Amendment rights – those rights are only triggered when the government is doing the spying. Spouses, on the other hand, have a completely different set of rights against the sleuthing of their once significant others.

One of those rights in Massachusetts is enshrined in our state's wiretapping law, M.G.L. c. 272, § 99. This statute makes it a crime to use a device to secretly hear or record an oral or electronic communication. While this is occasionally mistaken to mean that everyone involved in a phone conversation has to actively consent to the recording, cases in Massachusetts have stressed only that the recording cannot be a secret one, reducing the need to obtain consent down to merely a need to notify others. See *Commonwealth v. Jackson,* 370 Mass. 502 (1976) (which holds that, if everyone in the conversation knows that it is being recorded, the law is not violated). Although it has been years now, I recommend Attorney Owens' 2007 law review article about illegal eavesdropping between private citizens in Massachusetts for a good overview of the statute and case law.

While Massachusetts' wiretapping law clearly pertains to oral communications, it has less application to other forms of cyber spying, such as GPS tracking, identity theft, or hacking of computers and devices.

Another Weak Law: The Massachusetts Identity Theft Statute

If the eavesdropping statute is difficult to enforce, then the Massachusetts Identity Theft Statute, M.G.L. c. 266, § 266, is just plain weak and poorly written. Despite the state being a worldwide leader in technology, the Massachusetts legislature remains a backwards, stilted institution. The state's identity theft statute makes it a criminal act for any person to obtain personal identifying information for purpose of harassing another. However, the statute defines "personal identifying information" narrowly:

> [A]ny name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.

Notably, the statute fails to identify common modern technologies such as email, smartphones or apps, leaving only the vaguely defined "computer password identification" for police to use. Worse yet, the statute defines "harass" in terms that do not necessarily fit for a digital spying case:

> 'Harass'', willfully and maliciously engage in an act directed at a specific person or persons, which act seriously alarms or annoys such person or persons and would cause a reasonable person to suffer substantial emotional distress.

In the divorce context, spying is often a form of passive or concealed information gathering. In other words, the purpose of a spouse's digital spying is rarely to harass, annoy or alarm another person. Nor is passive eavesdropping by a spouse guaranteed to meet the standard of causing "a reasonable person to suffer substantial emotional distress". The law was clearly written with traditional stalking victims in mind, but cyber spying in divorce cases often involves strategic monitoring and intelligence rather than an intent to harass or alarm the victim.

Even the word "pose" is problematic under the eavesdropping statute:

> ''Pose'', to falsely represent oneself, directly or indirectly, as another person or persons.

An improved statute would define "pose" as any person who uses the computer, email or digital password of another, without permission, to access the other's

private information or data. In contrast, the Massachusetts statute seems to require the spy to actively pretend to be the victim by sending emails or communications to third parties while impersonating the victim. This appears to provide little protection for victims of simple spying.

The Massachusetts Hacking Statue: Shamefully Outdated for a Tech-Savvy State

Massachusetts is home to MIT and many of the world's top biotech firms. One might think that intellectual property laws preventing computer hacking would be among the strongest in the country. One would be *wrong*.

The Massachusetts computer hacking statute, M.G.L. c. 268, § 120F, provides in full:

> Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both.
>
> The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.

Ignore the legal standard here and skip straight to the penalty: *shall be punished by imprisonment in the house of correction for **not more than thirty days** or by a fine of not more than one thousand dollars, or both*.

You read that correctly. Massachusetts, one of the technology leaders in the world, punishes computer hackers with **no more than 30 days in jail** or a fine under $1,000! Compare the pathetically weak Massachusetts statue with the long, detailed hacking law in California, which punishes serious hacking crimes as a felony that carries a three-year sentence.

The hacking statute *should* be the primary criminal statute in most divorce cybercrime cases, but the Massachusetts law is so weak as to be meaningless.

The Federal Statutes: Stronger Laws that Are Rarely Enforced

In addition to the Massachusetts law, there are a series of federal statutes that make hacking email and other online accounts a serious crime. These statutes

include 18 U.S. Code § 1343, the Wire Fraud Act, which can apply when an individual steals personal and confidential information from another. A similar statute, 18 U.S. Code § 1030, has been used expansively by federal prosecutors to confront hackers with serious prison time. Similarly, 18 U.S.C. § 2701, punishes the use of a computer to access another person's "electronic communication service" where the person has their email or voicemail stored. This statute often comes into play if individuals illegally access "cloud" based email services, like Gmail or Hotmail, and could be used to prosecute individuals who hack into cloud-based communication mediums.

In many cases, there is nothing *technically* preventing Massachusetts police and prosecutors from charging individuals with violations of the federal law within a state court. However, in practice, this rarely occurs. Moreover, it is generally very difficult to get the FBI or US Attorneys office to pay attention to spouse on spouse spying cases, which simply don't rise to the level of seriousness for federal law enforcement to become involved.

What Can Massachusetts Do to Prevent Cyber Spying Between Spouses

The first thing Massachusetts needs to do is update its pathetically outdated cyber crime laws. One would think that all of the businesses storing intellectual property in Massachusetts servers would have already lobbied for a stronger hacking law, but the state's statute is among the weakest in the country (if not the world). The identity theft statute should be broadened to include references to modern technology and devices, and expanded to include conduct such as unauthorized access to online accounts for the purpose of obtaining personal information. Finally, Massachusetts should create state versions of the stronger federal laws, such as 18 U.S. Code § 1030, and 18 U.S.C. § 2701, since federal prosecutors rarely enforce these laws in state jurisdictions.

About the Author: Carmela M. Miraglia is a Massachusetts divorce lawyer and Massachusetts family law attorney for Lynch & Owens, located in Hingham and East Sandwich, Massachusetts.

Schedule a consultation with Carmela Miraglia today at (781) 253-2049 or send her an email.