Privacy/Free Speech

Spying on your spouse

by Jeremiah M. Yourth

As a marriage begins to dissolve, so does the trust that once was present within it. Privacy in the context of a deteriorating marriage is a hot topic, as perhaps demonstrated most recently when users of AshleyMadison.com, a website that connects married people looking to have an affair, had their private information released to the public. As a family law attorney, clients often ask if they may read their spouse's email, tap their phone, install spyware, or use a Global Positions System ("GPS") tracking system to monitor their whereabouts. Just as frequently, clients neglect to ask before doing so, and simply show up at my office with their spouse's emails or recordings. They appear confused when I respond by aggressively asking them numerous questions about how they obtained the materials and showing no immediate interest in viewing the newly dug up dirt on his or her spouse. Many of these questions can be surprisingly complex and very fact-dependent. The issues are only further complicated by our evolving technologies, such as smartphones and social media.

Eavesdropping and hacking

Electronic evidence can be extremely valuable in a family law case. As such, it is used often and extensively. This evidence includes emails, text messages, recordings, instant messages, computer files, GPS data, photos and videos. The capabilities and depth of electronic evidence will only grow as technology continues to develop. The evidence is only helpful if it was obtained legally. In my experience, the most common issue that arises is gaining access to a spouse's email account. Emails are often a virtual treasure trove of information that can be extremely beneficial in a divorce case. Whether emails were obtained legally generally boils down to two factors: authorized access and expectation of privacy.

The Federal Law, known as the Electronic Communications Privacy Act of 1986 ("ECPA")[1] was enacted to prevent certain types of electronic eavesdropping. Congress enacted these laws in 1986 to update the Federal Wiretap Act of 1968. The original ban on wiretapping protected a person's privacy while using telephone lines. Clearly, the 1968 legislation did not envision the use of modes of communications such as email and text messaging. Since the ECPA was enacted, it has been amended to account for new technologies. The ECPA created both civil and criminal penalties for any person who intentionally (1) intercepts, uses or discloses any wire or oral communication by using any electronic, mechanical, or other device;[2] or (2) without authority accesses a wire or electronic communication while in storage.[3] An important distinction is made between the interception of electronic communications and access to communications that are in storage. The statute defines interception as the "aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device."[4] Electronic storage is defined as "any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission

thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.[5]

The ECPA applies to traditional telephone wiretaps, cordless telephone interceptions, electronic messages, voicemail systems, pagers, chat logs, web-streaming video, voice over IP, and recorded or videotaped private face-to-face conversations. Virginia has a similar statute regarding the interception of wire, electronic and oral communications[6] as well as unauthorized access to the storage of electronic information.[7] The central question in both the federal and Virginia statutes is authorization. The ECPA and Virginia statutes only prohibit "unauthorized" use, disclosure, or interception. Authorization tends to play a larger role in the accessing of stored information, for example, by reading a spouse's emails or text messages as opposed to intercepting communications, as it is rare for a spouse to authorize the tapping of his or her phone or computer.

In many cases, the parties share accounts, have the same passwords for all accounts or have told each other their passwords. If a spouse provides his or her spouse the password of an email account and allows him or her to use it, that person is authorized to access the account as he or she pleases. The courts typically decide the issue of consent on a case-by-case basis, and it is not necessary for the consent to be explicit. In fact, it rarely is. Implied consent can be found when the surrounding circumstances are taken into account. However, the water grows murkier in situations where a spouse, under limited circumstances, gives his or her spouse consent to access an account. For example, a wife gives her husband the password to her email account and tells him she's giving it to him so he can pay the phone bill which was emailed to her. Is that consent for the husband to read through every email in her account? Under Virginia law, the answer is unclear. However, the ECPA envisions this type of privacy intrusion by prohibiting not only the unauthorized access to stored communications, but by also prohibiting the access of stored communications by a person exceeding his authority.[8] As such, it would appear that the husband would be exceeding his authority in the scenario above.

These statutes do not only apply to email. If a spouse's smartphone is password-protected it is viewed in the same manner as a password-protected email account. If spouse husband gives his wife the password to his phone, and is aware that his wife routinely uses his phone to make calls and access apps, he has no expectation of privacy and his wife's "snooping" around his phone is impliedly authorized. On the other hand, if the spouse just happened to guess the password it is not authorized and that spouse would be in violation of the ECPA by looking through the phone. The ECPA and Virginia statutes also apply to social media such as Facebook, Twitter and even dating websites. In today's world of technology and social media, the ECPA is extremely wide-reaching.

There are also numerous ways spouses can actively intercept both oral and electronic communications. Spyware can easily be found and installed onto a smart phone or computer. Many programs, typically known as "keylogging spyware," can be secretly installed on a computer and it will literally keep track of every key that is pressed and all activity conducted on that computer. Similarly, there are numerous apps that can be secretly installed on a smartphone, which will monitor every phone call, text message, email, picture, etc., exchanged on the phone and send that information to a third party. All the while, the user of the phone has no idea that his or her privacy is being invaded.

In fact, a Pakistani man was recently indicted in the Eastern District of Virginia for allegedly conspiring to advertise and sell "StealthGenie," a spyware application that could monitor phone calls, texts, videos and other communications on mobile phones without detection. According to allegations in the indictment, the business plan for StealthGenie stated that the target population for the marketing of the app was "[s]pousal cheat: Husband/Wife of (sic) boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behavior or if they just want to monitor them." The testimonials on the StealthGenie website focused significantly on potential purchasers who did not have any ownership interest in the mobile phone to be monitored, including those suspecting a spouse or romantic partner of infidelity.[9]

Whether a spouse illegally intercepts electronic information or oral communications it is not going to help him or her in their divorce case but will expose him or her to potentially severe civil and criminal penalties. In Virginia, "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court…"[10]

Recording telephone calls

Another issue that often arises in family law matters is the recording of conversations. In my experience, this typically arises in one of two scenarios: (1) One party records a phone conversation between the parties; or (2) One party records a phone conversation between the other party and their child. Virginia is a one-party consent state and, therefore, there is nothing illegal about the first scenario. The second scenario, however, violates both Virginia law and the ECPA. The recordings obtained in either scenario are useless as it relates to a pending divorce case.

Under Virginia law, no recording of a telephone conversation is admissible: "in any civil proceeding unless (i) all parties to the conversation were aware the conversation was being recorded or (ii)

the portion of the recording to be admitted contains admissions that, if true, would constitute criminal conduct which is the basis for the civil action, and one of the parties was aware of the recording and the proceeding is not one for divorce, separate maintenance or annulment of marriage."[11]

As such, the only possible scenarios where I can imagine a recording would potentially be admissible in a domestic relations case is if one parent admits to criminally abusing a child and the case is purely a custody case (not part of a divorce action) or if a party admits to assault or makes threats that are going to be used as the basis to obtain a protective order.

Tracking a spouse using GPS

Due to the rapid expansion of technology, another issue that most family law attorneys are facing is a client's request to place GPS on his or her spouse's vehicle to monitor him or her. When a client suspects that his or her spouse is having an affair, it is obviously important to obtain proof of the affair for use in an eventual divorce case. To do this, a client may hire a private investigator who can install a GPS tracking device on to the suspected cheating spouse's vehicle. The client may also simply install one herself or simply hide a smart phone, most of which now have GPS tracking capabilities, in the trunk of the vehicle. However, it is currently illegal and a Class 3 Misdemeanor for a spouse to install, or have someone else install, a GPS tracking device on a vehicle, even if they own it.[12] However, the statute makes a specific exception for registered private investigators. Thus, the only legal way to track a spouse using a GPS on a vehicle is to hire a private investigator and have him or her install the GPS on a vehicle that a client owns.

Breaking into your own property

Perhaps the most blurry issue is breaking into a spouse's filing cabinet, safe, drawer or other secure area. Is it possible for someone to commit a crime by breaking into a drawer in a desk that they own, which is located in their house? Probably not. Most personal property has no official "title" which indicates ownership and most property located in the marital residence is presumed to be jointly owned. Therefore, it is very unlikely that a spouse will face any criminal charges for jimmying open a desk drawer or forcing open a safety deposit box and taking the contents. Unless the contents are property that is specifically solely titled in the other spouse's name, law enforcement generally defer to the civil courts to determine such issues.

Also a frequent occurrence in divorce cases is the situation where one spouse changes the locks on the marital residence, and therefore, the other spouse can only access the residence by breaking into it. As long as the residence is jointly titled, and absent a court order to the contrary, each spouse has an equal ownership and possessory interest in the property. As such, the spouse who has no option but to break into his or her residence has every legal right to do so. However, if one spouse is granted exclusive use and possession of the marital residence, whether through a pendente lite order or protective order, then all the above examples constitute criminal activity.

Attorney liability

An attorney can face just as much liability as his or her client who violates the ECPA. Under the ECPA and the Virginia statutes, if an attorney has obtained information that he or she was aware was obtained illegally and the attorney looks at or listens to it anyway, the attorney is equally liable and may face the same consequences as the client. There is no attorney immunity under the ECPA or Virginia statutes.[13] Attorneys found to have violated these laws have been criminally fined, placed on probation, lost their law license and ordered to pay civil fines. As such, when a client presents materials—including recordings, emails, text messages, etc.—that could in any way be covered by the ECPA or Virginia statutes, a prudent attorney will not look at or listen to the materials until he or she has sufficiently inquired into the methods used to obtain them and is assured that they were not obtained in violation of any federal or state laws.

Endnotes

1. 18 U.S.C. §§2510-2522 (2014)
2. 18 U.S.C. §2511(1)(a)
3. 18 U.S.C. §§2701 – 2711 (2014)
4. 18 U.S.C. §2510(4)
5. 18 U.S.C. §2510(17)
6. Va. Code §19.2-62
7. Va. Code §§18.2-152.4 – 152.5
8. 18 U.S.C. §2701(a)(2)
9. http://www.washingtonpost.com/business/technology/make-of-app-used-for-spying-indicted-in-virginia/2014/09/29/816b45b8-4805-11e4-a046-120a8a855cca_story.html
10. Va. Code §19.2-65
11. Va. Code §8.01-420.2
12. Va. Code §18.2-60.5
13. *See Wuliger*, 981 F.3d at 1507 (stating that "nothing in the [Ohio] code of [Professional Responsibility] 'authorizes' the defendant to violate Title III in carrying out his professional duties"); *Lewton v. Divingzzo*, 772 F. Supp. 2d 1046, 1057 (D. Neb. 2001) (stating that "the court was unable to find any binding authority holding that an attorney who uses a communication intercepted in violation of the federal Wiretap Act is entitled to blanket immunity from Title III liability") *Babb v. Eagleton*, 616 F. Supp. 2d 1195, 1207 (N.D. Okla. 2007) (stating that "First, attorney did not cite, the Court did not locate, any authority holding that an attorney who uses a communication intercepted in violation of Title III is entitled to some type of privilege or immunity from Title III liability.")

Jeremiah Yourth practices with Owen & Owens in Midlothian. He focuses his practice on family law, civil and commercial litigation, and employment law. He is a graduate of the University at Buffalo, State University of New York, and the Albany Law School. He is active in a number of bar associations, including VTLA, as well as community service groups. He was named a "Rising Star" in Virginia Super Lawyers, Family Law category, 2015.

www.owenowens.com