Boston Bar ASSOCIATION

ILLICIT SURVEILLANCE OF ELECTRONIC SYSTEMS IN FAMILY LAW CASES

The truth is stranger than fiction, especially when the stakes are high.

By Mark Spencer and Regina Hurley
Originally published in the Boston Bar Association Family Law Newsletter, March, 30, 2017

As society increasingly relies on electronic systems and their interconnectedness, the interest in monitoring these systems and their users also increases. While some monitoring of electronic systems (particularly in corporate environments) is considered perfectly legitimate by reasonable observers, other kinds of monitoring are more insidious and involve illicit[1] surveillance of those systems and, by extension, their users. To satisfy that demand, innumerable companies (not to mention underworld figures) build and sell tools which facilitate illicit surveillance.

Arsenal Consulting has performed digital forensics in many cases involving illicit surveillance, from family law disputes to attacks on financial institutions. We quantify such illicit surveillance using the six methods shown in Table 1, organized roughly by increasing sophistication. Of note, some of these methods involve the use of perfectly legitimate tools used in illegitimate ways. Arsenal has leveraged digital forensics to uncover illicit surveillance employing each of these six methods.

In our experience, family law cases are high-stakes affairs involving custodial and financial issues having significant ramifications even beyond the adversarial parties. Consequently, the temptation to employ illicit surveillance in a family law case may be particularly high. After all, the parties have often had physical access to, and know critical information about, each other's electronic systems. Sophisticated methods of illicit surveillance tend to be less relevant when physical access and critical information about electronic systems are readily available.

THE TEMPTATION TO EMPLOY ILLICIT SURVEILLANCE IN A FAMILY LAW CASE MAY BE PARTICULARLY HIGH.

More specifically, some of our family law cases have involved spouses logging into each other's webmail accounts,

Table 1: Six Methods Used to Quantify Illicit Surveillance

Method	Example
Knowledge	Usernames & passwords
Embedded Remote Access	Microsoft's Remote Desktop
Third-Party Remote Access	TeamViewer GmbH's TeamViewer
Commercial Monitoring	Awareness Technologies' WebWatcher
Remote Access Trojans	Prince Ali's Bandook
Nation State Interception	HackingTeam's Remote Control System

continuing synchronization[2] of devices in each other's custody, accessing each other's devices using remote access functionality embedded into the Microsoft Windows or Apple OS X operating systems, and installing commercial monitoring tools while physical access to devices remained available.

Arsenal worked on a particularly interesting family law case with Verrill Dana's Regina Hurley, Attorney Hurley explains:

The truth is stranger than fiction, especially when the stakes are high. The saying, "You can't make this stuff up" is spot on. Divorce cases by their nature are emotional, but when you combine emotion with a dispute over children and millions of dollars, anything can seem justified. Divorce attorneys hear and see it all, and many would agree that "Criminal law is bad people at their best, and divorce law is good people at their worst."

In divorce work, every case is different, and the key to effectively representing one's

client is understanding those differences and how they inform one's approach to the case. I frequently tell new attorneys I work with this: When you hear something from a client that sounds implausible, and especially when you hear it more than once, no matter how far-fetched it may seem, pay attention to what you hear. Don't dismiss it, don't ignore it. Listen to the client, ground them in the need for careful fact finding, gather all the facts you can, consider the range of possibilities, and follow the facts where they lead.

ALTHOUGH SEPARATED FROM HER HUSBAND FOR OVER A YEAR, SHE WAS CERTAIN HE WAS GAINING ACCESS TO HER EMAIL ACCOUNT.

Our client was the defendant in a bitter, hotly contested, very high-net-worth divorce. It was anything but a "cookie cutter" case. It fell into the gray area of fact-driven, medium-term, childless marriages. Good, strong, compelling arguments could be made on both sides of the "v", and because the amount of money at stake was enormous, it was destined for trial. Until, that is, we listened to our client.

Our client frequently expressed concern that, although separated from her husband for over a year, she was certain he was gaining access to her email account. She felt he was gaining this access despite her meticulous online "hygiene" habits which included maintaining a distinct email account for communicating with attorneys and regularly changing her usernames and passwords. She even had her computer examined by a computer specialist to see if anything suspicious was installed on it, and the specialist found nothing. Indeed, multiple "computer savvy" people she spoke with dismissed her ongoing worries about unauthorized access as unsubstantiated, telling her "You've had it examined and there's nothing there."

Then one afternoon, we received a panicked call from our client telling us that while she was flying across country - without access to her electronic devices - her email had been accessed. The client was able to substantiate this because she had recently learned that her email service offered the option to see the Internet Protocol ("IP") addresses of computers used to access her account. She used this option and saw an IP address other than her own had accessed her email account not only during the time she was in flight, but also a number of other times. On the Internet, an IP address functions like a phone number. Generally speaking, it is a series of numbers that at any particular time are unique to each device on the Internet. It is often possible to connect the use of an IP address to an organization and ultimately to an actual person. Many IP addresses are publicly associated with the organizations and people responsible for them, but to identify who was actually using them normally requires subpoenas to Internet service providers. Finally, using geolocation tools with an IP address, it may be possible to triangulate the physical location of a device when it was assigned that address.

Again, rule one, when you hear the implausible, don't dismiss it – ground it in facts and follow the facts where they lead you. The client came to our offices shortly thereafter and showed us the feature of her email service that allowed her to identify those IP addresses which had accessed her account. As a quick test, we compiled a list of all the IP addresses that had accessed the client's email account during a specific time frame and then handed the list to our firm's IT Group. Our IT Group took the list and performed some background research on the IP addresses, which included geolocation.

RULE ONE, WHEN YOU HEAR THE IMPLAUSIBLE, DON'T DISMISS IT – GROUND IT IN FACTS AND FOLLOW THE FACTS WHERE THEY LEAD YOU.

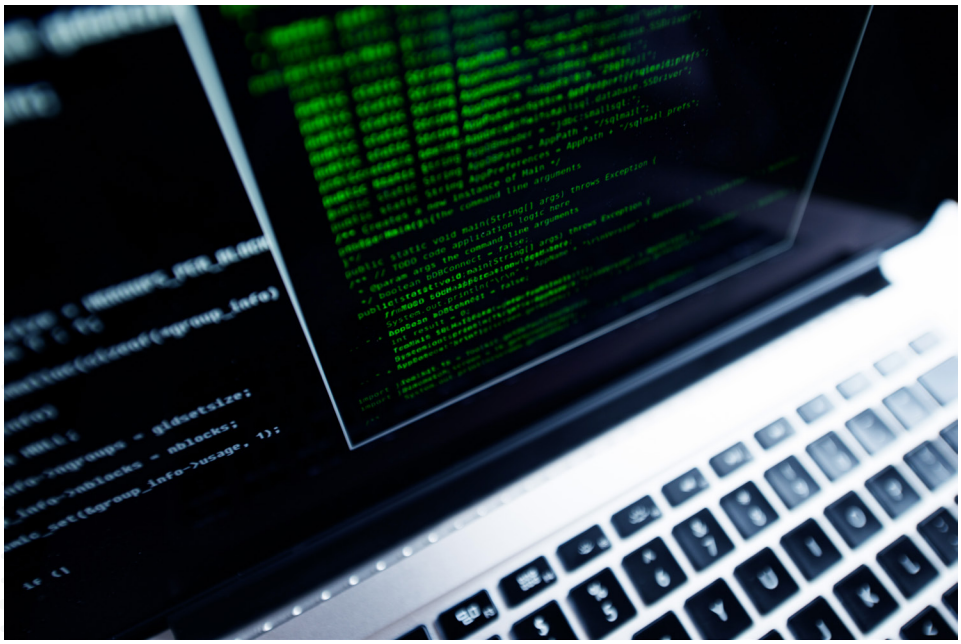
The phone rang. It was our IT Group.

Were we familiar with the law firm, ABC? Were we familiar with Company XYZ? And was there any connection between the client and a certain overseas location? The answer to all three questions was a bone-chilling, yes. ABC was the law firm representing our client's husband[3], XYZ was a company with whom the client's spouse was currently working, and the overseas location was where the client's spouse spent time in the winter.

Clearly, it was now time to call in the experts. Our next call was to Arsenal, to whom we immediately delivered our client's primary computer. Not long after it was delivered, the phone rang again. It was Arsenal: "Tell your client to stop using all of her devices immediately, and call us right back." Our hearts skipped a beat. Following a call to our client, we called Arsenal back. Arsenal explained the seriousness of their findings. They had uncovered a very powerful spyware installed on our client's computer. The spyware itself allowed remote monitoring of everything she did on her computer - every keystroke entered, emails drafted, sent, and received, documents read, websites visited, usernames and passwords created and updated, and more. The user of the

"TELL YOUR CLIENT TO STOP USING ALL OF HER DEVICES IMMEDIATELY, AND CALL US RIGHT BACK."

spyware had access to virtually all of our client's communications with everyone she corresponded via the computer, including her attorneys and various consultants. The spyware user had access to all the privileged, confidential and sensitive documents and reports we shared with her. Equally troubling, we learned that the spyware was insidious and very hard to detect. It was designed to "bury" itself in a computer in a way that allowed it to go undetected. By the time it was located in our client's computer, the spyware had been installed and operating for over a year – the potential damage to our client was staggering.



Using a detailed and readily defensible chain-of-custody protocol, we arranged for transfer of all our client's remaining devices to Arsenal for evaluation, including forensic imaging and analysis of all her computer hard drives.

Was this really possible? We had a collective 80 years of legal experience among us, but none of us had ever seen, or heard of anything like this. Was this a bad divorce, or a John le Carré novel? As the facts unfolded, it turned out it to be a bit of both, with a very high tech twist.

We had more work to do. While we had a solid factual basis to suspect that the client's spouse was the user of the spyware, we needed evidence directly connecting him to it. First stop, the courthouse. Armed with objective evidence of the connection between the IP addresses that had accessed the client's email account and her spouse, and armed with Arsenal's objective evidence that powerful spyware had been installed on the client's computer allowing

WAS THIS REALLY POSSIBLE? WE HAD A COLLECTIVE 80 YEARS OF LEGAL EXPERIENCE AMONG US, BUT NONE OF US HAD EVER SEEN, OR HEARD OF ANYTHING LIKE THIS.

monitoring of the client's interaction with email, documents, usernames and passwords, and essentially everything else on her computer, we went to court and asked for an emergency order. We sought an order requiring the client's spouse to surrender all his devices, (desktops, laptops, tablets, smartphones) whether from his home, work, cars, planes, trains, or boats, so that an expert could obtain forensic images from all those devices. We argued that if the spouse were notified of our request for this order in advance, he may alter or destroy the very evidence we sought.

The court was initially reluctant to enter such a broad, sweeping order, until the judge saw the objective evidence of (1) the IP addresses that had accessed the client's email account, including those from the guest WiFi system of the spouse's lawyer's offices on a date and time when the spouse was verifiably at his lawyers' offices; (2) the IP address originating with an organization with connections to the husband; and (3)

Arsenal's evidence of the powerful capacity of the surreptitiously installed spyware.

Persuaded of the emergency nature of the relief sought, the court issued an order requiring the immediate surrender of all the husband's devices, and then scheduled a hearing for the next business day, a Monday. The court also ordered the spouse not to remove any information from the computer or to make copies of the illicitly captured information.

That Monday, all parties arrived at court but never actually appeared before the judge, agreeing instead that the husband would surrender all his devices to a neutral computer forensics consultant for the purpose of creating inviolate forensic images of all his devices.

At the same time, we served a subpoena on the spyware manufacturer demanding all records relating to the purchase and use of the product identified on the client's computer. The manufacturer immediately complied with the subpoena. Their records showed that over two and one half years the husband and a third party closely associated with him (the "cohort") purchased numerous copies of the spyware, back-up CDs (shipped to both their residences), and some 80,000 "snapshots" to capture what our client was viewing. In addition, the records provided the following details:

- *The spouse's name*
- *The cohort's name*
- *Transaction dates*
- *Billing addresses (two were husband's, one was his cohort's)*
- *Shipping addresses (again, two belonging to the husband and another to the cohort)*
- *The husband's phone number*
- *The husband's email address*
- *The last four digits of the spouse's VISA card, demonstrably used to purchase the spyware*
- *The last four digits of the cohort's VISA card number, also used to purchase the spyware*

Following receipt of these records, preservation letters were served on Microsoft, Apple, Comcast, Verizon, and others directing them to preserve all potentially relevant evidence. Next, we held a meeting with the husband's attorney to discuss a protocol for examining the husband's computers and to address the staggering intrusion into our client's electronic records and privacy. Once counsel saw evidence from the manufacturer of the spyware, the discussion immediately shifted to potential resolution of the case and how to set appropriate protocols for preventing further dissemination of or intrusion upon the wife's personal security information and data. The case settled shortly thereafter on terms favorable to our client, including payment of her attorney's and expert's fees. In addition, all the husband's devices were securely destroyed.

Many things can be done to better secure oneself from illicit surveillance. See Table 2 for some basic recommendations from Arsenal that may prove to be particularly important when familial disputes arise. It certainly does not hurt to have a technical expert with whom you can discuss these recommendations. Also, a helpful Digital Spring Cleaning Checklist is available from StaySafeOnline at **https://staysafeonline.org/stay-safe-online/resources/digital-spring-cleaning-checklist**. and more-detailed information is available from the Electronic Frontier Foundation's Surveillance Self-Defense website at **https://ssd.eff.org**.

MANY THINGS CAN BE DONE TO BETTER SECURE ONESELF FROM ILLICIT SURVEILLANCE.

If someone suspects that he or she has been the victim of illicit surveillance, we recommend that they contact an attorney immediately. The attorney can then build and execute a game plan with a digital forensics expert to make sure devices, accounts, and records[4] that may be relevant to any immediate issues (as well as ongoing or potential litigation) are preserved and analyzed.

Table 2: Eight Tips from Arsenal to Better Secure Yourself

What can you do to better secure yourself from illicit surveillance?
Audit and control both physical and remote access to electronic devices
Reassess synchronization of your devices and across accounts
Review and revise social media settings related to sharing and privacy
Update firmware, operating systems, and applications
Enable multifactor authentication everywhere possible
Utilize anti-virus software and maximize its value with aggressive settings
Improve password management (cease sharing with others, don't reuse or recycle)
Educate family members about these recommendations and overall safe computing

ABOUT THE AUTHORS

Mark Spencer is President of Arsenal Consulting, where he leads engagements involving digital forensics for law firms, corporations, and government agencies. Mark is also President of Arsenal Recon, where he guides development of digital forensics tools. Mark has more than 15 years of law-enforcement and private-sector digital forensics experience. He has led the Arsenal team on many high-profile and high-stakes cases, from allegations of intellectual property theft and evidence spoliation to support of foreign terrorist organizations and military coup planning. Arsenal is headquartered just outside Boston, Massachusetts and has an office in the Wan Chai district of Hong Kong. ArsenalExperts.com

ARSENAL CONSULTING
— ARM YOURSELF —

Regina M. Hurley is a partner in the law firm of Verrill Dana, LLP where she heads the Family Law Practice Group, comprised of 11 attorneys, 2 paraprofessionals, and 4 specialized staff members. Regina's practice concentrates in complex, high net worth family law matters, in particular those involving international issues, such as jurisdictional disputes, disputes concerning the validity of foreign marriages and/or divorces, Islamic marriage contracts, removal of children, and international parental abduction (both Hague and non-Hague Convention cases). Regina also devotes significant time to non-international cases involving complex custody issues, the identification, valuation, and division of complex income, business interests, and assets, and most recently, cases involving computer intrusion and forensic examination and computer-related discovery. Regina is past President of the Massachusetts Family and Probate Court American Inn of Court. She was admitted to the Massachusetts Bar in 1986. Regina holds a J.D. (Common Law) from Tulane University (1986); an M.Sc. in International Relations from the London School of Economics and Political Science (1982); and a B.A. in History from the University of Massachusetts at Amherst (1981). Regina has been a frequent presenter at continuing legal education programs. She is AV Rated by Martindale Hubbell, was selected for inclusion in the Best Lawyers of America 2017; and was a Massachusetts Lawyers Weekly 2013 Top Women of Law honoree. Verrilldana.com

Verrill Dana LLP
Attorneys at Law

---

[1]Of course, the illicit nature of surveillance is debatable depending on both context of the particular case and which end of the surveillance one finds themselves on.

[2]For example, Apple's iCloud may have been configured across a family's devices prior to a family law dispute and not disabled in a timely fashion after a dispute has arisen.

[3]The law firm was not involved in the access. While at the firm, the husband had used their guest WiFi system.

[4]Which may only be available via a court order.