



THE Connection

Official Newsletter of the Georgia Association of Professional Private Investigators, Inc.

UPCOMING MEETINGS

The Next
GAPPI Atlanta
Chapter Meeting
January 11, 2010
at Ryan's Restaurant
705 Jimmy Carter Blvd.
Norcross
(770) 840-9096

Networking and lunch from
11:30 a.m.—12:00 noon
Meeting from
12:00 noon—1 p.m.

The cost is \$15.00 for GAPPI
members

\$20 for non-members
(includes lunch and beverage)

Students and potential members are
always welcome.

"We look forward to seeing
you all there!"

Data Security Basics for the Private Investigator By Jeff Kimble, P.I.

How's this for a bad day at the office: You've worked your heart out for years building your small [private investigator](#) agency. The business has grown to include yourself, your partner, a full-time secretary, and a few part-time operatives to help out with the more complicated cases. Nothing fancy yet, but you have big plans. You've survived the first three years—actually made a modest profit—and you've managed to keep afloat in the worst economic downturn since the Great Depression.

You arrive at work Monday morning, park your car, and walk to your building with the usual thoughts of cases, clients, bills, etc., floating hazily through your mind. As you step through the front door, you're snapped to frantic alertness by your secretary, who is crying openly about missing files, a stolen laptop, and what essentially amounts to a devastating tsunami in the cyber world: a *data breach*. Your heart sinks, and you face the possibility that your business may now be sunk as well.

It's a disturbing fact that within the last five years alone, over a half a *billion* sensitive data records, the majority of which included Social Security numbers and credit card information, were breached in this country, and nearly a quarter of those breaches occurred in small businesses. The final kick in the groin is that approximately three quarters of those small businesses went bankrupt either directly or indirectly due to the experience. Ouch.

But don't board up the office and start selling your precious bodily fluids to put food on the table just yet. There is hope for the small private investigative agency to secure its parapets, reinforce its ramparts, and generally keep the data-thieving barbarians at bay without sacrificing an arm and a leg in the process. Here are a few pointers to get things on the right track:

Figure Out What You Got and Where You Got It. Make a list of where the sensitive information is, who has access to it, and what's the most important and least important, as in, "If this were stolen, we'd be screwed, but if this got snatched, no one would care . . ." Prioritize and categorize. What's in the laptops? What's in the main office computers? The exterior hard drives? The USB storage devices? The file cabinets? The boxes of documents that you should have shredded years ago but just stuck in the basement to get them out of the way? Write it all down and organize it in a way that gives you the full picture of your vulnerabilities and strengths in terms of what someone could get and how could they get it, e.g., over the Internet, through a window, via grand theft auto, or by seducing your secretary. Once you've got the facts down on paper, you can begin planning your defense.

(Continued on page 2)

2010 Officers

President
Roy Wilkinson

Vice President
Pamela Griggs

Secretary
Ted Viator

Treasurer
Harriet Gold

Board Members:

Willis Craig
Michael Barker

Create a Solid Company Policy on Data Transport, Storage, and Personal Use. *FACE-BOOK!* Need I say more? Tighten the lid on all data in and out of the office and do so by making it clear to your employees exactly what you expect of them. You'd be surprised—or you may not if you're a working P.I.—what spills out of office doors through social networking and the like. Corral all those loose USB storage devices that you listed on paper that are currently floating around in purses, pockets, and laptop cases. Find out what's on them, who uses them, and what their physical proximity is at any given time. Inventory them, decide how you want your employees to treat them (do they go home at night, get locked in the safe, or what?). Drill hacker defense tactics into your subordinates as if you were General Patton: "If your computer ever appears compromised, yank all the plugs like s**t through a goose!" (I actually heard of a secretary trying to reach her boss on the phone for half an hour in order to tell him that the main computer was acting funny. Meanwhile, the hackers drained every ounce of information via a corrupted Internet connection while she sat there doing her nails.)

Upgrade everyone's computer security software to the best you can afford. Increase password complexity and discourage employees from writing them down. Limit or forbid Internet use on certain extra-sensitive computers. Limit or forbid the "take-home" computers and the information on them. Insist that "take-homes" be transported in a locked trunk and that any sensitive information in them is encrypted. Forbid all employees from receiving or transmitting company info over public Wi-Fi hot spots. Shred sensitive printed documents destined for disposal ASAP, and be sure to use a diamond cross-cut shredder. If you really want to do the "Liddy/Magruder Midnight Shuffle" the superlative way, burn them too.

Completely destroy—not just "erase"—all decommissioned computer hard drives. Never let an employee sell or discard a PC/laptop that was used for agency work even if it was their own personal property—make it part of your pre-employment agreement. Give that old computer a taste of *Office Space* stress-relief in an open field with a baseball bat to make sure sensitive information permanently stored on the hard drive is completely obliterated and can therefore never fall into the wrong hands. If that seems too unprofessional and/or politically incorrect, turn the thing over to a trusted—emphasis on *trusted*—computer expert to dispose of it humanely.

Know Your Employees Like Family. If you can, *keep it in the family!* Our office *is* family: My partner is my wife, my secretary is our unofficially adopted daughter whom we raised as our own since she was a teenager, and most of our licensed operatives are blood relatives. Not everyone is so lucky in their business, but I can't tell you how much better you'll sleep if you have complete trust and confidence in your employees. If you don't have the luxury of literally keeping it in the family, perform thorough background checks on all potential hires. Sounds obvious, right, especially for private investigators? But I've known agencies that will hand out associate P.I. licenses to anyone with a Social Security card and a smile.

First get to know your applicants personally. Go out to dinner a few times, make lots of small talk to get information, take them to a ballgame and ask them to bring *their* family or friends—birds of a feather, so to speak. Better to dig deeply into their lives and find out who they *really* are than be forced to dig the proverbial knife out of your back when they sell you up the creek. You're a detective—detect! Don't take on anyone you wouldn't trust with your own children, because ultimately you're putting your own children at risk, i.e., your livelihood and ergo theirs. Don't make the potentially fatal mistake of hiring some yo-yo who ap-

pears solid in his or her resume and demeanor, but later turns out to be Robert Hanssen incarnate.

Were You Born in a Barn? This is really basic stuff, but you'd be horrified to learn how many agencies have little or no physical security and yet handle extremely sensitive data on a daily basis. Keep sensitive areas locked, and install deadbolts on all interoffice doors to better secure them from illegal entry. Lock file cabinets whenever possible. Give keys to only your most trusted personnel. Your best overall strategy is to improve your physical security in increments in proportion to your budget. Start by thinking like a burglar. Then, a little bit each week, make your workplace less appealing to the potential data thief by making it harder and harder to break in. No physical security is foolproof, but determination to make a breach as difficult as possible should be a no-brainer. Motion detectors and cameras are great if you can afford them, but a living, breathing, security-minded human presence combined with solid locks and barriers are always your best bet to deter a data breach before it happens, or at least slow the bastards down so police have a better chance of catching them in the act if it's an after-hours B&E.

Hire Somebody. Consider outsourcing security or hiring a consultant. It's likely that a qualified security service can provide better security than you can. Plus, it allows you and your staff to concentrate on the business of private investigations rather than locksmithing, alarm systems, and the complicated minutiae of modern data storage. But can you afford it? Can you afford not to? Only you can answer these questions.

My advice in all things is to do *what* you can *when* you can, and don't sweat the rest. And remember, it's much more expensive for you and your business to repair a data breach *after* it's occurred than it is to prevent one from ever happening in the first place. Lao Tzu said, "All difficult things have their origin in that which is easy, and great things in that which is small." Apply that thought to your agency's data security, along with the pointers above, and you shall go far, young Grasshopper.

Jeff Kimble is a frequent guest writer for PInow.com, which is a nationwide trusted network of private investigators. He is a licensed private investigator and co-owner of Arizona Legal Document Services LLC in Arizona. Visit www.PInow.com to learn more.

CyForensics, LLC[®]
GA License #PDC002282
www.cyforensics.com
info@cyforensics.com

(478) 731-0752



Louis M. Schlesinger, MMIS, LPI
CCE, CIFI, CFC, ACE, WCSI
Member: ISFCE, IISFA, ACFEI, GAPPI, ISPAG
GA Lic. #PDE047590



Computer Forensics Investigations / Data Recovery
Password Recovery / Expert Testimony

Follow that Car: 10 Mobile Surveillance Tips for Private Investigators

By Scott B. Fulmer

Texas [private investigator](#) and current TALI President Kelly E. Riddle wrote an excellent surveillance book years ago titled *The Art of Surveillance*. Mr. Riddle was correct. Mobile surveillance is indeed an art form. There's an exception to every rule. Much of it depends on traffic flow, location and the time of day. The following 10 tips will help you conduct a successful mobile surveillance.

1. **We have Ignition!** The timing of your initial departure from a stationary position to a mobile or rolling surveillance behind the subject is critical. The tendency is to either begin following too soon (and get burned) or to hesitate (and lose the subject.) You have to allow the subject a short amount of time to drive off. Following too quickly or closely at the outset will make the subject notice you. Later on when you're miles down the road and still behind them they'll wonder why the same vehicle from their neighborhood (yours) is still behind them. Let the subject get down the block before you ease into traffic.

2. **Follow that car! (But not too closely)** The distance you maintain between your surveillance vehicle and the vehicle you are following during a mobile surveillance is dictated by the amount of traffic on the road and your environment. For example, during rush hour on a busy street or highway you should maintain no more than one car between you and the subject. In rural areas you can allow a greater distance between you and the subject. This is all very relative. The more congested the traffic, the closer you need to be to the subject. Make sure you keep an eye on the subject's vehicle and use your peripheral vision for everything else. Find something unique about the subject's vehicle such as a bumper sticker, brake light pattern, spoiler, etc., and keep your eyes glued.

3. **Choke Points:** During a mobile surveillance keep your eyes focused on the subject's vehicle and the traffic ahead of them. This will allow you plenty of time to determine the best course of action. Major intersections, highway intersections, bridges, toll roads, etc., are all choke points. Be alert for these types of areas. You'll have to decrease the distance between you and the subject's vehicle until you get through these choke points. If you fail to do so they will breeze through a green light and you'll be cooling your jets at a red light as they slip away.

4. **Double traffic lights:** Beware of streets having two sets of traffic lights on the same block, one right after another in very close proximity. It's like that old Tennessee Ernie Ford song *16 Tons* about the guy with two fists of steel: "If the right one don't get you ... then the left one will." When following someone through double traffic lights keep your eyes on the second set of traffic lights. Those are the lights you have to stay ahead of. If you're not alert the subject will make it through and you'll get stuck.

www.revealaudio.com/audioenhancement



Is your sound recording "at a loss for words?"

Audio enhancement, speech extraction, noise reduction
from video, microcassette, analog and digital sources.

Over seven years' experience working with
PI's, attorneys, individuals, and law enforcement agencies.

David Leonard

david@revealaudio.com

770.928.1955

5. Right Turns and Left Turns: When the subject turns right at an intersection you should speed up to that intersection. Once at the corner quickly decrease your speed and slowly turn right. Burning rubber around a right turn will cause the subject to look in his rear-view mirror and notice you. Double left turns can present a minor challenge. If the subject is in the right-hand lane of a double left turn he could be turning left or going straight. You usually have no choice but to pull up behind him in the same lane or you risk losing him at this choke point.

6. Sunday Drivers: Slow or “Sunday” drivers magically appear out of nowhere to torment you as soon as your mobile surveillance begins. Do not sit and think about whether you should pass them or whether they will eventually speed up: you should because they won’t. Don’t hesitate. Pass them right away. Get around them quickly or you’ll lose your subject. It’s that simple.

7. It Tolls for Thee: Be aware of all toll roads, turnpikes and other private or publicly built roads in your surveillance area that require a fee for usage. More importantly, consider whether or not your subject will take the toll road and blow through with an EZ tag like someone I recently followed in Houston. Maybe your subject will stop and pay the fee at each toll booth. Either way you have to be prepared with an EZ tag or plenty of coins. I’d have both on hand. If you operate in Dallas, Houston or other big cities that have toll roads you would do well to purchase an EZ tag.

8. Free Parking: One of the more difficult aspects of a mobile surveillance is the fact that you generally do not know where the subject is going. When it comes to clients, *video is everything*. As the subject arrives at his destination you have to immediately determine where they will park and at the same time scout out a suitable surveillance position for you. Do this quickly and you will be able to get video of the subject walking in. Handicap-accessible parking spaces and other reserved spots are usually up front in prime locations and allow for excellent opportunities to videotape. I am not suggesting you break the law by parking there, but using these parking spaces, if only for a few minutes, will allow you to secure good, close, solid video of your subject as they walk into a place of business. Once they’re in you can relocate to another parking space to videotape them walking back to their vehicle. You have to do what you have to do to secure video. There are no excuses. Clients have no understanding of how difficult our job can be.

9. The Sun is Not Your Friend: As I mentioned in tip #8, when you follow a subject to their destination you must quickly park and set up your surveillance vehicle to acquire videotape as they walk in. As you do so, remember the sun is not your friend. Videotaping against the sun will wash out the video and reflect off your windows, giving you poor-quality video. Along with everything else going through your mind as you get the subject to their destination, don’t forget to set up your surveillance vehicle so that the sun is behind you as you videotape.

10. Taking Notes on the Go! It is difficult to try to accurately write down every detail of a subject’s activity during the middle of a mobile surveillance. Although there are periods when you can reach for pen and paper and update your notes, more often than not things are happening too quickly to do so. It is also best not to simply rely upon your memory. Remember: you’re gathering evidence and what you write may end up being read back to you in court one day. It has to be factual. A simple solution is to verbally dictate the subject’s activities into a digital recorder during the mobile surveillance and then use these audio files to complete your notes once the surveillance has ended.

As I said earlier, surveillance is an art form. It takes patience and a keen understanding of human nature. The reality is much of it is learned through trial and error; what works and what doesn’t work. Adding these 10 techniques to your surveillance tool kit will improve your odds of having a successful surveillance. Good luck! Send me a quick e-mail if you have any questions about mobile surveillance.

If you liked these tips, read Scott B. Fulmer’s articles on [successful surveillance](#) and [interviewing techniques](#).

Scott B. Fulmer is a private investigator, speaker and president and CEO of Scott B. Fulmer Investigations, LLC based in San Antonio, Texas. He is a frequent contributor to PInow.com, which is a trusted nationwide network of private investigators. Visit www.PInow.com for more information.

Annual Financial Report for GAPPI

As we close out the year we are proud to announce that GAPPI is financially sound. We have seen the membership grow and had very good turn-outs for the Spring Training and the SEIC Fall Conference. This has allowed the Association to accrue a one year's operating capital which runs about \$35,000 annually. This was one of the goals assigned to the Board of Directors in order to provide financial stability for GAPPI. As we closed out the profit and loss statement for November, GAPPI showed a net income of just over \$9,000. Our projected year end numbers should come in pretty close to this same amount.

The Board of Director's next priority is to be more proactive legislatively. There were issues last year that caused a lot of concern to our members and could have adversely affected your livelihood and these issues will be back to haunt us again in the 2011 State Legislative Session which starts in January. The cost of legislative advocacy is more than what the basic GAPPI budget can handle and we will be asking for voluntary donations on the dues renewals invoice to help fund GAPPI's legislative efforts. We know these are tough times and the Board did not want to see an increase in dues in order to cover these additional costs. Please give what you can to help us protect our industry. If you can't donate right now please consider giving of your time to talk to our State Legislators so that they will be better educated on issues that affect Private Investigators.

If you have any questions please give me call at 404-766-1632 or you can e-mail me at vernon@ahqi.com.

Vernon Thomas
Executive Director, GAPPI

Advertise in The Connection!

Business Card—Approximate size: 3.5" x 2"
\$10 per issue or \$100 per year
(11 issues)

Quarter Page—Approximate size: 3.5" x 4.5"
\$25 per issue or \$250 per year
(11 issues)

Half Page—Approximate size: 7.5" x 4.5"
\$50 per issue or \$500 per year
(11 issues)

Full Page—Approximate size: 7.5" x 10"
\$100 per issue or \$1,000 per year
(11 issues)

For more information, contact us at:
vernon@ahqi.com / 404-766-1632

The Connection is published 11 times a year (monthly, Nov/Dec issue is combined) by the Georgia Association of Professional Private Investigators, Inc. (GAPPI). The staff of *The Connection* reserves the right to review and edit articles, advertisements, or other writings that are submitted for inclusion in this newsletter. The writer may contact *The Connection* Editor to request an exception to this policy. Articles printed in the newsletter may not necessarily reflect the views of GAPPI officers or members, and GAPPI does not necessarily endorse any product or service advertised in the newsletter. Contact GAPPI at Vernon@ahqi.com, 404-766-1632 for advertising information or notification of change of address, phone or e-mail.