



Support Your Provincial Private Investigator Association

Inside this issue:

Support Your Provincial Private Investigator Association	1
The Lure of the Internet	2-5
Password Protection & Computer Encryption	6
News Stories and Publications of Interest	6
Evaluating One-On-One Allegations	7-9
Military Rations For PI's and Protection Agents?	10
Contact Information	11

Not all the provinces and territories in Canada have private investigator associations. Of the ones that do exist, some struggle to grow due to lack of support from permit holding private investigators that either do not join, or do not renew their memberships. By supporting these associations you become part of a bigger picture. There is power in numbers. Whenever the government wants to implement new laws that directly or indirectly affect the private investigation field, your association will be on the frontlines, battling for you and your livelihood.

Here's a list of Canadian Private Investigators association websites:

Alberta Association of Private Investigators

<http://www.alberta-investigators.org/>

Private Investigators association of British Columbia

<http://www.piabc.ca/>

Council of Private Investigators Manitoba

<http://www.cpi-manitoba.com/>

Council of Private Investigators - Ontario

<http://www.cpi-ontario.ca/>

Professional Association of Quebec Private Investigators

<http://www.apepq.org>

Canadian Association of Private Investigators

<http://www.capicanada.ca/>

The lure of the internet

by Diane Walsh

Can't say I am the only one stunned by the number of complaints that have recently emerged in the press on the government's growing infringement of privacy for ordinary Canadians. Particularly on E-media there has been an outpouring of criticism of the Harper government modus operandus with attacks focused on conservatives allegedly complicit in a booming 'US spy-wagon'.

This recent outcry is coming from traditionally left-of-centre outlets e.g. www.nupge.ca/news_2007/n21oc07b.htm who, for the most, not so surprisingly, hone in on risks to Canadian social rights - as first priority. However there's no doubt, other private-enterprise stakeholders are beginning to get just as concerned.

In a January 18th, 2008 statement, the Greens alarmed Canadians suggesting that the FBI's international database raises privacy concerns - Press Secretary Labchuck pointed to: concern over the potential loss of privacy with the United States' proposed international database dubbed the 'Server in the Sky'. Going on to say,

"The project, which would allow the international exchange of biometric information, could result in a significant loss of personal privacy for Canadian citizens and should be subject to Parliamentary approval. FBI has been speaking with the RCMP regarding the establishment of an international database that would allow personal information such as fingerprints, DNA and eye scans to be easily exchanged between the US, Canada, the UK, Australia, and New Zealand. It is estimated that the database would hold personal information from millions of people".

Party Leader Elizabeth May warns publicly that measures taken toward enhancing public safety, however, must always be balanced with the Canadian values of personal privacy and freedom as enshrined in the Charter of Rights and Freedoms.

Private investigators, in particular, have a burden of responsibility to be acutely aware of a changing ethical landscape - what we've all understood to be Charter-protected privacy rights is changing.

It is true that traditionally in Canada it has been accepted that if people are to be videotaped they can't also be audio-taped (that is video-recorded and heard, talking, at the same time as it were) - this is not so anymore with the proliferation of cross-border government-legitimated clandestine investigations. We need to look at what part or role, if any, private investigators play in this new wave. What was once a formerly-understood careful practice of private investigating is gradually eroding - a rule in the midst of change. This is due in part to an E-market's quick-proliferating internet and software inventions e.g. www.actapress.com/PaperInfo.aspx?PaperID=28627&reason=500 - which represent insidious "recording" opportunities some citizens have complained are being used to invade wrongfully into ordinary people's lives - under the guise of government, police and associates allegedly doing "their 'job' to protect society" .

We're at a point in Canadian life where on the one hand many citizens agree we are gradually gaining greater access to historically-held "secret" government information, while at the same time, private life, as we know it, is being infringed upon without our knowledge. Increasing it's the state claiming it needs more protection for itself in order to protect its citizens. Indeed a slippery slope!

Concerns over privacy are being aired regularly on watchdog blogs and e-publications.

This list may prove useful to PI's in shaping best-practices for the future:

Canada still ranked high in terms of a country that protects privacy but this privacy landscape is changing radically as we speak. Visit:

www.eu-digest.com/labels/Citizens%20Privacy%20Rights.html and

www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597 out of interest.

It is true that PI's can play a role in not being complicit in cross-border government inquiries that infringe on Canadian rules, using the excuse that the "the US authorities are bullying us to do so". Importantly PI's must have central resource where they can compare notes and band-together so that they are not exploited by technologically-advanced neo-fascist ways of governing. In other words – not just chase business ops and the dollar but participate in the shaping of best professional practices.

www.lundboats.com/privacy_ca.html is in my view a mildly suspicious website (e.g. containing references to a US address, yet also displaying the Canadian flag). This could be cited as an example, also to demonstrate an increasing blurring of Canadian national boundary and distinction between US and Canadian privacy laws.

www.canada.com/ottawacitizen/news/business/story.html?id=21e669c9-5f1d-45f8-ae0f-f6e56884070f&k=20706 touches on the issue of home TV recording and passing info over the internet, outlining, in part, the uncontrollable effect of internet technology in the hands of the many. This is not to suggest it shouldn't be this way, but rather a citing of the sheer complexity of privacy protection legality as we move into the future.

www.referenceforbusiness.com/small/Di-Eq/Employee-Privacy.html shows employee privacy is not protected – this is clear when employers under the direction of PI's look into their staff's computers due to a leak from somewhere that he/she should be a target of inquiry albeit it can be said that some national unions are beginning to look into this employer-freedom more scrupulously.

www.p2pnet.net/story/14197 shows how experts in e-commerce and the Law are beginning to salivate at the mouth with some of these changes occurring, requiring their input and direction; hence money in their pockets.

www.privacyjournal.net/newsletter.htm is an example of a resource of citizens speaking-out about the surveillance controversies.

www.cippic.ca/public-video-surveillance/ looks at Canadian internet policy – indeed a very complex and challenging issue for government which on the one hand ensures citizens that e.g. medical records are protected and on the other hand does nothing to fund inquiries into wide-spread hacking.

www.anonequity.org/weblog/archives/2007/01/citizen_journalism_and_privacy.php represents another example of citizen journalism and blogging culture which is having little effect on protecting privacy in any concrete way – in fact websites can be part of the problem i.e. the double edged sword of promoting info over the net.

www.infosource.gc.ca/common/help/help-aide_e.asp is a fairly inadequate site on Canada's privacy act which does little to outline the most recent issues around surveillance and US gradual co-opting of our historically-held privacy notions.

www.citizen.org/campaigns/articles.cfm?ID=12350 is a US resource called, Public Citizen which may help to fill in the gap on some the cross border issues needing to be addressed in this context of Canadian activism.

In addition to some of the discussions in the aforementioned sites, the following story may shed more light on some of the concerns I've raised:

A small business owner subscribed to the innovative VOIP (Voice-over-Internet-Protocol) system that he'd understood had credibility in the telecommunication market worldwide. Enthusiastically he opened his account in one of the newest VOIP businesses, using his real company name and proceeding to apply for one (1) core telephone line with an option of two (2) secondary lines. Not long after John Doe Ltd. opened his telephone account he began to get repeated telemarketing phone calls from the telephone number: 402-930-3659 (found later to be out of Omaha, Nebraska) – based on the short conversation between the caller and Doe, it became clear to Does that the woman at the other end of the telephone line knew not only Doe's company name, his main telephone number, but worse, still she knew the secondary numbers associated with his core account.

Absolutely, frightening? - one could assume, fairly reasonably but not necessarily accurately, that one of the ways the caller could have come to know this 'private' information was John Doe's beloved telephone company gave or sold the information to her; and/or she, herself, is associated knowingly or unknowingly with people who infiltrate accounts manipulating their way into private profiles, retrieving not only full business names but any corresponding numbers associated with a private account.

It should be noted, VOIP numbers are not listed with 411 or the telephone directory.

But indeed they are getting into the wrong hands.

It may be more likely that the Doe Company # was obtained from servers programmed to comb through IP addresses rather than the VOIP company releasing/leaking information. This is the process that produces scam emails promising money etc. or selling pills - those emails are always from difficult to trace sending addresses - usually out of the country.

Those emailers have discovered details about the subjects and addresses on an email account enabling them to write to the target account. It's all done automatically, computer to computer. The same may be true in calling Doe Company's number.

Perhaps nobody will have called his VOIP telephone carrier. The information has more likely I expect been gathered by a computer looking at information that is being carried over the internet - remember it's called Voice over INTERNET protocol. It's the internet that is 'leaky'.

This article is: food for thought.

About the Author

Diane Walsh, MA, is an independent investigative reporter, born in Montreal. She has owned her own media group company since 1995 Geode Media Ink Tech Inc. and has been a watchdog of both industry and government. She recently graduated with a diploma in private investigation (2007). Contact: geode@shaw.ca

New Stories and Publications of Interest that you'll find in our Resource Centre

- The necessity of HUMINT
- Canada's Foreign Affairs Minister resigns over security breach
- Canada's secret spy days are over: CSIS chief
- Secrets to Canadian "Spy Quarters" takeover of USA revealed
- Secretive Canadian spy agency to get \$62-million HQ
- French bugs 'discovered in UK Defence Minister's office'
- U.S. Investigates Laptop Spying Suspicions

Password Protection & Computer Encryption

Creating a password for your Windows XP account is fairly simple, click Start>>Control Panel. Double-click User Accounts and select your account. Select "Create a password."

For Windows Vista, log in with your user account. Click Start>>Control Panel. Double-click User Accounts. Click "Create a password for your account." Enter the password and then enter it a second time for confirmation. Click "Create password." Your password has been created.

Protecting your user accounts is a good start and may be sufficient to keep casual snoops away. But, these passwords can be easily cracked. So, if you have particularly sensitive data, you should use an encryption program.

Windows XP includes encryption abilities. To encrypt a file or folder, right-click it and select Properties. On the General tab, click Advanced. Select "Encrypt contents to secure data" and click OK. Click Apply and select your options. Click OK.

Unfortunately, Windows stores the encryption key with your user account. Anyone who knows your Windows password can automatically access your encrypted files. Or, given a little time, your Windows password, no matter how strong, could be broken. There are numerous tools available on the Web to do just that. So, XP's encryption is also easy to crack.

Your best bet is using third-party programs to encrypt data in Windows. To download free encryption software visit our "Free Investigative Software & Publication Downloads" category in the Resource Centre. There you'll find several free softwares that will protect your files with 128-bit encryption algorithm as well as military grade 256-bit AES encryption.

Evaluating One-On-One Allegations

One-on-one allegations are very common in criminal investigations. The accuser may be an alleged victim. The accused, of course, denies involvement and offers an explanation for the false allegation. In other situations, an incident occurs and there are only two possible suspects. Obviously, both suspects will name the other as being the guilty party.

These “He said, she said” cases are inherently difficult to investigate for a number of reasons. Often, there is not a clear separation between a truthful and false account. That is, both parties may be telling part of the truth and also omitting or embellishing information. In many cases, these interviews are conducted when one or both parties are in an emotional state of mind which can cause misleading behavior symptoms. Finally, because these cases are often spontaneous, a decision to make an arrest must be made without the benefit of conducting an interview in a controlled environment. This web tip will offer suggestions to help assess the credibility of the people involved in one-on-one allegations.

1. Question both parties separately.

There is no better illustration of the problems associated with having both the accused and accuser present during questioning than on television court shows such as, “The People’s Court” or, “Judge Judy.” Invariably, the liar becomes more committed to his or her position and rarely confesses even when confronted with evidence. The truth-teller may become angry or reticent out of frustration and staunchly face the judge with his or her arms crossed. Suffice it to say, to learn the truth requires that both accused and accuser be questioned separate from each other.

In a domestic violence case involving a husband and wife, for example, one investigator could question the wife in one room while another investigator interviews the husband in a separate room. In a traffic stop, one occupant may be left in the vehicle while the other is questioned away from the vehicle. Following the initial interview, the first occupant could be asked to wait in the vehicle while the second is questioned away from the vehicle.

If the interviews are conducted by the same investigator at different times, it is beneficial to first interview the accuser and then the accused. If two possible parties to a crime need to be interviewed, the person most likely to tell the truth, or least likely involved, should be interviewed first. This assessment may be based on age, strength of evidence, as well as behaviors or attitudes displayed during initial questioning.

2. Consider having both parties write out a statement.

In a controlled environment, such as a business where an employee is making allegations of unwanted sexual advances against a supervisor, it is often beneficial to not only question each party separately, but also to have each party first write out a statement. This suggestion applies equally well to any one-on-one allegation where both parties are in a controlled environment.

To obtain the statement the investigator should give the suspect a couple of sheets of lined paper and pen. At the top of the paper the investigator should write out a question which he instructs the person to answer in writing. The question should require that the person explain everything about their behavior, knowledge or observations. The following are possible introductory questions to ask in different situations:

Domestic violence: “Tell me everything about what happened between you and your husband (wife) this evening.”

Sexual harassment (complainant): “Tell me everything about what you experienced at (Company) that led to your complaint.”

Sexual harassment (respondent): “Sally Smith reported that you made sexual remarks to her. Tell me everything about any sexual remarks you have made to Sally Smith.”

Gun found in dorm room: “Tell me everything you know about the 9mm gun found in your dorm room last Friday night.”

Hit and run with two possible drivers: “Tell me everything you know about the damage to the front right bumper of your room mate’s car.”

While it does take extra time to obtain a written statement (most of these, even from truthful subjects, are only a couple of paragraphs long) there are a number of benefits. First, the statement can be assessed for credibility by applying statement analysis techniques. Second, information from the statement can help the investigator prepare for a formal interview of a suspect in that he knows what topics to cover and may have identified problem areas within the statement to pursue. Finally, because the statement is a permanent document from the suspect, any documented lies or inconsistencies can be used to support decisions relating to the case disposition.

3. Obtain behavioral information from both parties.

It does the investigator little good to learn that a husband yelled at his wife and scared her. To assess credibility, the investigator must develop behavioral information. Behavior is objective and fixed in time. It is not subject to justification, rationalization or individual interpretation. The investigator needs to find out specifically what was done, who was present, what object was used, where something happened, what was said, etc.

While it is certainly more efficient to ask questions that require a yes or no response such as, “Did your husband threaten you with a weapon of any kind?” or, “Did your husband strike you at all?”, these closed-ended questions can invite deception. Especially during early portions of an interview, the investigator should ask open-ended questions that require a narrative response. This approach is much more likely to result in truthful information as the following dialogue illustrates:

I: “What happened here this evening?”

S: “My husband came home drunk and starting yelling at me and accusing me of cheating on him. We argued and he threatened me. I was scared for my life. That’s when I called 911.”

I: “Tell me how he threatened you.”

S: “He was yelling and calling me a bitch, and he said I would pay for what I did.”

I: “Tell me about any physical contact he had with you this evening.”

S: “Physical contact? He got right in my face and was yelling and threatening, like I said.”

I: “So he did not have physical contact with you this evening?”

S: “No, but I think he was going to.”

I: “What did he have in his hands when he was arguing with you?”

S: “Well, nothing. But his voice had a threatening tone.”

If two investigators are simultaneously questioning the accused and accuser, it is much easier to establish what really happened if both investigators focus their interviews on behavioral information. When the two investigators compare notes, they can identify which behaviors both parties agree upon, and which behaviors are disputed.

4. Suggested behavior provoking questions

The unique dynamics of one-on-one interviews present the opportunity to ask a number of behavior provoking questions that may be helpful in determining which party is telling the truth. One of these is a BAIT question where the subject is asked, "If (accuser) was given a polygraph examination concerning the statement that you pointed a knife at her this evening, what would her polygraph results be?" An innocent suspect typically predicts that the accuser will fail the polygraph. On the other hand, the guilty suspect will not have that level of confidence and may offer an evasive response, e.g., "I don't really know much about polygraphs" or perhaps even predict truthful results, "She's a really good liar – she might be able to beat a polygraph." As a legal aside, an employer is not in violation of the 1988 Employee Polygraph Protection Act by asking an employee how another employee would do on a polygraph.

A second behavior provoking question is the CREDIBILITY question. It is simply phrased, "When (accuser) says that you (did issue) is he/she lying? e.g., "When Sally says that you forcibly pulled down her jeans and underwear, is she lying?" It is very difficult psychologically for a person who knows that the accuser is telling the truth to respond to this question with a confident agreement. A deceptive suspect may offer a qualified response, "I believe she might be, yes." or an evasive response, "I know what happened, and that's all I can say."

In the controlled environment of a laboratory study, one-on-one allegations are the easiest type of case to solve. By design, one subject is telling the truth and, therefore, the other subject must be lying. In real life, however, these cases are often not cut and dried because the subjects' behavior is contaminated by numerous outside variables including intense emotions, intoxication of one or both parties, and the telling of partial truths. An important key in assessing the credibility of parties involved in a one-on-one allegation is to interview both parties separately and focus the interview on specific behaviors, not opinions or judgments. In a controlled environment, requesting that both parties respond in writing to a central question can be beneficial both in making an initial assessment of credibility as well as conducting a subsequent interview.

The topic covered in this web tip is derived from information covered during our advanced course on interviewing and interrogation. If you have attended our basic course and are ready to enhance your ability to detect deception and elicit confessions, check our course calendar for the location of the advanced course nearest to you.

For further information on interrogation or interviewing techniques consider attending our advanced course on interviewing and interrogation. All CPIRC members get discounts on Reid seminars.

This article was prepared by John E. Reid and Associates, Inc. as their Monthly Web Tip and was reprinted on our web site with their permission. For additional Monthly Web Tips, go to www.reid.com and click on "Helpful Info".

Military Rations For PI's and Protection Agents?

Military rations or MRE's (Meals-Ready-to-Eat) are usually not at the top of the priority list for private investigators or personal protection agents. Here is a brief explanation of what MRE's are and how they can be useful to yourself and your team.

A Brief History

In 1975, the U.S. Department of Defense began testing MRE's to try and come up with not only a nutritionally balanced meal, but also a palatable one so soldiers would finish every meal. Over the years they have made many improvements to MRE's by adding Flameless Ration Heaters (FRH), allowing soldiers to have a hot meal, introducing more entree options and larger serving sizes. By the mid nineties, plastic spoons and napkins were added and the number of menus increased from 12 to 24 different entrees, all including a variety of ingredients. Today, soldiers can choose from up to 24 entrees, and more than an additional 150 items.

Special Characteristics of MRE's

- Each meal provides approximately 1,200 Calories.
- The shelf life of MRE's range from 1 month when stored at 49 degrees Celsius, to 8 years when stored at 10 degrees Celsius. Some manufactures claim over a 10 year shelf life.
- Prices per meal range from \$9 to \$13 per meal.
- Every meal is packaged in retort pouches which are made from a technologically advanced multi-layered film and aluminum material, filled with food, sealed, and heated for sterilizing purposes. These pouches are lightweight, flexible and durable. Retort pouches can be air-dropped and subjected to extreme heat without affecting its contents, as long as the package remains sealed.

Why would an Investigator or Protection Agents ever need MRE's on hand? Well, in North America the uses would be limited. But, when working overseas in remote areas MRE's can be a life saver. If working a protection detail in a remote region in Africa where safe food may not be readily available, you do not want to take the chance of getting a food borne illness which may render you incapacitated for several days. Depending on who your client is he/she may not even want to entertain the idea of eating food that's been sealed in a plastic bag for a few years. But, what happens if your vehicle breaks down on a dirt road miles away from any help? It is the job of the protection team to be prepared for the unexpected and MRE's are a great addition to a survival kits.

As for Private Investigators, conducting a covert static surveillance for long periods of time poses several challenges. The two main challenges are readily available washrooms and food. For Most PI's in a vehicle, using the old 2 litre soda bottle trick to help relieve the pressure. When conducting a surveillance for 2 to 3 days straight, in rural or remote areas, granola bars and other snacks can only take you so far . One or two MRE's in an emergency kit can really help you keep your focus on the task at hand and not on your hunger.

HOW TO CONTACT US



Monday to Friday	09:00 -17:00 (Eastern Standard Time)
Saturday & Sunday	Via Email Only
Canadian Statutory Holidays	Closed

Telephone:	(514) 373-8191
Fax Inquiries:	(514) 303-8841
Mailing Address:	CPIRC 2348 Chemin Lucerne, Suite #506 Ville Mont-Royal, QC H3R 2J8 Canada

For all membership, product or general enquiries please [click here](#).

www.cpirc.com

