



The Canadian Investigator

July 2009

A newsletter for Canadian Investigative Professionals

Issue 4

New Street View may breach law

Privacy office keeping an eye on Google

By Vito Pilioci. *The Ottawa Citizen*

The Internet giant Google Inc. may be in breach of federal privacy laws with its Street View initiative, according to the office of the Federal Privacy Commissioner.

The company announced that camera-laden cars would soon be driving through major Canadian cities taking pictures for Google's Street View feature. The special camera technology takes pictures of daily life.

The announcement was required under the federal Personal Information Protection and Electronic Documents Act (PIPEDA). According to the act,

Google must notify the Canadian public they are undertaking the photographic initiative before they begin.

However, the company has revealed it has been taking pictures for months. A spokeswoman for Google said that the company has already collected enough images to offer Street View in many Canadian cities.

Google spokeswoman Tamara Micner said that any further images Google captures will just be used to update photos where surroundings have changed. "We drove to get our initial set of imagery and that is what we will be launching soon. This second round of driving

Continued on page 2

Investigations Canada exhibits at CAMA Conference in Whistler BC

Brian Lawrence and Ken Cahoon, of Investigations Canada, (shown at right of photo) exhibited at the CAMA Conference (Canadian Association of Municipal Advisers) in Whistler, BC in June 2009.



New Street View may breach law

Privacy office keeping an eye on Google

Continued from page 1

is to update the imagery and hopefully add more," said Micner, who added that the announcement was done at the behest of the privacy commissioner's office, which asked for more public disclosure before Google's next round of Street View image collection.

The company issued a statement: "We've been working with Canada's federal and provincial Privacy Commissioners, and we'll continue to work with them, and we've had very positive discussions. Google Street View helps users better understand their areas and explore others, and our users have told us that this ability to view a location as if they were actually there helps them better understand and find information about the places they live and visit."

An official in the privacy commissioner's office said the office is aware of Google's Street View image archive and is in discussion with the company about its obligations when it comes to privacy laws in Canada.

"We have expressed our concerns about a lack of previous notification which is why we are encouraged at this time to see notification on a go-forward basis," said Elizabeth Denham, assistant privacy commissioner of Canada with primary responsibility for the federal private-sector privacy law. "It is possible that there could be a violation of PIPEDA (Personal Information Protection and Electronic Documents Act), but we can't simply make that determination without more due diligence."

Schedule 1, section 5, subsection 4.2, entitled "Identifying Purposes" of the act clearly states: "the purposes for which per-

sonal information is collected shall be identified by the organization at or before the time the information is collected."

Denham said an investigation into the way the company has collected its images may be necessary. However, the commission's hands are tied until Google officially launches Street View in Canada and puts the images online for people to see.

All that is needed to trigger an investigation is for a group or an individual to file a privacy complaint with the commissioner's office once the service is launched.

Denham says the commission has chosen to continue an open dialogue with Google in hopes of avoiding a fight and resolving any contentious issues before Google launches Street View here.

Aside from collecting images without proper disclosure, Denham said the com-

Continued on page 9

Letter to the Editor

Trish

I found Norm Groot's article to be fascinating. It is obvious that the process when dealing with the Registrar's office is something to be wary of. I hope there are many agencies in the same category as ours, we have never had to deal with the Registrar's office regarding a serious complaint. I would suggest as a follow-up to the article that Norm prepare something that deals generally with the procedures and gives business operators some information as to how we should respond from the onset of contact by the Registrar and any subsequent investigation by the licensing office. In any event, please thank Norm for providing us with his insight.

-Larry Hetherington, Albright Investigation Ltd

Advertising Rates			
Size	First 10 issues Each ad	11th issue	12th issue
Full page	\$300.00	Free	Free
2/3 page	\$225.00	Free	Free
1/2 page	\$150.00	Free	Free
1/3 page	\$100.00	Free	Free
1/4 page	\$75.00	Free	Free
Business card	\$50.00	Free	Free

Next issue of the Canadian Investigator will be published September 15, 2009. Get your news and photos in now to tdehmel@csiinvest.com

OPC releases guidance on private sector covert video surveillance

This article was submitted by Debra MacDonald, C3 Investigations Inc., with the notation that stakeholders in Ontario had not been notified that these guidelines had been posted on the Ontario website since May.

Introduction and scope

The Office of the Privacy Commissioner considers covert video surveillance to be an extremely privacy-invasive form of technology. The very nature of the medium entails the collection of a great deal of personal information that may be extraneous, or may lead to judgments about the subject that have nothing to do with the purpose for collecting the information in the first place. In the Office's view, covert video surveillance must be considered only in the most limited cases.

This guidance is based on the federal private sector privacy law *The Personal Information Protection and Electronic Documents Act* (PIPEDA), and is intended to outline the privacy obligations and responsibilities of private sector organizations contemplating and engaging in covert video surveillance. We consider video surveillance to be covert when the individual is not made aware of being watched.

This document serves as a companion piece to the following guidelines for video surveillance issued by this office: [Guidelines for Overt Video Surveillance in the Private Sector](#) (prepared in collaboration with Alberta and British Columbia) and [Guidelines for surveillance of public places by police and law enforcement authorities](#).

Please note that the following is guidance only. We consider each complaint brought before us on a case-by-case basis.

PIPEDA requirements governing covert video surveillance

PIPEDA governs the collection, use and disclosure of personal information in the course of a commercial activity and in the employment context of federally regulated employers¹. The capturing of images of identifiable individuals through covert video surveillance is considered to be a collection of personal information. Organizations that are contemplating the use of covert video surveillance should be aware of the criteria they must satisfy in order to collect, use and disclose video surveillance images in compliance with PIPEDA. These criteria are outlined below and address the pur-

pose of the covert video surveillance, consent issues, and the limits placed on collecting personal information through covert video surveillance.

A common misconception is that organizations are released from their privacy obligations if covert video surveillance is conducted in a public place. In fact, under PIPEDA, any collection of personal information taking place in the course of a commercial activity or by an employer subject to PIPEDA, regardless of the location, must conform to the requirements described below.

A. Purpose

The starting point for an organization that is contemplating putting an individual under surveillance without their knowledge is to establish what purpose it aims to achieve. What is the reason for collecting the individual's personal information through covert video surveillance? Under PIPEDA, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (subsection 5(3)).

In deciding whether to use covert video surveillance as a means of collecting personal information, an organization should closely examine the particular circumstances of why, when and where it would collect personal information and what personal information would be collected. There are a number of considerations that factor into determining whether an organization is justified in undertaking covert video surveillance. Given the different contexts in which covert video surveillance may be used, the ways in which the factors apply and are analyzed vary depending on the circumstances.

Demonstrable, evidentiary need

In order for the organization's purpose to be considered appropriate under PIPEDA, there must be a demonstrable, evidentiary need for the collection. In other words, it would not be enough for the organization to be acting on a mere suspicion. The organization must have a strong basis to support the use of covert video surveillance as a means of collecting personal information.

Information collected by surveillance achieves the purpose

Continued on page 4

OPC releases guidance on private sector covert video surveillance

Continued from page 3

The personal information being collected by the organization must be clearly related to a legitimate business purpose and objective. There should also be a strong likelihood that collecting the personal information will help the organization achieve its stated objective. The organization should evaluate the degree to which the personal information being collected through covert video surveillance will be effective in achieving the stated purpose.

Loss of privacy proportional to benefit gained

Another factor to be considered is the balance between the individual's right to privacy and the organization's need to collect, use and disclose personal information. An organization should ask itself if the loss of privacy is proportional to the benefit gained. It may decide that covert video surveillance is the most appropriate method of collecting personal information because it offers the most benefits to the organization. However, these advantages must be weighed against any resulting encroachment on an individual's right to privacy in order for a reasonable person to consider the use of covert surveillance to be appropriate in the circumstances.

Less privacy-invasive measures taken first

Finally, any organization contemplating the use of covert video surveillance should consider other means of collecting the personal information given the inherent intrusiveness of covert video surveillance. The organization needs to examine whether a reasonable person would consider covert video surveillance to be the most appropriate method of collecting personal information under the circumstances, when compared to less privacy-invasive methods.

B. Consent

As a general rule, PIPEDA requires the individual's consent to the collection, use and disclosure of personal information (Principle 4.3). It is possible for covert video surveillance to take place with consent. For example, an individual can be considered to have implicitly consented to the collection of their personal information through video surveillance if that individual has initiated formal legal action against the organization and the organization is collecting the information for the purpose of defending itself against the legal action. It is important to note that

implied consent does not authorize unlimited collection of an individual's personal information but limits collection to what is relevant to the merits of the case and the conduct of the defense.

In most cases, however, covert video surveillance takes place without consent. PIPEDA recognizes that there are limited and specific situations where consent is not required (paragraph 7(1)(b)). In order to collect information through video surveillance without the consent of the individual, organizations must be reasonably satisfied that:

- collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information; and
- the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

The exception to the requirement for knowledge and consent could, in certain circumstances, provide for the collection of a third party's personal information.

In the employment context, an organization should have evidence that the relationship of trust has been broken before conducting covert video surveillance. Organizations cannot simply rely on mere suspicion but must in fact have evidentiary justification.

Regardless of whether or not consent is obtained, organizations must have a reasonable purpose for collecting the information.

C. Limiting collection

When collecting personal information, organizations must take care to limit both the type and amount of information to that which is necessary to fulfill the identified purposes (Principle 4.4). Organizations should be very specific about what kind of personal information they are looking to collect and they should limit the duration and scope of the surveillance to what would be reasonable to meet their purpose. Moreover, the collection must be conducted in a fair and lawful manner.

As well, organizations must limit the collection of images of parties who are not the subject of an investigation. There may be situations in which the collection of personal information of a third party² via cov-

Continued on page 5

OPC releases guidance on private sector covert video surveillance

Continued from page 5

ert video surveillance could be considered acceptable provided the organization has reason to believe that the collection of information about the third party is relevant to the purpose for the collection of information about the subject. However, in determining what is reasonable, the organization must distinguish between persons who it believes are relevant to the purposes of the surveillance of the subject and persons who are merely found in the company of the subject. In our view, PIPEDA does not allow for the collection of the personal information of the latter group without their knowledge or consent.

Organizations can avoid capturing individuals who are not linked to the purpose of the investigation by being more selective during video surveillance. If such personal information is captured, it should be deleted or depersonalized as soon as is practicable. This refers not only to images of the individuals themselves, but also to any information that could serve to identify them, such as street numbers and licence plates. We advocate the use of blurring technology when required. Though we acknowledge its cost to organizations, we view the expenditure as necessary given that, pursuant to PIPEDA, the personal information of any individual can only be collected, used and disclosed without consent in very limited and specific situations.

The need to document

Proper documentation by organizations is essential to ensuring that privacy obligations are respected and to protect the organization in the event of a privacy complaint. Organizations should have in place a general policy that guides them in the decision-making process and in carrying out covert video surveillance in the most privacy-sensitive way possible. There should also be a documented record of every decision to undertake video surveillance as well as a record of its progress and outcome.

i. Policy on covert video surveillance

Organizations using covert video surveillance should implement a policy that:

- sets out privacy-specific criteria that must be met before covert video surveillance is undertaken;

- requires that the decision be documented, including rationale and purpose;

- requires that authorization for undertaking video surveillance be given at an appropriate level of the organization;

- limits the collection of personal information to that which is necessary to achieve the stated purpose;

- limits the use of the surveillance to its stated purpose;

- requires that the surveillance be stored in a secure manner;

- designates the persons in the organization authorized to view the surveillance;

- sets out procedures for dealing with third party information;

- sets out a retention period for the surveillance; and

- sets out procedures for the secure disposal of images.

ii. Documenting specific instances of video surveillance

There should be a detailed account of how the requirements of the organization's policy on video surveillance have been satisfied, including:

- a description of alternative measures undertaken and their result;

- a description of the kind of information collected through the surveillance;

- the duration of surveillance;

- names of individuals who viewed the surveillance;

- what the surveillance was used for;

- when and how images were disposed of; and a service agreement with any third party hired to conduct the surveillance, if applicable.

Best practices for using private investigation firms

Many organizations hire private investigation firms to conduct covert video surveillance on their behalf. It is the responsibility of both the hiring organization and the private investigation firm to ensure that all collection, use and disclosure of personal information is done in accordance with privacy legislation. We strongly encourage the parties to enter into a service agreement that incorporates the following:

- confirmation that the private investigation firm constitutes an "investigative body" as described in

Continued on page 10

A Picture's Worth a Thousand Words: Investigating the Claimant

1By Helen Pelton, M.Sc., LL.B, Pelton Law

When someone is injured and an insurance claim results, the challenge for the insurer is to separate genuine claims from those that are exaggerated, or even fake. The first question to be answered is whether there is any liability for the claim. The second involves an assessment of a fair quantum for the injuries and impairments. Both questions are answered by evaluating the evidence, but only the second question will be the focus of this article.

We all understand the basics – evidence is something that tends to prove the truth of a fact. Objective evidence rarely presents a problem. If an X-ray shows a broken bone, there is no argument that the person has suffered a fracture. Areas that cause the greatest difficulty are ones for which there is no objective metric. These are things for which the only evidence comes directly from the claimant. Pain is the most obvious example that springs to mind.

It is an established fact that some accident victims will go on to develop chronic pain - pain that persists after the expected healing time has passed. Unfortunately, there is still no objective method of determining when a person is experiencing pain, and no method of quantifying the degree of pain being experienced. Current medical research focuses on methods of imaging the brain and identifying pain responses. However, we still seem to be a long way from a reliable, readily available measuring tool.

Another symptom which relies on self-report is tinnitus. This is the sensation of hearing a ringing or buzzing when there is no external source, and can range from mild to totally debilitating. Unfortunately tinnitus cannot be detected by any of the normally available tests, and has been reported to occur after trauma. (On a side note, in the U.S. in 2006, the V.A. paid \$539 million to veterans with tinnitus.) Even if the initial injury and its severity are capable of objective measurement, the subsequent degree of impairment is often also largely subjective. X-rays may show the broken bone has healed, but the claimant may report continuing pain, reduced range of movement, and a general inability to function as before.

Cognitive impairments are measured by sophisticated psychometric tests which are purported to be very

reliable. However, there are critics of almost every test in current use. Plus there is enough knowledge in the public domain, despite attempts to keep the test questions confidential, that a determined individual could manipulate the results. So for now we rely on what the claimant says.

The fundamental question then becomes – is the claimant telling the truth. Once again – we have no direct way of determining this – no fool-proof lie detector is available to us. We therefore have to come at this indirectly. If we can obtain evidence that suggests the claimant is not telling the truth in some area, then we can draw the inference that they may not be telling the truth about their symptoms or impairments. Sometimes we will collect evidence that directly contradicts that of the claimant.

2 The classical tool in the defense arsenal is the surveillance video. Good surveillance contains clear, focused images of the claimant taken for continuous periods over blocks of consecutive days. If the footage shows the claimant engaged in questionable activity on any given day, there should be several days of surveillance after the event. For example, if the claimant is found playing golf on one day, it is important to demonstrate that this was not followed by three days of bed rest. Written reports of the surveillance should be confined to facts, and not opinions. A report which provides the observers own opinions of the lack of signs of pain, or the ease of walking will provide fertile ground for cross examination at a trial. Assuming that useful surveillance has been obtained, there is then the question of how best to use it. Assuming that the file is now at the stage where counsel have been retained on both sides, the defense must decide whether to give a copy of the video to the claimant's lawyer, or to claim privilege and save it for impeachment purposes at trial. (Impeachment refers to challenging something the claimant has said in direct testimony.) There are pros and cons to both approaches.

Firstly, no matter which route is chosen, the existence of the video must be disclosed, and a fair amount of detail about the contents must be re-

Continued on page 7

A Picture's Worth a Thousand Words: Investigating the Claimant

Continued from page 7

vealed. These include the dates and times of the surveillance, and a statement of what activities are depicted. If defense counsel plans to show the video at the trial as substantive evidence, then the actual video must be given to the claimant's lawyer at least 90 days before the trial. If it will only be used for impeachment, no copy need be given.

Understanding the difference between substantive evidence and impeachment evidence is no trivial task, and one that confuses juries. An example may make it clear. Suppose the defense has video of the claimant playing golf. If the defense plans to use it substantively, they must give the video to the claimant's counsel more than 90 days before trial, and can then show the video no matter what the claimant says, or does not say about playing golf. However, suppose the defense continues to claim privilege over the video, and wants to use it only to impeach the claimant. If the claimant testifies in direct evidence about playing golf, then there can be no purpose to showing the video – it will not contradict the earlier evidence and the defense will not be permitted to show it.

It may then seem that the best practice is always to use the video as substantive evidence and hand over a copy within the time limits. There is a lot to be said for this approach. If the video demonstrates unequivocally that claimant is clearly less impaired than claimed, the case should settle before trial.

However, it is the grey areas that cause all the problems. The video may show the claimant out and about in public, seemingly unimpaired, perhaps carrying something. A carefully prepared direct examination of the claimant at trial may elicit the testimony that this was the public face, not revealing the inner pain, or that this was taken in unusual circumstances, or was followed by days of pain etc. Many defense counsel are reluctant to give the claimant's counsel 90 days to prepare this rebuttal.

An interesting case to read about the admissibility of surveillance at trial is the 2006 Ontario Court of Appeal decision in *Landolfi v. Fargioni*¹. The defendant had appealed the trial decision on three grounds, one of which was the judge's refusal to admit surveillance of

the plaintiff. In his trial testimony, Mr. Landolfi said he had almost constant neck pain and restricted neck mobility. At a *voir dire*³, the judge was shown video of Mr. Landolfi working out in an exercise room, and being very active outside his home. He disallowed the video, finding it was grainy and hard to see Mr. Landolfi's facial expressions. He was also concerned because the videos were not continuous or complete. The Court of Appeal disagreed and set out the test for admissibility of a videotape. In addition to the usual requirements that all evidence must be reliable and necessary, videotapes must be accurate, a fair representation of the facts, and capable of being verified by a person under oath. Addressing the possibility that the jury would use the video as substantive evidence, not just for impeachment, the Court said this was always a risk, but required a proper limiting instruction to the jury. A new trial was ordered. Shortly after the *Landolfi* decision was released, the issue was considered in *Lis v. Lombard Insurance Co*². There Justice Bryant refused to admit surveillance taken over 7 days of the plaintiff loading groceries and picking up cases of water. The judge held that the plaintiff had never said she could not do these things, only that she suffered from constant pain. He held that the jury would be likely to misuse the tape as substantive evidence. By contrast, Madam Justice Walters reached the opposite conclusion in *Howe v. Garcia*³. The plaintiff claimed daily pain in her neck and back with associated headaches. Applying the *Landolfi* test, video of the plaintiff shopping, driving and gardening was found to be

Continued on page 8

**Have news about your PI
association or your Agency?
Send your news to
tdehmel@csiinvest.com**

A Picture's Worth a Thousand Words: Investigating the Claimant

Continued from page 7

inconsistent with this evidence and thus was admitted for impeachment. Anyone commissioning surveillance needs to be very careful how it is obtained. The case of *Cowles v. Balac*⁴ is a sobering example.

This is the famous African Lion Safari case. David Balac and Jennifer-Ann Cowles were mauled by Bengal tigers when driving through the African Lion Safari park. Somehow the windows came down, allowing the tigers access to the occupants of the car with devastating results. An investigator was sent to Hanrahan's Tavern, where Ms. Cowles was continuing to work as an exotic dancer, and he engaged her in conversation. The trial judge excluded the investigator's evidence on the grounds that defense counsel had violated the Rules of Professional Conduct that prevent a lawyer from contacting a party who is represented by counsel. The investigator was acting on behalf the lawyer, which is considered direct contact. The trial decision was appealed on several grounds, one of which was the exclusion of the investigator's report. The appeal was denied on all grounds. All three judges of the Court of Appeal panel agreed that the trial judge erred in excluding the report. However, the majority held that the investigator's evidence would have made no difference to the outcome. Despite the ruling in this case, it still appears to be prudent practice to instruct investigators not to make direct contact with plaintiffs. Courts permit surveillance videos on the basis that they are taken when the claimant is out in public, and has no expectation of privacy.

What expectation of privacy exists for a claimant who posts images on Facebook or other websites? It seems obvious that if the pages are accessible to the general public, then the claimant has put them in the public domain and has no expectation of privacy. It is analogous to handing out copies on the street. However, if access to images is only achieved by making direct contact with the claimant, then that would seem not to be permissible, just as the defense cannot approach the claimant

directly in person. Facebook for example, requires you to ask to be "a friend" in order to view private pages.

However, in posting images at all, even if supposedly only to "friends", has the claimant relinquished the right to privacy? The fine print to which you agree when you become a user of Facebook gives Facebook the right to publicly display and distribute the content for any purpose. It will be interesting to see how courts will interpret this agreement for the purpose of access to "private" pages. In the meantime, all adjusters and defense counsel should routinely search claimants' names on all the commonly used personal websites as soon as the file lands on their desks, and if images are found which contradict the claimant's story, should download all such material and store it in a safe (electronic) spot.

Some recent cases show the trend that is emerging. On December 17, 2000, an 18 year old woman, Fotini Kourtesis, was rear-ended and alleged that she went on to develop chronic pain. During the five week jury trial, Fotini gave evidence that her social life was non-existent as a result of the accident. This was backed up by evidence from her brother John. Unfortunately for Fotini, she had posted pictures on Facebook that painted an entirely different picture, showing a vigorous and active social life right up to the time of trial. These pictures came to light during the trial and defense counsel sought their admission in a *voir dire*. The judge allowed them to be admitted into evidence, but gave Fotini the opportunity to be recalled to address them. The judge took note of the fact that Fotini had control over the photographs, and she placed them on the website to present herself to those who had access. Ruling that the plaintiff's claim for general damages did not cross the threshold, the judge also noted that when recalled, Fotini gave an animated and detailed account of the times and places of the events depicted, in contrast to other evidence of memory and concentration problems. Fotini was awarded only \$25,000 for future financial loss, all other claims, including FLA, were dismissed. The *Kourtesis* case⁵ was promptly followed by a pre-trial motion in the case of *Murphy v. Perger*⁶. Defendant's counsel was aware that the plaintiff had a publicly accessible site called "The Jill Murphy Fan Club", but also knew there

Continued on page 9

New Street View may breach law

Privacy office keeping an eye on Google

mission has also expressed concerns to Google about creating mass databases of images containing photos of Canadians. While the images that appear on the Internet will have people's faces blurred, as well as license plates on cars, the commission is concerned about the original unblurred images, how they are being stored and how long Google plans to keep them on file.

At least one expert on Canadian privacy laws thinks Google is going to have to continue to fight an uphill battle to roll out Street View in Canada.

"The commissioner has said, and I certainly agree with her, that consent is the foundational principle in the act. The whole point of privacy legislation is to ensure that I have a say about how my personal informa-

Continued on page 10

A Picture's Worth a Thousand Words: Investigating the Claimant

Continued from page 8

was a private site created by Jill's sister, but controlled by Jill. The defendant sought access to this site. The plaintiff resisted, saying this was a fishing expedition, the photographs were taken by friends, thus the plaintiff could not control the content, the defendant was not prejudiced because she had access to the public site, and finally the request was unfair, being made four weeks before trial. The defendant relied on the decision of Justice Browne in *Kourtesis 5* (above) who held that the photographs were analogous to surveillance, over which the plaintiff would have no control, the photographs were highly relevant, and although they had minimal probative value, they related to a material issue, namely the assessment of general damages. The judge ruled in favour of the defense, finding that any invasion of privacy was minimal, and was outweighed by the defendant's need to have the photographs in order to assess the case. The judge commented that the plaintiff clearly considered some photographs to be relevant, having served photographs of herself taken before the accident. The plaintiff was ordered to provide the defense with copies of the web pages. This case settled three days before the trial. While one can never know for certain the impact of these very revealing pages on the settlement discussions, it is a fairly safe bet they did



not help the plaintiff. Facebook also seems to have played a role in a third decision in which a plaintiff failed to cross the threshold. In *Goodridge (Litigation Guardian of) v. King*, Stacey Goodridge claimed to be embarrassed by scars on her face and shoulder sustained in a car accident⁷. However, the judge noted she had posted pictures of herself on Facebook, and that she had acted as a bridesmaid, wearing an off-the-shoulder gown.

Helen Pelton is a civil litigator in Hamilton, Ontario. She practices in the area of personal injury for both insurers and plaintiffs. She can be reached at hpelton@peltonlaw.ca or at www.peltonlaw.ca.

¹ *Landolfi v. Fargione* (2006), 79 O.R. (3d) 767

² *Lis v. Lombard Insurance Co.*, [2006

[O.J. No. 2578 (S.C.J.)

³ *Howe v. Garcia* (2008) CarswellOnt 5671 (S.C.J.)

⁴ *Cowles v. Balac*, [2006] O.J. No. 4177 (C.A.)

⁵ *Kourtesis v. Joris*, [2007] O.J. No. 2677 (S.C.J.)

⁶ *Murphy v. Perger*, (2007) Carswell Ont 9439 (S.C.J.)

⁷ *Goodridge (Litigation Guardian of) v. King*, (2007) Carswell Ont 7637 (S.C.J.)

OPC releases guidance on private sector covert video surveillance

Continued from page 4

PIPEDA "Regulations Specifying Investigative Bodies";

- an acknowledgement by the hiring organization that it has authority under PIPEDA to collect from and disclose to the private investigation firm the personal information of the individual under investigation;

- a clear description of the purpose of the surveillance and the type of personal information the hiring organization is requesting;

- the requirement that the collection of personal information be limited to the purpose of the surveillance;

- the requirement that the collection of third party information be avoided unless the collection of information about the third party is relevant to the purpose for collecting information about the subject;

- a statement that any unnecessary personal information of third parties collected during the surveillance should not be used or disclosed and that it should be deleted or depersonalized as soon as is practicable;

- confirmation by the private investigation firm that it will collect personal information in a manner consistent with all applicable legislation, including PIPEDA;

- confirmation that the private investigation firm provides adequate training to its investigators on the obligation to protect individuals' privacy rights and the appropriate use of the technical equipment used in surveillance;

- the requirement that the personal information collected through surveillance is appropriately safeguarded by both the hiring organization and the private investigation firm;

- the requirement that all instructions from the hiring company be documented;

- a provision prohibiting the use of a subcontractor unless previously agreed to in writing, and unless the subcontractor agrees to all service agreement requirements;

- a designated retention period and secure destruction instructions for the personal information;

- a provision allowing the hiring company to conduct an audit.

Keeping an eye on Google

Continued from page 9

tion is used and who gets to see it," said Ian Kerr, Canada Research Chair in ethics, law and technology and author of a soon to be released book about privacy concerns in the digital era called *Lessons from the Identity Trail*. Kerr said just because the images were taken in public places doesn't mean they are immune to Canadian privacy legislation. "To the contrary, the privacy commissioner has publically expressed concerns about the privacy implications of Google Street View," he said.

Kerr said tough Canadian privacy legislation is likely the reason Google has taken so long to roll out the Street View service in Canada. Street View was first introduced in the United States in 2007. It has already expanded to much of Europe and Britain.

Google has argued that the service is an incredibly useful tool, as it allows tourists to take a virtual walk around the Eiffel Tower or to see pictures of an area around a hotel they may consider booking.

© Copyright (c) The Ottawa Citizen

CAPI Executive-2009

Position	Member	Location	Telephone	E-mail
President/Secretary	Don Wilkinson	Alberta	403.257.5703	donwilkinson@shaw.ca
Vice President/BC	Garth Dunn	British Columbia	604.575.0799	gddunn@ridgeinvest.com
Treasurer/Atlantic Canada*	Fred Dehmel	Nova Scotia	902.450.0697	fdehmel@csiinvest.com
Past President/Ontario	Bill Joynt	Ontario	416.955.9450	billj@investigators-group.com
Saskatchewan	Vacant			
Manitoba	Gord Oliver	Manitoba	204.942.8002	goliver@oliveryaskiw.com
Quebec	Louis Laframboise	Quebec	514.281.2811	lframboise@garda.ca

* Atlantic office is headquartered in Halifax but covers the provinces of New Brunswick, Nova Scotia, & P.E.I.