



## **PRIVACY AND LAW ENFORCEMENT – GETTING THE BALANCE RIGHT**

### **24<sup>th</sup> Annual Training Symposium BC Crime Prevention Association**

**September 19, 2002  
Surrey, BC**

**David Loukidelis  
Information & Privacy Commissioner for British Columbia**

#### **1.0 INTRODUCTION**

I'd like to thank you for the invitation to be here today. Your Association and its volunteer members across the province play a crucial part in making our communities safe. I'm inspired looking around this room at so many people who are generous with their time in working to make our communities healthy and safe, and I'm grateful to you. Events like this training seminar are an important part of your work and I welcome the chance to share with you some of my thoughts about the elusive balance between individual privacy and community security.

In May of this year, landfill workers in Storm Lake, Iowa discovered the body of a newborn baby. His body had been mangled by landfill equipment. Authorities could not identify him or a cause of death. Hoping to find the names of pregnant women who'd given birth around the right time, the local prosecutor subpoenaed records from the local hospital and doctors. They turned them over and police visited people at home and work to ask if they'd given birth or not. Some women who'd been thought to be pregnant, but had no baby to show for it, were asked to give DNA samples to police, to prove it was not their baby.

But the local Planned Parenthood clinic – which offers pregnancy testing – refused to turn over its records. The Iowa Supreme Court will decide later this year whether the subpoena is valid or whether medical privacy should prevail. In the meantime, the local prosecutor, apologizing for what he called “any inconvenience”, said – and I quote –

A human being was thrown into the garbage and shredded and I think that crime was important enough to society to at least attempt to find out who did it.

Closer to home, Alberta's new *Health Information Act* says hospitals, doctors and other health care providers must turn patients' medical records over to police only if they have a subpoena, warrant or court order. Calgary's Police Chief, who wanted easier access to confidential medical information, condemned this law, saying it would turn hospitals into "sanctuaries for criminals".

Now, I'll pause here to wonder – lightheartedly of course – whether Alberta hospitals have filled up with criminals seeking some sort of medieval sanctuary, trying to avoid capture under the shield of the new health information law. I'm pretty skeptical that hardened criminals have been making themselves sick just so they can get into hospital and enjoy hospital food while hiding from the law.

On a more serious note, the Iowa and Alberta situations raise very serious questions of balance – how easy or difficult should it be for police to get at our medical secrets in order to fight crime? In Iowa, everyone was caught in the dragnet, not just suspects for whom there was probable cause putting them under suspicion of a crime. Is this justifiable? If we have nothing to hide, should we care if police get to leaf through our intimate medical files? Or should police have to do more?

These kinds of issues arise almost every day – issues of balance between individual rights and community interests. Privacy rights are increasingly in play, especially in our post-9/11 world. Now, I don't pretend for a minute to be able to answer these questions. I can't tell you how to reach the right balance between individual rights and community interests.

For one thing, it's not my place to do so. That's a task our elected representatives have to address, since they make the laws. Of course, it's an exercise the courts are now charged with undertaking, since our judges have been given the unenviable task of balancing various interests under the *Charter of Rights and Freedoms*. Our representatives ultimately are guided by what we say as citizens, so at the end of the day it's up to each of us as members of the community to find the right balance. And I believe the courts do try to account for community values, even if many observers think they aren't as responsive as our democratic institutions.

My role is more limited than the courts' or legislatures'. Strictly speaking, my job as privacy commissioner for British Columbia is to interpret and apply British Columbia's *Freedom of Information and Protection of Privacy Act*, which governs public sector privacy practices and about which I'll have more to say in a few minutes. As privacy commissioner, I also get to wonder out loud about privacy issues for which I ultimately bear no direct responsibility, as I've just mentioned. And that's why I'm here today – to raise questions, really, not answer them.

My aim is raise questions about the proper balance between community interests and individual rights in order to encourage you to go back to your communities ready to debate questions of privacy when they come up – locally, provincially and nationally – in

the context of law enforcement activities. When it's claimed that law enforcement goals are jeopardized by privacy claims, I urge you to seriously question whether that is true, even if you don't think your own interests will be affected. When privacy rights are supposedly at risk because of some law or law enforcement activity, question that equally vigorously. Let your views be known. Enter the fray.

Today I'm going to take you through some examples of law enforcement programs that raise privacy issues and try to give you a sense of how these concerns are or are not dealt with. These examples will, I hope, help you decide how privacy issues in your own community's law enforcement issues should be resolved.

### *What is privacy?*

The first thing to tackle is a basic, yet very slippery, issue. What do we mean when we talk about 'privacy'? There's so much talk about privacy in the media these days that I recall a typical John Crosbie wisecrack, from his time as federal environment minister. 'Yesterday', he slyly said to the media scrum, 'I'd never heard of the environment, but I woke up this morning and the damn thing's all around me.'

Privacy's kind of like that. It seems to be everywhere these days, largely because it's under threat from so many quarters. But it's hard to get any two privacy advocates to agree on what privacy means. Maybe it can only be grasped by thinking about it in the same way as Potter Stewart, a U.S. Supreme Court judge, approached pornography in a freedom of expression case in the 1970s: 'I can't define it', he said, 'but I know it when I see it'. Maybe something like that is true for privacy – we really only know what it is or what it's worth when we realize we've lost it.

It's safe to say, though, that privacy is a multi-faceted concept. This is clear from what is perhaps the best-known definition of privacy. It was formulated by Louis Brandeis, who later was a revered U.S. Supreme Court justice in the early 20<sup>th</sup> Century. In the early 1890s, he defined privacy as "The right to be let alone".

The notion of a 'right to be let alone' conjures up a concept of privacy as solitude, or reserve. The time-honoured saying that 'One's home is one's castle' touches on this. We think of our homes as our private places, our sanctuaries from the hustle and bustle of life, but also from the scrutiny of our neighbours and friends – and the state. I'd bet all of us here today believe we should be able to more or less do and say as we like at home, without prying eyes or ears eavesdropping or watching our every move – at least where there's no compelling state interest in doing so.

The right not to have your house bugged or searched by police without getting a judge to issue a warrant based on reasonable cause – the right to be free from unreasonable searches and seizures, in other words – is a right that protects your property from unjustified invasion. But it's also a right – not an unlimited right – that protects your thoughts and emotions as expressed in your private papers and belongings. Freedom from arbitrary search and seizure is, in other words, a long-standing privacy right.

As I've already said, other concepts of privacy exist. Many privacy laws – including British Columbia's *Freedom of Information and Protection of Privacy Act* – are not concerned with privacy in the same way as search and seizure laws. Such laws deal with the privacy interest in our own personal information, in recorded information about us as individuals. These laws deal, in other words, with informational privacy – information about our thoughts, beliefs and opinions. Information about our health and medical history. Information about our finances. Information about our employment history. These kinds of information are what modern privacy laws aim to protect.

As the eminent American scholar Alan Westin said 30 years ago, information privacy means the “claim of individuals ... to determine for themselves when, how and to what extent information about them is communicated to others”. I also believe that information privacy refers to the claim of individuals to have some say in how, when and for what purpose information about them is used, not just disclosed (or communicated) as Westin suggested.

The idea that each of us should have some control over the collection, use and disclosure of our personal information is aimed largely at the power of the state. Modern information privacy laws limit the state's power to collect, use and disclose personal information about citizens. They recognize that the state's power to compel or coerce individuals to give up personal information about themselves, about their lives, is very powerful and that some limitations on that power are necessary to ensure an appropriate balance between the state's power and individual rights.

This is what British Columbia's *Freedom of Information and Protection of Privacy Act* does. Like the similar laws across Canada and the federal Privacy Act, the Act limits the purposes for which the provincial government and some 2,220 other so-called public bodies around British Columbia can collect, use or disclose personal information about individuals. These public bodies include provincial government ministries, Crown corporations, local government, hospitals and health care bodies, universities and colleges, schools and self-governing professions. They also include police forces and other law enforcement agencies, but not the RCMP or other Federal agencies. The Act imposes rules on the methods these public bodies use in collecting information about individuals. It also restricts their use and disclosure of information they collect. And it requires them to take security precautions against inappropriate use or disclosure of our personal information.

I'll interject here something about my role, which I mentioned earlier is to interpret and apply British Columbia's *Freedom of Information and Protection of Privacy Act*. I am a non-partisan officer of the Legislature, appointed by the Legislature as a whole for a single six-year term. Under the Act, I have the responsibility for hearing appeals involving requests for access to records made to public bodies. I conduct formal hearings and issue written decisions and can compel public bodies to disclose information where I consider they should have done so.

Under Part 3 of the Act, which contains the privacy protections I've already described, I receive and investigate citizens' complaints that public bodies have unlawfully collected, used or disclosed their personal information. I can order a public body to correct its practices, to stop doing what it has been doing and to destroy unlawfully collected information.

### *A challenging climate for privacy*

As this description indicates, my mandate is restricted to informational privacy – what happens to our personal information in the hands of government bodies. This is a very challenging role these days. I mentioned earlier the difficulty in achieving the right balance between privacy and security. The atrocities of September 11, 2001 have focussed attention on surveillance and security technologies as never before. And in the name of security and safety, governments around the world quickly gave themselves considerable new powers to spy on their citizens and took away or watered down rights and protections that had stood in some cases for centuries.

Surveillance technologies already in the pipeline are now more widespread than they might have been but for September 11. These range from the FBI's Carnivore system – which trolls through all e-mail traffic looking for keywords or other information of interest – to technology that tracks cell phone users' precise locations and movements. Before September 11, the US Federal Communications Commission mandated that all cell phones sold in the US after this past June must have built-in trackability, ostensibly so 911 calls can be traced. This may be the sole reason for the requirement, but it means cell phones are now handy mobile tracking devices for spy agencies and law enforcement.

Facial recognition technology, coupled with surveillance cameras, is also increasingly resorted to in airports and even tourist sites, like the Statute of Liberty. Its high rate of failure has led to its abandonment in many places, notably Logan Airport in Boston, but improvements are being made all the time. The goal is to use this technology to track the movements of individuals of interest, however that may be defined, and to guard public facilities at risk of attack.

Again, since September 11, a number of historic protections against state power have given way in the name of safety from terrorism. Citizens remain – quite understandably – generally supportive of these measures. But whether these new technologies and state powers yield benefits remains to be seen. Only time will tell which measures go too far and should be scaled back or eliminated. It's hard to get the balance right in a rush, but we have to make sure the right chord is struck and citizens must keep an eye on the need for these powers in coming years.

The importance of privacy, I should emphasize, has been acknowledged by the Supreme Court of Canada. It affirmed, in a 1997 case called *Dagg*, that the "protection of privacy is a fundamental value in modern, democratic states". As the Court put it in *Dagg*, a case that dealt with information privacy:

An expression of an individual's unique personality or personhood, privacy is grounded in physical and moral autonomy – the freedom to engage in one's own thoughts, actions and decisions.

As this quote suggests, privacy is not just a matter of individual rights. Our ability to keep our thoughts and beliefs private is of course crucial to the health and success of our communities and our democratic way of life. Citizens need to be free to think about issues and express themselves privately without fear of state surveillance, in the ordinary course, in order to participate fully and freely in public life. Without an appropriate sphere of privacy for each of us as individuals, we cannot have healthy and free societies.

At the same time, we must acknowledge the needs of our communities as a whole. I can't say it better than David Blunkett, the UK's Home Secretary – the Cabinet minister responsible for policing and anti-terrorist operations – put it in an article in *The Guardian* last Saturday:

I prefer a positive view of freedom, drawing on another tradition of political thinking that goes all the way back to the ancient Greek polis. According to this tradition, we only become fully free when we share, as active citizens, in the government of the affairs of the community. Our identity as members of a collective political community is a positive thing. Democracy is not just an association of individuals determined to protect the private sphere, but a realm of active freedom in which citizens come together to shape the world around them. We contribute and we become entitled.

How we balance this entitlement to both liberty and security is more pressing now than at any time since the second world war. On the one hand we have the spectre of global terrorist networks, perpetrating outrages beyond our wildest fears. At the same time we have an explosion in communications, expanding the horizons of our working and personal lives, while offering to a deadly minority greater ability to work across national borders and outfox national security and policing services.

Now, this isn't to say that I agree with everything David Blunkett has done or proposed. Many of his recent initiatives have little or nothing to do with terrorism but represent far-reaching incursions on traditional liberties with little evident need.

But I wholeheartedly agree that now more than ever – as I said earlier – it's crucial that we get the balance right and that citizens participate in that debate. It's in this context that I hope to examine issues of technology and privacy and leave you with perspectives on how privacy matters and how it should be protected. I'll focus on two examples. The first is the sharing of information, through computerized databases, for law enforcement operations. The second example is the vogue – a cynic might suspect it is being promoted by equipment manufacturers and vendors – for using video surveillance to monitor public spaces 24/7.

### *Computerized databases for law enforcement operations*

Before discussing the first example, I should flesh out my earlier description of British Columbia's privacy legislation a little bit. Part 3 of the Act says a public body – which includes municipal police forces but not the RCMP – can collect personal information for the purposes of “law enforcement”. “Law enforcement” is defined to mean “policing, including criminal intelligence operations”. It also includes investigations or proceedings that could lead to a penalty or sanction being imposed. So a public body can collect our personal information for law enforcement activities. It can also use or disclose personal information for law enforcement purposes. Many commentators have described these as very generous provisions, although they clearly do not give law enforcement agencies complete *carte blanche*. These rules attempt to ensure that police forces and other law enforcement agencies collect, use and disclose only personal information that is relevant to and necessary for legitimate operational needs.

I'll discuss two law enforcement databases that potentially raise privacy concerns. The first example comes from Vancouver. In June of 1999, the BC Civil Liberties Association complained to my office about the Vancouver Police Department's DISC Program. DISC stands for “Deter and Identify Sex-trade Consumers”.

DISC is a database that contains the name, birth date, address, driver's licence, vehicle licence, vehicle description and identifying marks of any driver stopped by police on suspicion of soliciting or seeking sex from a sex-trade worker. The Department told us that the unexplained disappearance of many Lower Mainland sex-trade workers made it necessary to have a focused database of sex-trade consumers to help solve sex-trade workers' disappearances and to help protect sex-trade workers.

Officers only stop a car if they have observed behaviour that gives them reasonable grounds to believe that a solicitation offence under the *Criminal Code* may have been committed. For example, they stop a car only if it has continually cruised an area where sex-trade workers are present on the streets, if the driver has picked up a sex-trade worker, if a driver is found in the company of a sex-trade worker, or if the driver has continually stopped and talked to sex-trade workers.

These individuals are not charged with anything, but their personal information is entered into the DISC database. When a driver is stopped, he is told the personal information is being collected for the purposes of a law enforcement database. The information in the DISC database is used to assist investigations involving crimes against sex-trade workers or their disappearance. As part of this, the Vancouver Police Department has made the DISC database available to certain law enforcement agencies.

As a result of my investigation, I was satisfied the Department had the authority to collect, use and disclose sex-trade consumers' personal information for the purposes of the DISC Program. I concluded the information was being collected for the purposes of policing, if not specific law enforcement investigations, and was therefore authorized by

the Act. I was equally satisfied that the personal information could be collected and used by the Vancouver Police Department for law enforcement investigations or proceedings.

Last, I was also satisfied the Department could disclose information in the DISC database to other law enforcement agencies, but only for the purposes of actual investigations or proceedings. For this reason, I recommended that the Vancouver Police Department should allow other law enforcement agencies to have access to the DISC database only pursuant to a user agreement between the Department and the other agency.

That recommendation, which has been implemented by the Department, requires a user agency to agree to use the DISC information only for ongoing law enforcement investigations or proceedings and then only to the extent the information is necessary for those purposes. Only one or two designated officers are permitted to have access to the DISC database. (This is also true with the Vancouver Police Department – only two officers have access to the database.) The user agency also must agree to keep the database information confidential and to not disclose it without the prior consent of the Vancouver Police Department and then only for law enforcement investigations or proceedings by another law enforcement agency in Canada.

The obvious reason for these requirements is that DISC contains detailed personal information about individuals who have never been charged with any criminal offence, much less convicted of any offence. It's true, of course, that individuals in the database could probably have been charged with a criminal offence, but they have not been and they may in fact be entirely innocent of any wrongdoing. They have, nonetheless, ended up in the DISC database and for this reason it has been considered important to restrict access to and use of that database for legitimate law enforcement activities. It is also important to ensure that confidentiality and security requirements are being met.

I think it is fair to say that the BC Civil Liberties Association, while it has not challenged the outcome of my investigation in court, is not satisfied with my ruling. In that case, however, I was persuaded that the DISC program complied with the *Freedom of Information and Protection of Privacy Act* and struck a reasonable balance between community interests and individual privacy rights.

The next example I'll discuss is PRIME, which stands for "Police Records Information Management Environment". This is a joint effort of a number of Lower Mainland police agencies, including at least one RCMP detachment acting as a municipal police force. As I understand it, PRIME links, online, various individual police force databases. The idea is to provide police officers with online access to databases that would previously not have been accessible. PRIME contains the kind of notes, observations and comments that would traditionally have been found in a constable's notebook. These online notes can include an officer's observations of an incident, descriptions of items seized from a vehicle and so on.

For example, a Vancouver police officer might stop a suspicious pickup truck in Vancouver at 10:31 p.m. She notes the presence of a large metal toolbox in the back.

She enters into PRIME the vehicle's licence number and a description of the toolbox and the serial numbers of power tools found in it. An hour later, the toolbox is reported as stolen from a house in Surrey. The Surrey RCMP detachment is able, using PRIME, to identify a suspect. This more or less real-time access to important investigative information obviously has great investigative value.

Although I have not formally investigated PRIME, my understanding of how it operates satisfies me that it complies with the privacy provisions of the *Freedom of Information and Protection of Privacy Act*. Nonetheless, PRIME must be rolled out subject to strict usage rules, including a rule permitting access only for law enforcement purposes. In other words, no browsing or searching of the databases to see if you can dig up any dirt on your sister-in-law. PRIME should include a mechanism for auditing system access, to detect unauthorized browsing or use of information for illegitimate purposes. Police forces should also have in place employment penalties for misuse of PRIME and similar databases.

My concern about improper use is not idle. My predecessor as privacy commissioner investigated unauthorized use of CPIC by a Lower Mainland police constable who was active in anti-abortion circles. He ran licence numbers to check the names and addresses of owners of vehicles seen at or visiting abortion clinics in Vancouver.

In Saskatchewan, the RCMP is actively investigating allegedly systematic abuse of CPIC access, perhaps for profit, by public officials. Risks of abuse of systems like PRIME are therefore very real and police forces must ensure that such systems are used properly.

### *Video surveillance*

My next topic is very current in British Columbia. I'm speaking, of course, about video surveillance. I know that John Bishop is conducting a workshop tomorrow on video surveillance – or CCTV as it's called in the UK. I have seen some of his work before. Cameras have been keeping public spaces under surveillance in the UK for well over 10 years. Much of the push for CCTV in the UK came from the very real problem they have had with terrorist violence, with bombings and assassinations being common beginning in the 1970s. These are problems that neither Canada nor the US has had until last year, the Oklahoma City bombing notwithstanding.

The UK now has, by some estimates, over two million public and private surveillance cameras in operation, although that number is surely too high for public sector CCTV alone. The present Labour government has spent hundreds of millions of pounds installing new cameras in the fight against crime, correctly perceiving that anti-crime measures are popular in the face of increasing crime rates. Yet violent crime in the UK continues to steadily trend upward – despite the presence of cameras everywhere in many urban centres. The question arises whether this is because the cameras detect more crime, but the evidence suggests crime is actually increasing.

The experience here in Canada, of course, is in the opposite direction. After climbing upward from the 1970s on, crime rates in Canada have been falling since 1991. Most notably, violent crime has continued a downward trend. The numbers for 2001, released this summer, show a 1% increase in *Criminal Code* offences over 2000, but this has been attributed to a sharp increase in car theft and some petty offences such as mischief.

Perceptions of crime rates are another matter. A recently released survey by the Canadian Policy Research Networks, *Quality of Life in Canada*, says that in 1999 29% of Canadians believed that crime rates had increased and 54% believed crime rates had stayed the same. This was the case even though 1999 saw the lowest crime rates of the 1990s and continued the downward trend I've already mentioned. There's other evidence to suggest people feel less safe and more vulnerable, even though crime is down. I won't speculate if this is partly due to our being saturated daily with reality shows like COPS and often graphic news reports of violent crimes from around the world, reported in real-time right in our homes. The fact is, people seem to feel that crime is getting worse all the time, even though that is a highly debatable proposition, at a national level at least.

Yet many Canadian police forces are either seriously considering video surveillance or are implementing it. It's difficult to say whether this is because of budgetary pressures, which understandably lead police forces and boards to look for cheaper ways to watch the streets, or because of the siren song of a quick technological fix.

Certainly, my view of the evidence from the UK – and I have carefully read the studies done by the Home Office, the Scottish Centre for Criminology and others – is that it does not live up to the promise that it reduces crime overall. I do accept that video surveillance may in limited cases be a cost-effective tool for policing special cases, such as high-crime areas that are otherwise difficult to police. Video surveillance is nothing more than the modern equivalent of the constable on the beat telling people to move along. As the UK evidence suggests, video surveillance displaces crime – it moves it from the area under surveillance to other areas. As an example, no one could seriously claim that heroin addicts will kick their habits because surveillance cameras are installed in their neighbourhood. They'll move somewhere else as a group or – perhaps worse – they'll disperse across a city. But it can't be contended they'll clean up or altogether stop the petty thieving that they rely on to feed their habits.

A logical extension of displacement is that video surveillance cameras will have to be everywhere if there's any hope of deterring criminal activity in an entire city or nation. That's hardly likely to happen, if only because of the high cost of installing cameras, monitoring them and following through on the implicit commitment to respond appropriately when criminal activity is observed. There's no point installing video surveillance if you're not going to respond. Criminals won't be displaced for long if they know there's no follow-through and citizens may be lured into danger by the false sense of security that cameras give them.

I'll step aside here, for a moment, to repeat my skepticism about video surveillance's effectiveness in reducing crime overall. The UK Home Office has, despite infusing

millions of pounds into CCTV, apparently recognized this concern. It has commissioned a groundbreaking, rigorous study of the effectiveness of video surveillance in the UK, the results of which won't be known until at least the fall of 2004 (an interim report is due in November). So while video surveillance might be useful on a localized basis, to deal with serious problems of public order and violent crime by displacing or dispersing it, I remain skeptical about its cost-effectiveness. I mention this in passing only because I think this is something you should raise in your communities whenever video surveillance is proposed. Ask for the facts before accepting this. Ask yourselves if you're willing to pay for more police on the beat as a more effective first step. CCTV is not always the best, much less correct, solution.

Again, despite my skepticism about its cost-effectiveness, I accept that video surveillance may be useful, in specific cases, in dealing with localized problems of serious criminal activity in hard-to-police urban areas. But because video surveillance does raise privacy concerns, the privacy impact has to be considered.

I simply don't buy the argument that, if you are in a public place, you have no expectations of privacy. Sure, if I'm walking along Robson Street in downtown Vancouver, I expect that passersby will see me. I expect to be caught in passing on a tourist's video camera or still picture. Snippets of my conversation will be overheard. I'll be caught by in-store security cameras as I pass by. Police officers on the beat will see me.

But in central London, for example, surveillance – remember that word, surveillance – cameras will observe me several hundred times a day. It's entirely possible for the authorities to use footage from those cameras to track my every move. As I've said before, and as my colleague the federal privacy commissioner has also said, in central London the effect is the same as if a police officer followed you around as you go about your business, video-taping your every move from a point about three feet behind your left shoulder.

A detailed picture of your daily movements, habits and transactions – including the people you meet with and what you do with them – can easily be constructed. This undoubtedly reveals details about you, as an individual, and impinges on your private life. The fact that you are in plain public view while this happens is beside the point. You may not have a strong or overriding privacy interest as you go about your ordinary business in public, but the presence of comprehensive, systematic surveillance of this kind does, in fact, engage individual privacy interests.

I've already mentioned the need to ensure video surveillance is a sound investment of tax dollars before it goes ahead. It is also necessary, however, to consider the impact on privacy and liberty before deciding to go ahead. One likely impact is hard to quantify. The concern is that, if people know they are under surveillance, they will alter their habits and go about their daily business differently. They may, for example, draw back from showing affection to certain people, refrain from going to certain places or otherwise conduct themselves differently. If they think that the unblinking eye is watching them

everywhere they go, in other words, their lives will have been altered in a way that is perhaps unnecessary.

For this reason alone, I felt it was important to issue guidelines for video surveillance and we did that back in June of 2000. Our guidelines, which are available on our web site, suggest that police forces – with full participation of their governing police boards and their communities – should only adopt video surveillance if the need is clearly demonstrated. There should be verifiable ongoing evidence of serious criminal problems, notable examples being violent crime and theft. This should not be a technology that is used to combat the odd case of juvenile graffiti on Canada Post mailboxes.

It should also be clear, in any given case, that there are no other traditional law enforcement methods that are workable. For example, has community policing been tried, with more officers on the beat? Would improved street lighting be more cost effective in combating the problem? Can volunteers assist with the situation in any way? Only if traditional methods have been tried and are found lacking should video surveillance be given serious consideration.

Our guidelines also acknowledge that many video surveillance privacy impacts can be addressed through data protection approaches like those I described earlier for DISC and PRIME. Even if the decision is made to go ahead with video surveillance, practices and rules should be put in place to ensure that video images are used only for appropriate law enforcement investigation purposes and that they are securely stored and monitored. Tapes or other storage media should only be retained for as long as necessary and should be securely erased or destroyed once they are no longer needed. Examples of publication of surveillance tapes showing embarrassing or tragic incidents can be found in the UK and in the US and they should be avoided at all costs. In the UK, for example, a man tried to commit suicide by slashing his wrists and the tape showing his suicide attempt and rescue was, I understand, broadcast in the UK. This is not acceptable and must be avoided at all costs.

### ***Conclusion***

My theme has been one of engagement. Engagement by each of us, as individuals and community members, in decisions that will affect our privacy and other liberties and rights. I told you I wouldn't offer solutions to particular problems today. My goal has been to bring home to you the need to be vigilant in protecting both our rights and our communities. The balance can be tricky to get right. But we have to try based on the best information possible and a careful and reasoned analysis in each case. Don't just assume that individual rights are nothing more than a nuisance that hinders law and order. Equally, don't proceed as if every right or liberty is inviolable – that's just not the case. All rights and liberties have limits and those limits intersect with community interests. Our job as active citizens is to find where those limits lie in each case. Please try hard to do that, as the health of our communities depends on you. Thank you very much.