Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

LEVERAGING THE TRANSPARENCY EFFECT IN POLICE GOVERNANCE

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Keynote Presentation to the
BC Association of Police Boards
Victoria, British Columbia
February 28, 2014

Good afternoon everyone. Thanks David Winkler for that introduction

It is true that law enforcement has been on my mind a lot lately. 2013 may have been declared as the year of Privacy… but 2014 is shaping up to be the year of law enforcement for our office!

Drones, body worn cameras and mass surveillance are all hot issues right now—not to mention they are squarely within my purview as Commissioner. All of you will know better than anyone that this is a very interesting, and very challenging time to be in law enforcement.

What's happening in policing in BC today, especially around the collection of personal information, the advent of new technologies and big data, is in essence a microcosm of

the privacy issues playing out on the global stage. And all of you, as community leaders through your police boards, are on the leading edge of this wave and have a unique opportunity to set the tone and lead by example on these important issues.

OIPC Mandate and Role

At this point I want to take a moment for a word or two about the role of my office for those who may not be familiar with it. As Commissioner, I am independent from government. My office is charged with the important task of monitoring and enforcing public sector and private sector information and privacy laws. I am also the Registrar of Lobbyists—although today I am wearing my Commissioner's hat.

Whether it's a new government initiative, a social networking program, or shiny new databases—my office takes a deep dive into new and emerging technologies in order to uncover the how and the why of when personal information is collected, used and shared. We do this to assess compliance with the law, but also so that citizens can understand and decide for themselves whether a technology is OK or whether it's creepy.

We have a staff of 34, including investigators, lawyers, policy and technical analysts, and our intake team, doing this important work. As I say often—a small team with a big mandate.

In addition to my investigative and enforcement powers, I have a mandate to make public comments on programs, policies and services affecting information and privacy rights in BC. So -– order-making powers and a bully pulpit.

Some of you will know that under the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), law enforcement agencies have broad authority to collect and use personal information. There are special provisions for collecting and using information without consent and without notice for "law enforcement purposes", *e.g.* information collected to support an active investigation.

But—as they say—with great power comes great responsibility. There must be an appropriate balance struck between these broad powers and the legislated boundaries of the law. I understand that law enforcement wants to take advantage of new technologies to catch the bad guys in real time and in cyberspace. But that work must be done in a way that respects the privacy of citizens.

As I made clear in my investigation of police use of Automated Licence Plate Recognition technologies, better known as ALPR to most of you, collecting personal information for law enforcement purposes does not extend to collecting data on the movements and activities of law-abiding citizens "just in case it might be needed in the future". Any proposals which aim to increase law enforcement powers must be critically examined to ensure that the new powers are proportionate to the problem they seek to address, and that they do not unduly infringe on our personal privacy.

Commissioners across Canada made that very clear in the wake of Bill C-30, the so-called *lawful access legislation*, brought forward by the federal Government in 2012. While Bill C-30 did not ultimately pass, we're seeing the ghosts of that Bill in the cyberbullying legislation which was introduced last year, Bill C-13. While I commended the Cyberbullying Working Group for their efforts in this complex area, I have major concerns with this piece of legislation, specifically the amendments to the *Criminal Code* that increase the investigative powers of law enforcement, and lower the legal threshold for investigators to obtain production orders.

In my view, we need public transparency, informed and rational debate, and judicial oversight of expansion of police powers. There is no question the digital age has brought new opportunities for data collection and storage—and its application to law enforcement.

At Simon Fraser University, researchers in the Institute for Canadian Urban Research Studies are mining anonymized data to identify crime patterns and assess crime trends in the lower mainland. This is the tip of the iceberg in the emerging field of big data and predictive analytics in policing.

- A diagram from one of the many publications of the Institute shows specific research sought to create a predictive model about perceptions of crime in Vancouver neighbourhoods, and compared that data to actual crime in those areas.

- Earlier this week, the Vancouver Police Department launched Geo Dash—a police program that will be hard-wired into patrol cruisers, to give officers up-to-date information about recent crime in the city by location.

- Body worn cameras are a game-changer for policing—this technology is being implemented in Toronto and Calgary, and also tested in Edmonton, Montreal, New Brunswick, and Vancouver.

With these new technologies and new capabilities, there are new pressures to use the data in innovative ways and to share that information in cooperation with other law enforcement agencies. There is a huge appetite to collect, combine and mine data to identify patterns in crime in order to, hopefully, prevent it.

But, before we adopt these new technologies, we need to have a conversation about what is acceptable practice, both from a privacy law perspective but also what is acceptable to the general public. Police boards are uniquely positioned to lead this conversation. Your role, laid out in statute, is to set the overall direction and vision for law enforcement in your community. It's incumbent on you to be thinking about these bigger picture issues in terms of where we are going in policing on behalf of the communities you serve.

It is also reflected in your independent civilian oversight role. There is an increasing demand from citizens to know more about how police are doing their job and why. In that sense, you provide an important accountability measure for police and law enforcement activities for the public.

One needs to look no further than the debates and public comments on the NSA and CSEC revelations of mass surveillance—or the past debates on lawful access—to know that the principle of transparency and accountability is front and centre in the public mind these days. I encourage all of you to think very carefully about the courses you'll chart in the weeks and months ahead, particularly with regard to how these new technologies can and will be deployed in your communities but also opening up your decision-making and consideration of these issues to the broader public. You need to be ahead of the curve. These conversations must, obviously, take place with the active involvement and participation of the chiefs of police and other leadership in law enforcement. But, they should also engage public input and commentary on the changing role of law enforcement and technology.

Privacy Commissioners must also turn their minds to these issues – we have some work to do in this area. My office is using this transparency approach in two of our active files—both involving law enforcement.

Police Information Checks

The first is police information checks. Many of you will know that each year, tens of thousands of record checks are processed by municipal police and the RCMP, many of which are for employment screening purposes. In the past few years there has been a move afoot, on part of police forces across BC, to shift away from providing criminal record checks…to police information checks.

Some of you might know that a criminal records check is a search of a national police database for a summary of prior criminal convictions. This may be a legitimate employment screening tool, depending on the type of position.

A police information check is a broader search of police databases and includes non-conviction records. Police information checks turn up details about an individual's interactions with police that have not been proven in court: including investigations that did not result in charges, charges that did not result in convictions, adverse police contact and information related to attempted suicides or mental health apprehensions.

Let me be clear that this information is retained in a police database for legitimate policing purposes. My concern is about the use of this information (even with so-called employee consent) for employment purposes. I launched an investigation into this change of practice because I am concerned about the breadth and scope of these record checks and whether these checks comply with privacy laws. We want to know whether police information checks are beneficial in the hiring process. We also want to know how they affect individuals. If a potential employer requests a background check,

and it comes back with a flag, do you get the job? Do these checks perpetuate discrimination on the basis of past infractions, and reinforce a cycle of unemployment and crime? These are some of the questions this investigation will seek to answer.

We put out a call for public comment on this issue, and engaged key stakeholder groups including police boards. We also made a few house calls to three police departments in BC to see the system in action. A few weeks ago, I took to the airwaves in an effort to get more submissions from people who have experience with police information checks, and also to get feedback from employers who are getting these checks in the course of vetting employees.

Bright and early, coffee in hand, I did an interview with Rick Cluff on CBC's Early Edition. And no sooner had that interview wrapped our office started getting call, after call, after call. And emails! Countless emails with stories about how police information checks had affected citizens. And many from ordinary citizens voicing their opinions about these information checks. We've received nearly 100 public submissions to date. My investigative team is now reviewing that material, which will be taken into consideration as we produce a public report outlining our views and an analysis of the law on this important issue.

Hearing from the public on this issue is important because, I don't believe that even your boards were consulted in this substantive policy change.

BCACP BCAMCP

Another area where I've sought public input—including from many of you in this room—is the issue of whether I should recommend to the Legislature that it amend FIPPA to expressly list both BC Police Chief organizations as public bodies in their own right under FIPPA. Questions have been raised about the status of these organizations under the law for two important reasons.

First, Chief Constables regularly meet and speak collectively through the Associations they have created. Governments and others treat the Associations as the focal point for contact with the Chief Constables on matters of public policy. Second, from an access to records perspective, there are questions about the appropriate level of transparency of the Associations' records for FIPPA purposes. Presently, if a member of the public wants to request records of the Associations, they may have to rely on specific requests for documents held by individual Chief Constables at any given time. Assuming that the "custody or control" test is met in those situations the result may be incomplete or piecemeal.

I've received submissions from various police boards, police chiefs, and other stakeholder groups on this issue and I look forward to reviewing those submissions and providing a final analysis in the coming weeks.

GOVERNANCE AND THE TRANSPARENCY EFFECT

There are some of you in the audience who might be thinking, sure transparency and consultation are important, but these conversations typically bring out the usual suspects and the naysayers, bogging down progress on important public safety initiatives—just get on with it. I recognize that bringing the public into the discussion can add to the timeline. And yes, it can get a little messy sometimes. But those drawbacks are far outweighed by the benefits of bringing the public in. Law enforcement holds a very special position in our society—you are our protectors. You watch out for us. You keep us safe. The public must have trust in the work that you do.

Engaging the public and being more transparent about your activities is an important way to build that trust and confidence in your work. And I believe it is the only way we are going to find lasting solutions to the challenges ahead, because the answers to the increasingly complex questions of our data driven world cannot be left exclusively to those in the privacy world….or to law enforcement. The answers must also come from the people in your community.

All of you in this room who serve on Police boards act as critical links to your communities. As Commissioner, and as a citizen, I thank you for that. You are uniquely positioned to seek out diverse public views that can and will, I am sure, assist you in developing solutions to our most challenging issues.

Thank you for your attention this afternoon. I am open to any questions you may have.