OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Commissioner's September 29, 2010 Address to the BC Information Summit

Good morning.

I have been on the job as Information and Privacy Commissioner for almost 90 days. This is really my maiden speech, and I think it is time to introduce myself and talk about the direction I plan to take in protecting access and privacy rights in British Columbia.

Although I may appear to be a transplant from a distant Ottawa, I am in fact a BC native. I grew up in Richmond and am a graduate of UBC. Taking this position as Commissioner gives me a chance to return to my roots! As much as there have been many interesting times in my years with the federal Privacy Commissioner's office in Ottawa, and many challenges resolving privacy issues involving some of the world's online giants—Google and Facebook among them; it is an honour and a pleasure to bring my experience home. I also take great pleasure in rebalancing my interests in privacy and access. Most of my recent work has been in the privacy space. I spent four years with the Alberta Information and Privacy Commissioner's office, setting up the new enforcement program in Calgary to oversee Alberta's new private sector privacy law, pretty much a sibling to the BC law. I worked solely on private sector privacy issues there.

As Assistant Privacy Commissioner of Canada, my work by definition centred on privacy. I retain my passion for privacy issues, but let me assure this audience that access to information will not become the poor cousin to privacy under my watch. My graduate work was in archival and information science. In fact, I see my esteemed former professor, Terry Eastwood, in the room! As an archivist, my goal was essentially to mediate between researchers and the records, balancing openness with ethical and legal frameworks. Little did I know that this type of mediation and balancing, in the end, is one of the major tasks I face as Commissioner.

I don't believe there has been another access or privacy commissioner in Canada with experience in three jurisdictions. While some might suggest that this means I can't keep a job, I would like to paint a slightly more charitable picture. I hope my experiences in Alberta, starting up a new regulatory program, and in Ottawa where I focused heavily on online privacy issues, will help to inform my work here. Changing hats also puts me in a position to leverage greater collaboration among the commissioners across Canada.

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at 1-800-663-7867 or 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

I arrived to an office staffed with capable and committed staff—a testament to the ability of my predecessors to attract talented professionals to the office. And I have benefited from the very substantial groundwork of both my predecessors—sometimes referred to as David 1st and David 2nd. BC's numerous decisions on access matters, for example, are due to the considerable time that both David Flaherty and David Loukidelis spent writing orders. This has led to a remarkable body of access jurisprudence, one that is arguably second only to that of Ontario, which has significantly greater resources at its disposal.

My background as an archivist, an information manager and a policy wonk means that I will turn my focus to look at the broad policy issues involving privacy and access to information—including the social, legal, evidential and policy value of records.

The BC Access and Privacy Environment

One of the benefits of coming back to BC is the attention the media pays to access and privacy issues. The media here "gets it." Unlike other parts of the country, where privacy and access stories are often relegated the back pages, if they generate any interest at all, the BC media is on top of the most important access and privacy issues. A few weeks ago, for example, Vaughn Palmer of the Vancouver Sun published a story about three of my orders requiring outsourcing contracts at Vancouver Coastal Health to be disclosed. I suspect that media in many other parts of the country seeing a similar story would stifle a yawn and move on to other, likely more bloody or salacious, events.

BC also profits from a forceful civil society, something this province has in common with Quebec! No organization better characterizes this than the BC Freedom of Information and Privacy Association. FIPA is now almost 20 years old. A review of the names on the boards of directors and advisors to FIPA reveals a constellation of experts from across Canada willing to contribute to the dialogue on access and privacy. And among the many worthy of recognition, Darrell Evans merits special praise for his commitment over these decades. Public interest advocacy is not for the faint-hearted, the less tenacious or those intent on getting rich. But it is for the fair-minded, and Darrell typifies that fair-mindedness. I look forward to working with representatives of FIPA and with other stakeholders, and to being challenged by them.

Arriving here after leaving the federal Privacy Commissioner's office reminds me of the Wizard of Oz, when Dorothy says to her dog: "Toto, I've a feeling we're not in Kansas anymore." The federal Privacy Commissioner's office has a staff of over 160. The federal Information Commissioner's office has a staff of about 80. My office here—which must deal with both privacy and access issues—has 24 staff! In my previous life in Ottawa, I was a decision maker supported by policy analysts and a large team of investigators. In fact, the federal Privacy Commissioner's office has an entire branch devoted to research and policy, as does the Office of the Information Commissioner of Canada. Here in BC, most of my staff members are completely immersed in investigations. One of the first changes I made was to shift two investigators into policy work to focus on larger systemic issues, reviewing draft legislation and privacy impact assessments. I have also created and advertised the position of Manager of Communications and Public Education. I established this new team because we can't

keep looking just at the trees; we need to be able to assess the forest, and only a good policy foundation addressing systemic threats to access and privacy rights can help us do that. We also need to do a better job of educating the public about access and privacy issues. You will soon see more guidance materials and a revamped website.

Civil society, including FIPA and the BC Civil Liberties Association, has helped to fill the gaps in our capacity to address systemic issues, and there are attempts to coordinate research and investigations among the privacy and access bodies across the country. However, we still need to increase the capacity within my office. After all, systemic issues threatening privacy and access rights that arise provincially can be every bit as sophisticated and complex as those facing my federal counterparts. Being a smaller provincial organization doesn't mean that we get only the easy issues.

We do have a backlog of cases and orders. This is an enduring problem for an office that is driven by the complaints it receives. We will address the backlog of cases, including by implementing a triaging system to expedite some complaints or reviews that affect a broader public. We expect to be current on our backlog of orders by the end of this year! To ensure that we are not another cog in the wheel, I have already shifted resources to the front end of our processes to try to resolve more complaints informally and to refer certain matters on to other dispute resolution bodies.

We cannot afford to chase every rabbit that we see!

Timeliness

Those are my initial observations about the access and privacy world in BC. You now understand more about who I am and how I perceive my task. With that out of the way, I would like to talk briefly about where I want to go on some key access issues. One of them is timeliness. As you know, I monitor the compliance of some 2700 public bodies in this province with the *BC Freedom of Information and Protection of Privacy Act* ("FIPPA"). The Act establishes a framework that requires public bodies to respond in a timely manner to requests for information.

In August, my office released its second yearly report, called *"It's About Time",* to document whether the provincial government is meeting its mandatory deadlines for responding to access requests. David Loukidelis started this "report card" process in 2008 to address chronic delays. He gave the government a failing grade in the first report card. Ministries did not meet deadlines in more than one-third of their responses to requests. That prompted the government to centralize its operations in the Information Access Operations Unit of the Ministry of Citizens' Services. The government also adopted four strategies to expedite the process—executive involvement, effective use of technology, delegation of decisions, and staff training.

Those strategies appear to have addressed the timeliness issue, and the government has made extraordinary efforts. I also want to recognize the staff of the Information Access Operations Unit for their role in securing greater respect for deadlines. Of more than 7700 access requests closed in 2009, 90 percent were completed on time, a significant improvement over the 71 percent completion rate the previous year. I intend

to continue to monitor this progress and will issue a third report in 2011, and possibly further reports if warranted.

Despite generally good news, our report revealed delays in the government's response to requests for general information from the media and political parties. I will be reviewing the government's performance in this area early next year. There was also a small but troubling increase in the number of files where not a single requested record was released. Our office is currently investigating an adequate search complaint relating to HST documents.

Routine Proactive Disclosure

While I am pleased that government made improvements in meeting deadlines, that isn't and must not be the final goal. The "It's About Time" report addresses the need to increase routine release and proactive disclosure. Earlier this year, in representations to the special committee of the Legislature reviewing the *Freedom of Information and Protection of Privacy Act*, my office called for measures to promote routine proactive disclosure. The committee endorsed this recommendation in its May 31, 2010 report.

Although I have only been here a short time, I am finding senior government officials receptive to my position on proactive disclosure. I had the opportunity to raise the matter with the Minister responsible for administering the Act, the Honourable Mary McNeil. I was encouraged by her interest and her deputy's commitment to work with our office on this important issue.

I have chosen to press for routine proactive disclosure in part because I believe we have to be realists. Public bodies will never have enough resources to deal with all the access requests as quickly as we all want. There will always be backlogs—despite the best efforts of hard-working government analysts. Responding to access requests is expensive and time-consuming for the public body involved. This is a significant concern, particularly in times of fiscal restraint. The process is often expensive and frustrating for individuals making a request as well. This undermines the whole objective of promoting trust and confidence in government through providing access to information.

Routine proactive disclosure means stepping back from the process laid out in the *Freedom of Information and Protection of Privacy Act* and embracing the spirit of the law. We should come to treat reliance on the Act as a last resort. The default position should be openness. Public bodies should open their doors without anyone having to knock on them. We have found that government is largely opening its doors as quickly as it should when somebody knocks. But it needs to take that extra step and keep the doors open most of the time.

My office is not the only one calling for greater routine openness. Less than a month ago, federal, provincial and territorial access and privacy commissioners met in Whitehorse. They issued a joint resolution calling on governments at all levels in Canada to respect open government principles. They recommended that governments

identify data sources and proactively disclose information in open, accessible and reusable formats. And they called for access to be provided free or at minimal cost.

In my current report on the timeliness of government responses to access requests, I stated that I would evaluate how ministries are doing with routine proactive disclosure in our next report. Of course, I will be making those results public—proactively!

A Word About Privacy

I intended to speak mostly about access to information today, as this is International Right to Know Week! However, we are in the midst of a rapidly unfolding communications universe! New technologies and applications—be they electronic health records, social networking sites or internet traffic management systems—these developments are constantly raising novel privacy challenges for individuals and regulators. We tweet, blog, text, sext, and upload digital bits and bites of our life with hardly a thought. The social ramifications of the digital revolution are only beginning to hit home: ICT's have huge economic and political benefits—witness the success of Obama's social media-based campaign. But the internet and mis-use of personal data can also have devastating effects We were all disgusted and dismayed by the dissemination of the gang rape video—a video that went viral with untold damage to the sixteen year old victim and her family.

Personal information is being collected, shared, analyzed, transferred and stored at an absolutely astonishing rate, and too often it is not being properly protected, either by the individuals whose information it is or by the organizations that retain it.

My office faces a daunting list of cyber-privacy challenges in both the public and private sectors. We are confronted with technologies that enable large-scale data sharing and analysis. Massive amounts of personal information contained in disparate databases held by public and private sector organizations can easily be matched and mined to produce personal profiles that may be used to affect the rights of individuals. It is especially important to address these privacy challenges proactively and meaningfully. This is critical to public trust in government and use of citizens' data.

The government's submission to the special committee reviewing FIPPA detailed government plans to share data more broadly across ministries to improve service delivery. Recent examples include the provincial Electronic Health Record project, the Prolific Offender Management Pilot and the Homelessness Intervention Project. Other governments in Canada and elsewhere are also looking for efficiencies and service improvements through data sharing and data matching. I understand the need for greater efficiency, and I applaud the use of technology for citizen-centric services. But privacy is a value and a right that must be taken into account. The threat to privacy comes from building systems for data sharing without adequate regulatory oversight and transparency. My job will be to remind government that transparency and robust oversight are critical to data sharing and data matching activities.

Public and private sector organizations must also be made to understand that they face a real risk to their reputations if they act without ensuring the public trust in their actions.

Many data sharing and matching initiatives are being undertaken by well-meaning people, but these initiatives threaten to kill privacy by a thousand small cuts. My worry is that we are building the system of linkages, each one in itself defensible and benign, without taking into account that in the longer term, under future governments, those linkages can be used for inappropriate ends.

We can learn from the experiences of other levels of government with data sharing. Ten years ago, the Federal Human Resources Minister, Jane Stewart, was forced to dismantle the government's Longitudinal Labour Force File, a set of linked databases that rightly worried Bruce Phillips, the federal privacy commissioner of the day. It was to be used for ostensibly legitimate purposes—research, policy and program analysis in government departments. However, Mr Phillips described it as a de facto citizen profile because of its comprehensiveness, lack of transparency, indefinite retention period and lack of protective legal framework.

I am also concerned about public and private sector data breaches—losses or thefts of personal information. Earlier this month, a laptop containing personal information of more than 600 patients of the Fraser Health Authority was stolen from Burnaby General Hospital. None of this personal health information was encrypted or protected by a password. In July, the newly-minted BC Lottery Corporation's online gaming site, PlayNow.com, was shut down due to a data breach that compromised scores of individuals' personal data. My office is conducting a comprehensive review of the BC Lottery Corporation's web-site. The public report will provide a blueprint for privacy and security requirements for online sites.

Conclusion

In conclusion, we live in an increasingly complex society, confronted on one hand by the risk of massive privacy intrusions that were unimagined even at the end of the last century and, on the other hand, by governments or private sector organizations that are not transparent about their work. I have only begun to open the book on the challenges facing me as Information and Privacy Commissioner. I'm asking the assistance of all of you—citizens, members of advocacy groups, academics and public servants—to help me be as effective as possible as Commissioner. I am always willing to listen to you. After all, the interests that my office is trying to serve are yours.

Please join me and the organizers of this conference in celebrating Right to Know Week!

Thank you for your attention this morning.