CHECK AGAINST DELIVERY

"Technology, Enforcement & Legislative Change News and Views from the Commissioner"

Elizabeth Denham, Information and Privacy Commissioner for B.C.

Address to the
Canadian Bar Association
May 30, 2012

Thank you for that kind introduction. I would also like to thank the Canadian Bar Association for inviting me to speak this evening. Considering that it is the first game of the Stanley Cup finals, I am extremely impressed with the turnout.

INTRODUCTION

It has been almost two years since I was appointed Information and Privacy Commissioner for British Columbia.

Hitting the one-third mark in my term is exciting because I am seeing how plans we put in motion shortly after my appointment are starting to produce results—both in improved service to the public, and moving the yardstick for access and privacy rights.

Not long after my appointment, I addressed you in the fall of 2010.

At that time, I shared my initial goals with you—to enhance the policy, public education, and information technology functions of the office—in order to better address privacy risks in the face of rapidly advancing digital and internet technologies.

Tonight I'd like to share some of the results of this work, to review some of our significant files and decisions, and end with some of the challenges I see on the horizon. A bit of a cook's tour.

NEW STAFF

I am pleased to report that it has been a CRAZY year of growth and change, but we now have more of the resources we need to provide effective oversight in BC.

The Legislature has granted my office budget increases in each of the last two fiscal years, most recently to address an increased mandate in Bill 3.

This year, we have hired three new policy analysts—doubling the size of our policy and technology group. In addition, for the first time, the office now has a Manager of Communications and Public Education.

Part of my statutory responsibility is to comment publicly on access and privacy issues. After just one year, I am seeing significant improvements to this part of my mandate.

For example, last year we increased our speaking engagements by 80%, delivering 90 presentations to public and professional audiences. We increased the numbers of op-eds and open letters, most recently, letters to the Legislative Assembly regarding Bills that I believe undermine British Columbians' access and privacy rights. The media is covering our work and commentary; interviews are up by 30% this year.

These numbers tell me that we are doing a better job of engaging the public and staying current with what is happening outside our office walls.

Technology is another critical area where my office cannot afford to fall behind. In 2010, I told you that I was going to ask the Legislature for resources to hire a technology expert.

I'm pleased to report that we were granted those monies and we used them to hire a very experienced technology investigator—Angela Swan.

Several of the investigation reports released in the last year, including a report on BC Hydro's Smart Meter program and ICBC's use of facial recognition technology benefitted greatly from having in-house technical expertise to assist with these reviews.

In addition, during our day to day work, we now have someone to consult with as we increasingly deal with privacy issues related to encryption, cloud computing, location based systems, and other technologies.

TRAINING

Added resources have allowed us to provide more training for access and privacy practitioners working in both the public and private sectors.

Last fall, Assistant Commissioner Catherine Tully and her team headed off to Vancouver to provide a full day of training to over 100 access and privacy coordinators from the lower mainland.

We also focused on training for businesses and non-profits—last Fall I co-hosted the 6th annual PIPA Conference in Vancouver.

With speakers from across Canada and the US, the conference attracted over 300 delegates, and included practical sessions on topics such as social networking background checks, cloud computing, privacy breach management, as well as a sold out privacy officer boot camp.

This year's PIPA conference will take place November 1-2 in Calgary—the conference is focused on mobile technology—Privacy on the Go!

I encourage you to consider attending—there is a call out for proposals and the information is on our website.

In addition to the private sector privacy conference—we have jointly released a guidance document, prepared with my Alberta and federal counterparts—*Getting Accountability Right with a Privacy Management Program.*

The guidance is intended to build capacity in organizations—the goal is that organizations not only walk the talk, but also have something to show for it.

Sound privacy management begins with an organizational commitment to a privacy-respectful culture, program controls including risk assessments and ongoing training.

And, businesses have to have mechanisms in place to monitor, assess and improve the program.

This blueprint for building and maintaining a privacy program is equally applicable to public bodies.

I highly recommend the paper to you and to your clients. I have already begun to use it in my enforcement work.

INVESTIGATIONS & REVIEWS

The bulk of our efforts are tied up in investigating individual complaints and access appeals.

Historically, access appeals have outnumbered privacy complaints 2 to 1. This year however, privacy complaints are up 39%. I suspect that British Columbians are more sensitized to privacy issues and aware of their rights. It will be fascinating to see if this trend continues.

This year we reported publicly on several investigations. One high profile investigation concerned whether or not the BC NDP was authorized under PIPA to collect Facebook passwords and social media information from prospective leadership candidates as part of their candidate vetting process.

This investigation was unique for two reasons. It was the first time that a Privacy Commissioner in a Canadian jurisdiction investigated a political party, and it was also the first time a data protection authority looked into the legality of collecting social media passwords, an issue that is getting quite a bit of play south of the border.

We determined that the NDP's actions failed to meet the reasonableness test in PIPA, an umbrella requirement that exists beyond consent.

An additional problem was the issue of collecting third party personal information.

By viewing prospective candidates' Facebook accounts, the BC NDP collected information about the candidates, but also personal information about the candidate's friends as well. The NDP certainly did not have the consent of these third parties.

Concurrent with the release of the investigation report, we issued guidelines on social media background checks—geared to employers in both the public and private sector.

The guidelines answer questions such as whether viewing personal information is collecting it, and whether personal information that is publicly available on the web is fair game for employers.

This is just one of several guidance documents we've posted on our website in the past year.

In order to really move the yardstick on privacy, we must focus on the big picture and conduct systemic investigations to determine whether an organization or public body is meeting their access and privacy responsibilities.

In other words, my approach increasingly will be to focus on the whole pie instead of a single slice.

A recent example of this comprehensive approach is our investigation report on ICBC's use of facial recognition technology, which I touched on earlier.

In that report, we examined whether ICBC's offer of the use of its facial recognition technology to assist police in identifying alleged Stanley Cup rioters complied with the *Freedom of Information and Protection of Privacy Act*, or FIPPA.

ICBC initially purchased the software to use internally to detect and prevent driver's license fraud by comparing an individual's facial features against its database of over four million people.

We determined that there is no authority under FIPPA for the use of ICBC's biometric database as a general tool to assist police.

ICBC must receive a warrant, subpoena or court order before using this technology to assist law enforcement with any single investigation.

This was an opportunity to consider head-on the often complex and competing values of individual privacy rights and law enforcement.

We also identified other areas where ICBC could improve its privacy management program, including the need for privacy risk assessments when implementing new technology.

ICBC cooperated fully with the investigation and has agreed to implement each of our recommendations.

JUDICIAL REVIEWS

If I might, I would like switch gears for a moment to discuss the adjudicative functions of my office.

Michael McEvoy, our senior adjudicator is with us here tonight and he and I are very pleased to say we have successfully cleared our backlog over the past two years and are turning inquiries around in efficient order.

One area of adjudication that continues to be a topic of discussion with the Bar is that of solicitor-client privilege.

The BC Supreme Court's recent decision in *School District No. 49* (*Central Coast*)[1] affirms that the Commissioner has the authority to consider solicitor-client privilege claims.

For those not familiar with it, the applicant in *School District No. 49* requested access to information regarding legal fees the school board spent on proceedings between himself and the board.

In reply, the district withheld some records, claiming solicitor client privilege. Our adjudicator ordered some of these records to be disclosed to the applicant. The School District applied for judicial review of the order.

In a decision rendered in March, Mr. Justice Butler stated that although the information at issue was "limited"[2] an assiduous applicant could deduce privileged information from it if it were disclosed.

He therefore agreed that the district properly withheld the information under the solicitor-client privilege exception.

Although the judge disagreed with our adjudicator on the specific matter of privilege of the records at issue, the judge's reasoning in the decision clearly reinforced the Commissioner's authority to deal with solicitor-client matters and distinguished *Blood Tribe* from the context of BC's access and privacy legislation.

In short, I believe the *School District No. 49* decision clarifies an area that has at times created friction between my office and public bodies that are hesitant to disclose documents over which they claim privilege.

LEGISLATIVE AMENDMENTS

As courts clarify the meaning of FIPPA, in November the Legislature passed a series of amendments to that Act.

---

[1] *School District No. 49 (Central Coast) v. British Columbia (Information and Privacy Commissioner),* 2012 BCSC 427.
[2] At ¶139.

One significant change is the requirement for public bodies to submit a Privacy Impact Assessment to the Commissioner, in advance of proceeding with a common or integrated program, or a data linking initiative.

This new oversight, as well as data linking regulations under development, is a check and balance to the new authorities for broader data sharing and data linking between public bodies and other agencies.

We are working on PIA guidance and have consulted broadly with public bodies.

One thing that did not change with the Bill 3 amendments is the restriction on trans-border data flows, which I know is a subject that many public bodies are keenly interested in.

Unlike most jurisdictions in Canada, public bodies in BC must ensure that personal information is stored and accessed only in Canada, subject to limited exceptions.

One new exception is that FIPPA now authorizes public bodies to engage the public and to promote programs using social media.

Our office continues to receive many questions about the rules for disclosing personal information outside of Canada.

To assist, we recently issued cloud-computing guidelines that specifically address the unique requirements for BC's public bodies.

HEALTH INFORMATION LEGISLATION

Now that I have spoken with you about some of the things my staff and I have been working on, I would lastly like to mention an issue that I have been spending much of my time thinking about lately—the legal framework for health information in this province.

In my view, the patchwork of legislation covering health information-overrides, and carve outs from FIPPA and PIPA, fails to provide the kind of transparency and consistency needed to both facilitate appropriate information sharing, and protect personal privacy.

There is confusion and misunderstandings on the front line, and no consistency in how health information is collected, used, disclosed and secured across the system.

This patchwork of legislation and conflicts of law will be under increasing pressure as more e-health databases come on line.

I think that the time has come to look for a different solution—time to go back to the drawing board and develop a new legislative framework—one that considers the unique needs of the sector and sets out a privacy and security framework that will work across sectors.

I have made this point in my recent letter to the Minister of Health in the context of the Bill 35, the *Pharmaceutical Services Act*.

My office is having discussions with the Ministry of Health and stakeholders, and for our part, we are preparing a white paper to set out a high-water mark for a privacy and security framework for personal health information in BC.

CONCLUSION

In conclusion, I am pleased to report that, two years in, I feel that we are on-track to achieving the goals I set for the office back in 2010.

My objective then, as it is now, is to maximize our resources by delivering practical reports and guidelines that can help build capacity and move the private and public sectors forward on access and privacy.

But before I do anything else, I'm going to enjoy some dessert. Thank you all very much for your attention this evening.