CHECK AGAINST DELIVERY

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

# THE TRANSPARENCY EFFECT

## Opening Address to the 15th Annual Privacy and Security Conference Victoria, British Columbia February 7, 2014


## Elizabeth Denham
## Information and Privacy Commissioner for BC


Thank you very much. It is nice to see so many of you here bright and early on a Friday morning before a long weekend!

Thank you to Deputy Minister John Jacobson for the kind introduction. I've certainly appreciated the working relationship my office has developed with you and Minister Andrew Wilkinson; I look forward to collaborating with you on issues "near and dear" to my heart like comprehensive privacy management for government ministries, and information management reform to ensure that decisions are properly documented and archived. A very good first step would be a rewrite of the 1936 *Document Disposal Act*!

Thanks to Greg Spievak and the team at Reboot for inviting me back for opening remarks at this important conference—you and your team always put on a great conference.

When I first started to brainstorm ideas for my speech, I looked back on the work undertaken by my office in the past year, as well as the major issues in privacy and security making headlines. And it gave me a bit of whiplash.

2013 was a HUGELY busy year. We grappled with some meaty policy issues, including a data breach affecting millions at the Ministry of Health, the roll-out of Phase 1 of the BC Services Card, and alleged information sharing between senior public servants and a political party. News headlines dealt with surveillance drones, police information checks and mass surveillance by national security agencies in Canada, the US and beyond and many other privacy issues.

Is it surprising then that dictionary.com chose "privacy" for their word of the year in 2013? Nearly everywhere we looked—journalists, citizens and civil society raised questions about privacy and security of personal data. As Privacy Commissioner, I think the increasing concern over personal privacy is a very good thing. It shows that privacy matters to citizens now more than ever, and is resilient in the face of 21st century challenges.

The major problem that I see is that our privacy laws, at the provincial and federal level, have not kept pace with technology and the new data eco systems, stretching our ability to regulate and enforce key privacy provisions. Which is why in October, when my fellow Information and Privacy Commissioners got together for our annual meeting, we called for fundamental reform of our information laws to catch up with new technologies and protect privacy rights in the years to come.

We called for mandatory breach reporting, stronger enforcement powers including penalties for non-compliance, and mandatory privacy impact assessments. If, as a modern democratic society, we want privacy to be an enduring value, we cannot allow our laws to fall behind a changing world environment.

There was a thorough and vigorous discussion about these needed reforms and how they could be achieved at a sold out special conference we hosted in last October in Vancouver—some of you were there! At that conference we feted the 20th anniversary of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), but focused heavily on how to promote and implement much needed and critical legislative reforms.

That conference was important and unique because we created a very big tent for public and private sector privacy professionals, public office holders, journalists, technologists, students, civil society and all of the commissioners from across the country to talk about reform of information rights, access and privacy.

It is clear to me that the traditional silos that have developed historically, between the public and private sector and between access and privacy are breaking down. Data knows no borders and to address the breathtaking challenges ahead, we need an approach that brings our diverse skills and experience together.

But this morning, I would like to talk about what I believe our approach to those challenges should be and what they must have at their core. In a word, the core is transparency. Transparency means openness.

It's often said that if you are nervous preparing for a speech you need only imagine your audience in their underwear! That thought is too frightening for a Friday morning and it is certainly not what I am referring to when I talk about transparency! What I am talking about relates to the fact that with respect to basic values, a free and democratic society relies on the consent, tacit or otherwise, of the governed. That includes consent for the collection and use of an ever growing amount of citizen data.

Knowledge and acceptance of this world of big data requires understanding—and you cannot have understanding without transparency.

Transparency is the process that allows citizens to understand the profound matters of privacy that are before us. Transparency also allows citizens to engage, in a meaningful way, the policy and legal choices that confront us. In short, transparency is about engaging people in society's decision making process. And in doing so, transparency of process and decision making ultimately builds the trust of citizens in the decisions that affect them.

I confess the answers to the increasingly complex questions of a data driven world can't be left to those of us who live and breathe the privacy and security world. We don't have all the answers. I know that as Privacy Commissioner I certainly don't. And, if we aspire to tackle the monumental challenges ahead, it will take our collective knowledge—and the courage on the part of decision-makers to seek out diverse views to find the right solutions.

The concept of transparency underlies the approach of my Office's work. Two of our active files right now are at the stage of public and community input.

The first concerns police information checks. Some of you might know that while a criminal record check is a report of an individual's prior convictions obtained from a national police database. In contrast, police information checks can contain a variety of details about an individual's interaction with police that have not been proven in court. For example, police information checks contain investigations that did not result in charges, charges that did not result in convictions, and information relating to suicide attempts, or mental health apprehensions.

There is an increasing trend towards the use of these broader police information checks as an employment screening tool. In order to understand the privacy

implications of these checks on British Columbians, we have invited the public, employers and other stakeholder groups to tell us about their experiences with police information checks and also their views on the impact these checks have on personal privacy. We will take these views into consideration as part of our analysis.

We've initiated a similar process for our review of the status of the BC Association of Chiefs of Police. We're currently accepting written submissions from all parties about whether my office should recommend to government that the Association be made public bodies under FIPPA, making them subject to FOI.

I believe that creating opportunities for public input and engagement in these two cases in particular, in other words—transparent will help to guide us to a more informed, publically acceptable decision. And I also believe that the global challenges of big data, surveillance and the growing number data breaches we're seeing today demand a transparency approach.

Let me address each of these challenges in turn.

There is no question that big data has arrived. We know that a massive amount of information created by and about us is mined by companies and governments seeking to create new and better tools, services and insights. The story is no different in BC, where researchers are using big data in big ways. To give just one example: Researchers at the Genomics and Networks Analysis Lab, based at Simon Fraser University, are innovating genome technologies for clinical use.

If they are successful, not only will they have devised the first ever test for personalized medicine in Canada—test to diagnose a specific form of cancer affecting 200 British Columbians each year—but they will also know the best treatment for that cancer based on that patient's unique genetic makeup. Pretty cool stuff.

We know that governments are clamouring for access to larger data sets, and to search, aggregate and cross reference discrete data to offer new insights into previously unsolvable problems.

But big data is still a fuzzy topic in the public mind.

There is a significant information gap. Citizens do not understand how data is collected, used, combined and analyzed. And there is a general concern that digital data trails, from social media interactions, phone logs, health records, and web-site visits will be collected and combined creating very real privacy intrusions. Knowing this, how do we balance the potential benefits of big data, against the personal privacy risks?

While others focus on the technical aspects, in my view, the first step is to build a bigger tent. Invite citizens and civil society into the conversation about how big data it

is going to be used, and how it will be regulated. Let's move to being more transparent.

There needs to be a real discourse about the ethical and legal underpinning of this new data ecosystem, including who is responsible to ensure that individuals and communities are not harmed by algorithms that sort us, take our data out of context or by opaque decisions based on statistical predictions. This dialogue must include what types of government-held information we are prepared to leverage in the name of big data, and what types we are not.

The BC Government is well positioned to lead this conversation.

Our province was first out of the gate with the launch of the BC Services Card almost a year ago. But before proceeding to future phases, or onboarding new services, government agreed to consult the public about the program and future possible uses of the Card. The Ministry of Technology, Innovation and Citizens' Services is to be commended for undertaking an extensive consultation with both technical experts and with citizens from different parts of the province.

I had the privilege of attending, and spoke at, two of the consultation sessions. I was impressed by the overall engagement of the group, especially the citizen participants who showed a deep understanding of the complex nuances of the Services Card file, after just a few weekends of study. We are anxiously awaiting the results of that consultation—but the fact that government was prepared to have that conversation and engage in that process is a very positive step, and I am confident that the BC government could lead a similar conversation with British Columbians about big data—an issue that needs an open and transparent policy discussion.

The benefits of an open and transparent dialogue with citizens are made crystal clear when we are presented with the alternative—a lack of information, resulting in uncertainty and an apparent loss of trust in some government institutions. Which is exactly where we are today with the other big story of 2013—mass surveillance.

Whether you think his actions are heroic or treasonous (and public opinion is divided on that issue) there is no question that Edward Snowden's revelations put privacy and transparency in the front and center of the political debate in the United States and beyond. Every day, another news story exposes a new wrinkle of the NSA's mass surveillance methods including leaky apps, a dragnet of telephone call logs, and radio wave technology. In contrast to the U.S., there have been few Snowden-like revelations in Canada to pull back the curtain on CSEC and CSIS activities that impact personal privacy. And there has been little, if any information provided to Parliament or by Canadian security agencies about these activities.

Civil society, journalists, and privacy regulators are taking action on this issue. In 2013, Open Media launched a "protect our privacy coalition," with citizen, academic, and industry partners. They are also participating in the international day of action

against dragnet surveillance on February 11, which is being called “the day we fight back.” The BC Civil Liberties Association initiated a lawsuit against CSEC, claiming its surveillance is unconstitutional, and last week interim federal Privacy Commissioner, Chantal Bernier, issued a special report with a number of recommendations, several of which are about bringing more transparency and accountability to the national security programs—recommendations I fully support.

Let me be clear. There are legitimate circumstances in which secret surveillance and intelligence gathering is necessary for national security purposes. But we don’t know the scope of these programs, the extent to which secret surveillance is taking place, and whether they exceed legal limits. Certainly last week’s allegation that CSEC tracked travellers using wi-fi at a major Canadian airport gives rise to issues of potential lawlessness. Perhaps this revelation will be the tipping point for the Canadian public!

The question raised by the wi-fi revelation, and CSECs response, makes it clear we need to debate whether CSECs mandate should include collecting the metadata of Canadians. The law is insufficiently clear. Rather than get into a mug’s game of lawyerly disputes about metadata—the antidote is transparency!

The antidote to these challenges is in pursuing more openness and transparency. Shine a light on these programs. Let’s have an informed debate about what we as a society are prepared to accept – and where the limits are – when it comes to surveillance. And this can only happen with transparency.

Transparency and open dialogue is the only way we’ll renew confidence in our public institutions. There is nothing short of our democracy at stake. Of course, I would be remiss if I didn’t mention some of the high profile data breaches we’ve seen in recent weeks and months. While many of these breaches are beyond our borders, Canadians and British Columbians are not out of reach. We have all heard about a data breach affecting Target customers where hackers gained access to 40 million credit and debit card accounts and the personal information of 70 million customers, including some British Columbians.

With increased use of smart and mobile devices for financial and commercial activities, experts expect we will see even more breaches this year. We’ve seen a consistent year over year increase in the number of data breaches voluntarily reported to our office—112 reports last year alone.

Mandatory breach reporting regimes are on the rise. Virtually every U.S. state has some form of mandatory breach reporting. It is also a requirement in many countries in Western Europe. Our neighbours across the Rockies have legislated breach reporting for the private sector, and four other provinces have similar provisions in their health information laws.

In my view, BC needs to keep up with these other jurisdictions and legislate breach reporting in the private sector, and in the wake of high profile breaches we've seen in recent times in the public sector, such as the Ministry of Health, the University of Victoria, and BC Hydro, I am considering whether mandatory breach reporting is also necessary for public bodies in this Province. To this end, we will be auditing the breach management practices of a select number of public bodies.

In the meantime, I urge you to consider how openness and transparency can help address the data breach dilemma. Being forthright about your privacy practices in the wake of a breach can be a good strategy during the fallout. Tell the truth, and tell it fast. Advise affected citizens or customers about what happened and what steps you are taking to fix the problem. Report the breach to us, and seek our assistance in dealing with the aftermath. Make your information practices public; be clear about what you collect, why, and how you will secure the information.

Having to account for your practices up front has the benefit of making you think carefully about all the ways you collect information, who you share it with and how to minimize risk of loss of this data. Implement comprehensive privacy management across your organization; it will help you mitigate risks and prevent future breaches. Investigations and audits by my office will be measuring public bodies against this standard. As we outlined in our accountability guidance, we expect public bodies and private companies to stand ready to demonstrate how their practices comply with the law.

So as you leave this conference and return to work on Monday, whether you're in the private, government or non-profit sector government or the private sector, I want you to consider the critical concept of transparency and how it can apply to the work you're doing in privacy and security.

You need to ask how you can inspire and implant openness and transparency across your organization. That means more than answering questions when a regulator comes to visit. It's about inviting the public into the conversation in a deliberate and meaningful way. I guarantee you, after the year we've had, the public will embrace the opportunity to ask questions, and offer their thoughts on where we go from here on the current domestic and international issues of personal privacy. .

Creating the opportunity for public engagement will help you make better policy and program decisions that will be met with increased trust and confidence. A little bit of sunshine goes a long way.

I appreciate your time and attention this morning and enjoy the rest of the conference!