Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO THE

BIG DATA SURVEILLANCE PLENARY RESEARCH WORKSHOP

MAY 12, 2016

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Thank you David.

I'm glad to have a chance to connect with the group before I leave for the United Kingdom.

Over the course of the next 5 years, this research will open Canadians' eyes to the realities of big data surveillance.

And I am honoured that my office is a part of this team.

I think it's critically important to have privacy regulators around the table.

Privacy Commissioners are action figures.

We investigate, consult, educate and call for legislative and policy reform.

But we need clear, practical and evidence-based research to propel us into action.

This research project will set the groundwork for regulators like me to take action on big data surveillance.

We will experience the greatest success … if we can persuade law-makers and the general public why they should care and why these issues matter.

Which is why clear and strategic communication will be so important to this project. We need to make sure our key findings make their way into the public realm.

I am disappointed to be leaving my role in this project behind.

BUT… you are in good hands with my Deputy Commissioner, Michael McEvoy. Michael will be the executive lead on this project going forward.

***

It was a stroke of genius to host this meeting on the border of the International Association of Privacy Professionals conference in Toronto.

There were 9 sessions and 20 speakers categorized as "big data" topics on the IAPP agenda – including a session on big data and privacy protection, with Colin Bennett earlier today.

Those of you who were at the conference… heard speakers talking about the need for a strong ethical and legal framework for big data -- and how innovation and privacy work together.

I am heartened to see those conversations taking place.

That said, it's a conversation being driven almost entirely by the private sector.

B.C. Examples

Which might lead one to believe that the private sector is where the big data party is happening.

But it's big business in the public sector, too.

In my view, there is a lack of **transparency** for big data activity on the part of government, and a lack of **knowledge** about government's big data activities in the public mind.

Yet it's where the most pressing policy challenges for big data surveillance lie.

Government agencies beyond law enforcement are seeking access to larger and larger data sets -- to search, aggregate and cross-reference data.

Their goal: offer new insights into previously unsolvable policy problems.

The public is, at most, superficially aware of big data's purported benefits.

But they're not aware of the big data processing that's happening behind the curtain.

They may not know, for example, that the B.C. government has a plan to build a platform for researchers to access **personal health information for research purposes**.

While still in the planning stages, the Data Innovation Centre is envisioned to be a one-stop shop where large health data sets are brought together under one roof for research purposes.

In future, the Centre aims to integrate social services, education, health and justice data.

Those planning the Centre know little about the privacy implications of **predictive uses of big data** targeting large populations – where public agencies are using client databases to target problem individuals.

POLICY QUESTIONS

All of these cases raise big picture, capital-p policy questions.

What is the **threshold for the use of big data in the public sector** – remembering that citizens have little choice but to hand over personal information in exchange for public services?

Who decides **what types of datasets** can be used for predictive analytics or pattern identification… and what are the no-go zones?

When should **personal information** be used, and when can anonymization fulfill the same purpose?

When and to whom should public agencies **disclose** their big data activities – including the people whose information it is about and the general public?

And who is assessing the **risks** of amassing large data sets in-house?

There is the risk of **breaches**… but also **legal and ethical liabilities**.

Some of you will know there is a case before the B.C. courts… where a tobacco company is requesting access to large datasets containing the health information of millions of British Columbians over a 20-year period.

They've made this request… because the provincial government is using this data in a lawsuit against big tobacco.[1]

The most recent decision saw the BC Supreme Court rule that Imperial Tobacco should get access to individual-level data from provincial databases so that it can adequately defend itself in court.

The decision is currently being appealed. And late breaking news, I sought and today succeeded in getting intervenor status in this case. The Court said I would bring a different and useful perspective to the issue before the courts. That perspective is important because the patients whose records are at issue are not before the courts.

So these are all complex questions.

And they demand proactive policy leadership to ensure that data can be used to harness innovation – **not** for mass surveillance purposes or vague policy outcomes.

The challenge facing this group – is to document and describe the real-world impacts of big data surveillance… outline where there gaps in law and oversight… and use that information to press legislators and policy-makers to fill those gaps.

Legal Challenges

There are several advantages to taking a privacy law approach to challenging big data surveillance:

The laws are **principle-based**, which gives them the flexibility to address the emergent challenges of data processing and predictive analytics.

Privacy law is a **familiar framework** for citizens and governments – giving them a lens or through which to assess the opportunities of big data surveillance and the legal uses of that data for compliance.

It provides for **independent oversight and enforcement**.

And it gives us the **language** to describe the individual impacts and broader societal harms of ubiquitous, creeping surveillance.

[1] HMTQ v. Imperial Tobacco Canada 2015 BCSC 844. Accessed April 29, 2016 via web: http://www.canlii.org/en/bc/bcsc/doc/2015/2015bcsc844/2015bcsc844.pdf

Commissioners and Data Protection Authorities around the world have been engaging experts in big data, and talking amongst themselves about how to map privacy law against big data.

And there are some mechanisms within the law that could be used to challenge certain big data activities.

In B.C.'s public sector legislation, for example – FIPPA authorizes the collection of personal information for the purposes of evaluating programs or activities of a public body.

But the threshold for collection in the law is one of "necessity." And one could ask, in what circumstances would big data be truly necessary to a program or activity?

B.C.'s private sector law has a lower threshold – a "reasonableness" standard against which private sector organizations must justify collection of personal information.

Again, such a provision could potentially allow for big data processing – but what is "reasonable"?

And what is reasonable might not be what is ethical.

Independent of the letter of the law, there are also tried-and-true policy positions Commissioners have established to defend against the growth of more traditional forms of surveillance.

These are guideposts that could be extended to challenge big data surveillance.

Canada's Commissioners have long established – through legal rulings, consultations and policy– that public agencies must first make the business case for surveillance, and clearly show that other less privacy-invasive tools could not achieve the same purpose.

If they meet this threshold, the surveillance must be limited to the identified problem. Notice must be provided. Programs must be put in place for controlling the personal information collected, ensure its secure storage and disposal, and ongoing review to ensure the program is actually addressing the problem.

Challenging big data surveillance from a privacy law perspective puts these tools in regulators hands, but also the public's hands.

Yet big data is in some ways a different beast. And it turns privacy law completely on its head.

Big data is the very definition of function creep – using personal information and data for purposes other than for which it was collected.

Opaque big data processing restricts a person's right to request their own personal information, or call to account how their information was used to make a decision affecting them – for example, withholding of a public benefit or service.

And big data fundamentally challenges the requirements of knowledge and consent.

Data-Linking Regulation

One possible model to address big data surveillance challenges **within** a privacy law framework – is British Columbia's forthcoming regulations on data-linking.

Data-linking matches and compares personal information:

- From more than one public agency
- Where the purpose of collection in at least <u>one</u> of the data sets is different from the purposes of the linking.

This is not anonymized data. This is personal information being linked, often across agencies.

Data-linking authorities were granted to public agencies in 2011 with amendments to B.C.'s FIPPA. Those new authorities were balanced with increased oversight powers for my office, notice to my office and including mandatory Privacy Impact Assessments in certain cases.

I am of the view that there should be a **principle-based** regulation governing data-linking that provides for transparency, accountability and appropriate use.

First and foremost, public agencies should have to demonstrate why they need to participate in data-linking. They need to make a clear business case for why linking <u>personal information</u> is the only way for a specific policy outcome can be achieved, instead of anonymized data or another less privacy-invasive method.

If a public agency makes the case to use data-linking, certain best practices should apply, including controls around personal identifiers – no use of SIN or personal health numbers – and retention and destruction policies for when the data is no longer needed.

In addition to the general principles, there should be specific requirements where data-linking activities could adversely affect an individual. These cases need more stringent oversight and controls, including:

- **Privacy impact assessments**
- A direct or public **notice** informing affected individuals
- **Manual verification** to make sure the right person has in fact been identified
- And annual **public reporting** on the aggregate results of data-linking activities, including how many people were affected and how many linkages made

Taking a similar approach to big data would provide certain advantages:

It would give **independent oversight** and transparency to big data initiatives and could mandate privacy impact assessments in certain cases.

It could promote **public disclosure** of big data activities of public agencies to the affected individuals – if it is a narrowing exercise – or the general public, if it is a predictive or undefined exercise.

And regular reporting to the Commissioner's office could provide opportunity to share those results with the public.

For example, New Zealand's Privacy Commissioner regularly publishes summary information about government's data-linking activities on its website… in an effort to inform the general public.

However big data is different from data linking:

With data-linking the focus is on individual privacy harms, whereas big data analysis focuses on the **collective.**

We would need to articulate how to capture the **broader societal harms** of persistent and ubiquitous big data surveillance and build that into the oversight model.

And there may be **indirect consequences or harms** associated with big data that are not the case with data-linking (i.e. being in a predictive category vs. targeted as an individual).

There is a need to reach out to academics and regulators in the human rights area.

I would be interested to hear from all of you whether you think such a model could be made to work for big data.

Oversight Challenges

Privacy law and Commissioner oversight is only one piece of the puzzle.

Big data raises human rights issues and ethical issues.

Oversight of big data surveillance will require a constellation of actors, many of whom are represented on this research team.

But we also need oversight from citizens.

I believe there needs to be a public discourse about the ethical and legal underpinning of the big 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.

I called on the provincial government to lead this conversation.

They haven’t yet taken me up on that offer.

But in the interim, the public sector is in the big data game – whether citizens know it or not.

Perhaps there is a role for this group to play… to act as a catalyst for that public dialogue and debate about big data.

Closing

I will continue to follow this project with interest in my new role in the UK.

In the meantime, I look forward to engaging with you on these topics—to further explore the questions and the dilemmas of big data surveillance – over the coming days.