Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

EDMONTON ACCESS AND PRIVACY CONFERENCE - JUNE 2011

KEYNOTE ADDRESS BY INFORMATION AND PRIVACY COMMISSIONER ELIZABETH DENHAM

DATA SHARING IN A GOV 2.0 WORLD

INTRODUCTION

How many people in the audience know what the Dewey Decimal System is?

Well, as a former archivist / librarian, I sure do.

The **Dewey Decimal System** is a proprietary method of classifying library books, developed by Melvil Dewey in 1876. Over the last 135 years, it has been modified 22 times, the most recent in 2003. The system attempts to organize **all knowledge** into **ten** main classes, which are further subdivided into ten divisions, and each division into ten sections, giving ten main classes, 100 divisions and 1000 sections.

It is a taxonomy system, meaning it categorizes a body of knowledge or collection of objects in a hierarchical manner. Each tier of the hierarchy "inherits" or possess all attributes of the one immediately above—whatever those attributes might be. When one views a hierarchy from top to bottom, the matter becomes more particular and more specific the lower one goes in the hierarchy.

So for example, a book on butterflies would be given the number 595.789. Dissecting the number: 500 for natural sciences, 90 for zoological science, 5 for "other insects" .7 for insects, .08 for Lepidoptera and .009 for butterflies for a sum total of 595.789. Very intuitive.

Some of you remember that as patrons we would look up subjects in massive card catalogues. Oh, and Mr. Dewey reviewed and classified every single book himself.

The world has changed a lot since 1876. A lot.
Developments in new technology are making it easier and easier for organizations, specific to this conversation, governments, to amass, share, store and manipulate personal information about citizens in increasingly sophisticated ways. Data sets can be manipulated and analyzed in a myriad of ways. And they can be merged into mega

databases. And it all happens in the blink of an eye. Given the unlimited storage capacity of IT systems, the potential scope of data sharing today is truly breathtaking.

The BC government has made no secret of the fact that it views the current privacy framework as a "barrier" to effective information sharing and innovation. Last year, the government made a pitch to a legislative committee reviewing the privacy rules to relax those rules to allow it to leverage technology, increase information sharing, integrate data and facilitate cross ministry data sharing of personal information to better serve citizens. The committee was not persuaded, and instead recommended that any plans to expand data sharing across government be preceded by meaningful public consultation. As of today, there has not been a public consultation process.

In fairness to the government, this issue is a tough one to publicly engage. How do you meaningfully describe the privacy risks inherent in data sharing and data matching to the average citizen?

How do you educate the public that bulk disclosures of personal information from a database of one public body to another public body, usually mean that citizens will not know how their personal information is being reconfigured, who is accessing it, for what purpose, whether it is accurate and how they can access it. This is particularly true where the transferred data is linked with personal information in other databases.

As a taxpayer, I expect government services to be delivered in the most efficient and effective manner. I expect to receive online services. I expect that any decision made about me is made with the requisite information. I expect that processes be streamlined. I expect new technology to enhance my experience when receiving government services. I expect government to utilize data for planning, program evaluation, research and customer satisfaction surveys. I expect integrated service delivery. I understand that this means proper and timely information sharing.

Let's be clear though. Efficiency and privacy is not an either/or equation. Privacy is not simply a barrier to be dismantled by government when it challenges data sharing initiatives.

In reviewing government data sharing initiatives we often hear that data sharing is about getting the right information to the right people at the right time. My job is to give a shout out for the next critical piece – **IN THE RIGHT WAY.** That is, in an open and transparent, secure and privacy protective manner.

It is my view that privacy is not a barrier to data sharing within government to achieve legitimate and important public policy goals. It is all about proportionality and ensuring that goals outweigh the privacy risks. That steps are taken to mitigate those risks to the maximum extent possible. And that public trust and confidence is maintained through openness and transparency about the data flows and proper information governance.

As with most things, it is a matter of doing it "right". How do you do it right? By making sure you don't do it wrong.

TEN COMMON MISTAKES IN DATA SHARING INITIATIVES

1. No clear objective

Basic privacy rule number one is that there must a specific purpose for the use of personal information; at or before the time the information is collected. Government must identify the purpose for the data sharing in clear and certain terms. We sometimes see data being collected because it would be "nice to have" or because "it might come in handy one day". That is not good enough. The rules are not "let's collect as much information as we can and find a use for it later." A clear public policy objective for the collection, use and disclosure of the data must be articulated. Data flows from one ministry to another are only authorized where it is necessary to achieve that public policy objective.

So that is the first key step -- a public body must be clear about why they are collecting any personal information.

2. No legal authority

Once the purpose is nailed down, the next step must be ensuring that there is legal authority for the data flows. In BC and Alberta, cross-government data sharing is permitted where it is for the purpose of a "common or integrated program or activity"

Simply having common clientele does not necessarily render programs common or integrated--children's hospitals and elementary schools for example. Or even having a common outcome does not render programs common or integrated---for example, the department of highways may paint cross walks at school crossings, but this does not make it an integrated program with the anti-bullying initiative, even though both are hoping for increased safety.

We have consistently maintained a common or integrated program must be established through a formal written instrument such as a memorandum of understanding or a project charter. It is not sufficient to just characterize the data flow itself as a common or integrated program. There must be evidence of a joint activity with defined roles and responsibilities and deliverables. This helps to ensure that the data flows are for a defined purpose and are necessary to achieve that purpose.

Examples of common or integrated programs or activities in BC that we have reviewed included the Prolific Offender Management Project and the Downtown Vancouver Community Court. Both involve the sharing of personal information across sectors (health, justice and social assistance) to inform case management decisions about individuals with a multiplicity of needs.

I wish to note, however, that in both cases these reviews by the former Commissioner occurred after the fact. When we heard about these programs we wanted to have a look at how privacy issues were being addressed. Following our reviews we made recommendations to properly structure the program and improve the privacy framework for the data flows.

3. No privacy expertise at the table

If you ask someone how much information they need to do their job, the usual answer will be much more than they really need. A critical review of the data needs with someone with privacy expertise is required in any data sharing initiative—with emphasis on the word "critical." The second key step is to determine how data should be shared, in particular what and how much data, and by what means. In order to do this, it is absolutely essential that privacy impact assessments be completed in a comprehensive and timely manner throughout the life of the data sharing project. Where this involves building a new electronic records system, such as eHealth, PIAs should be completed at all three phases – conceptual, design and implementation. They should be evergreen documents that identify privacy impacts from the very beginning -- right through to the operational changes and enhancements that occur post-implementation.

My office will soon be providing guidance to government about our expectations for privacy impact assessments. The current template used by the BC Government does not lend itself to giving us all the detail we need to conduct our review of data sharing initiatives, particularly for new large electronic record systems where there are multiple data flows. Among other things, we want to understand the security framework. We want to see the access model. We want to know whether audits are conducted on a proactive or reactive basis. The more detail the better.

4. No consideration of using de-identified information

It is truly surprising how often the possibility of achieving the objective with de-identified data is overlooked. The problem is that repositories of data are "honey pots" that all kinds of folks find tempting to get into. They don't stop to think whether stripping the data of personal identifiers can meet their needs. The issue frequently comes up in relation to data sharing for research or planning purposes. Very often, anonymized statistical information is sufficient for those purposes.

Data stewards need to become more aware that considering using de-identified data is an essential first step in any decision on disclosure. The need to know principle is so fundamental.

5. Data minimization

Another aspect of the "need to know" principle is that legal authority for data flows only extends to those data elements that are necessary for the purpose. For example, in a research project to evaluate services delivered to homeless individuals we said that it was not necessary to collect information about clients' medical diagnoses – only whether they are receiving certain types of health services. Identifying the "need to know" requires careful consideration of what data elements are in each database and separating out those not required for the purpose.

Another example where data minimization came up was with respect to a data linking project to reduce fraud. The project was to identify individuals collecting both workers' compensation and social assistance. We said that only names and dates of birth should be disclosed initially to see whether there was a "hit". Then further information about specific claims would be disclosed only in relation to those individuals where there was a hit.

6. Inadequate security framework

Under most public sector statutes, public bodies are required to make "reasonable" security arrangements. This standard of reasonableness varies depending on the sensitivity of the data and the expectations of individuals who disclose their personal information. Another factor is the number of users of the system.

In a recent investigation of BC Lotteries, we found the public would expect very robust security to protect personal information where government is involved in online gaming. Similarly, in our investigation of an electronic record system at a health authority we found a high standard was required because the system contained very sensitive personal health information.

So our finding on whether a particular security framework is reasonable will vary depending on the sensitivity of the data, the extent of access to the system and public expectations about the level of safeguards in that context.

7. Access model not granular enough

One of the best ways to protect data is to put a role-based access model in place. This means that an employee only has the level of access that is necessary to do his or her job – *i.e.* that is relevant to the tasks and services being performed. Roles need to be as specific as possible—not "male" or "female".

We are currently reviewing a new electronic case management system that combines role-based access with a transactional context. The intent is that users will only see the information they need <u>when</u> they need it. The level of access varies depending on the purpose for the transaction at the time the person is accessing it. Very impressive.

8. No privacy training and education

Why does privacy training and education always seems to be an afterthought? It is, in fact, absolutely critical in a robust privacy framework. If users do not know the "rules of the road" then what's the point? When more and more employees are accessing the same data it is easy to see why there are greater risks of privacy breaches.

For example, in a new Integrated Case Management system in BC there will be 8000 users of the system by March 2012. The majority of users will be service providers around the province. Clearly, adequate privacy training and education will be essential.

Privacy training and education is also particularly important when personal information is migrating between sectors. While there may be a strong culture of privacy in one sector (such as health) this may not be true in other sectors. The result is that very sensitive personal information collected in one sector where there is a strong culture of privacy could be exposed to significant risk when it accessed in a different sector that places less emphasis on privacy.

Confidentiality undertakings usually help emphasize the employee's obligations to protect privacy. And a critical corollary of privacy training and education is having appropriate disciplinary sanctions in place for non-compliance. A company processing health claims on behalf of the BC government has a zero tolerance policy for employees who peek at files. They have terminated nine staff in the past year. This sends an important message about employees' privacy obligations.

9. Incomplete information-sharing agreements

We all know that information-sharing agreements are not a panacea. But if done properly they do require the parties to figure out a lot of the pieces that make for a strong and accountable privacy framework – pieces such as access rights and information governance.

I would like to do more in terms of providing guidance to public bodies about the necessary elements of information-sharing agreements for cross-government data sharing. It is not enough that there is an ISA. It has to be comprehensive and cover the entire life cycle of the project right through to termination and secure destruction.

10. Lack of transparency

Government doesn't always think about the need to inform citizens about how their personal information is being collected and shared. At every opportunity, we remind government officials about notification and explain how citizens expect to be advised about how their data is being shared.

It is also important for people to have this information so that they can exercise their access to information rights and their right to request correction of personal information. Openness and transparency is always vital to maintaining public trust and confidence in how government uses the personal information of its citizens.

Generally, I find public bodies are responsive to our concerns about transparency and agree to notify individuals about how their personal information is being collected, used and disclosed in their forms or brochures or on websites.

Of course, the next step in informing the public is to give people the choice to have their personal information disclosed or not. We see this on our income tax forms where we can decide whether our demographic information can be passed on to Elections Canada.

I am advocating more of this kind of choice and control for citizens of British Columbia. One example in BC is that individuals can make a disclosure directive to restrict access to their personal health information in the provincial eHealth system. It remains to be seen, however, how effective this option will be. To date, there has been very little uptake on disclosure directives – partly because the public isn't informed well enough that this option is available.

DESIGNING DATA SHARING INITIATIVES WITH PRIVACY IN MIND

So what is in store for us?

We know for sure that the BC Government made public its desire to give themselves broader authority to share information across program and ministry boundaries to support the citizens' service needs and provide integrated service delivery

We also know that, despite the FIPPA review committee's refusal to recommend the Act be changed, this will not be a barrier if the government wants these changes badly enough.

If the government moves forward with legislative change, my response will be to push for greater transparency of government data sharing schemes, and greater independent oversight.

I will not be alone. Privacy commissioners around the world actively monitor and oversee the development and roll out of cross government data sharing, to ensure privacy is protected. These additional oversight powers take one of two forms.

The first is a model where the Commissioner actually writes rules that apply across the board specifying when and how any data sharing can occur. This is the UK model. The Information Sharing Code of practice was written by the Commissioner after broad consultation, and was presented to parliament. The Commissioner eloquently summed up the purpose of the code, which was, and I quote, to "help organizations work together to make the best use of the data they hold to deliver the highest quality of service, whilst avoiding the creation of the opaque, excessive, and insecure information systems that can generate so much public distrust."

Just the kind of things that keeps people like me up at night – data sharing systems that are “opaque, excessive and insecure”.

The UK code addresses issues of fairness and transparency, security and people’s access rights.

The second oversight model is one where each data sharing programme must be approved either by a Commissioner, or by Cabinet, and then published in a schedule to the Act. This model is under consideration in New Zealand. There, the Law Commission’s proposal is that the Privacy Commissioner must be consulted on all data sharing projects; she must provide an opinion to Cabinet. Cabinet then considers the matter, and may approve the data sharing, but only where they are satisfied that principles such as relevance and proportionality have been met.

Both approaches have merit and I will closely monitor their success. At this point, I think that a hybrid of the two approaches is the most promising for BC. An omnibus information sharing code of practice appeals to me because it educated organizations about the steps that should be taken to conduct data sharing in a privacy protective manner. I also believe specific rules should exist for those aspects of data sharing that post the greatest risks to privacy, especially access models, security specifications, and data linking.

As always, we are challenged to balance the utility goals of data sharing with the need to protect privacy in those processes. Default positions that privacy and data sharing cannot co-exist are unhelpful and do not recognize that technology can be used to protect personal information as much as it can be used to share it. Those in government who promote greater data sharing must never forget that legal liabilities and ethical obligations lie beneath each privacy risk.

As Privacy Commissioner for British Columbia, it is my job to ensure that there are no devils in the details, which means we must positively influence how data sharing initiatives are conducted within the BC government by pushing back when plans fail to demonstrate proportionality and lack mitigation strategies. It also means getting ahead of the project to review the plan, which is what the people of BC expect.

This will mean a change in the status quo, as sadly, the history of my office is replete with instances where we were the last to know about a new data sharing initiative. I believe this is changing – but hearing about data sharing through the grapevine and after the fact does not service the interests of British Columbians.

I will continue to promote and champion the best privacy framework for data sharing – one that will integrate privacy in technological designs, one which has a legislative framework outlining the rights of data subjects and the responsibilities of data suppliers and data seekers, one that is coordinated and one that is monitored and enforced by an empowered and resourced overseer. Data sharing within government is a reality and,

for the most part, serves laudable public policy goals. BUT it must be done right. Mistakes can be avoided. Public trust and confidence can be maintained.