

## **DATABASE NATION AND HEALTH PRIVACY**

– A TALK GIVEN TO THE ANNUAL MEMBERSHIP CONFERENCE OF THE BC CIVIL LIBERTIES ASSOCIATION, MARCH 2009 – by Micheal Vonn

---

Simon Davies, my colleague at Privacy International, refers to privacy advocates as the “sanitation engineers of civil liberties.” That’s because privacy is seen as uncool and not very glamorous, but boy-howdy, is it important.

Increasingly, privacy – spatial privacy, informational privacy – the entire arena of our sovereignty and control over what is properly personal -- is the key lever to all our other rights and freedoms.

But “privacy” needs a public relations make-over, in part because it has traditionally been defined as a shielding or an isolation, which, in an increasingly socially-networked culture, seems exactly the opposite of what is desirable to most people. Privacy as “isolation and seclusion” is going nowhere as a concept, especially with the Facebook generation.

That said, privacy as personal control, protection, autonomy, dignity and a fundamental human right is slowly gaining momentum. But we need to move faster: a lot faster. Because the surveillance society is very rapidly being built up around us, sometimes obviously and overtly, and sometimes silently and covertly.

Instead of doing the Sampler Platter of a vast array of current privacy issues, like police access to information held by telecommunication service providers; information-sharing between Canada and foreign governments; increasing calls for public video surveillance – etc. , I’m going to attempt something extremely radical.

I’m going to address the privacy issue that you are probably least aware of. This is a subject that clinical trials have shown is extremely likely to make people glaze over and fall into a trance. But, I’m going to try to make it come alive for you. The subject is Databases. (Work with me...)

Privacy, as an issue, really got onto the map of the public discourse by virtue of the debate over post-9/11 Security Culture. There would need to be a “re-balancing” of rights, the public was told, because of the needs of “security”. And privacy was going to take the biggest hit, but this was necessary for a greater good. Went the story.

While still a very significant force, the “Security” rationale as sweeping justification for privacy violations is increasingly subject to criticism and push-back. So the terrain of public justification has now shifted somewhat.

Like Twitter is the New Facebook, “Safety” and “Efficiency” are the new sweeping justifications for surveillance architecture. You can see this quite transparently if you know how to de-code the language

of government. Both the government of British Columbia and the feds are speaking the language of “transformational government” and “e-Government”. On the surface this looks merely like an issue of service-delivery model. But it reaches much deeper than that.

It is probably of interest to the average citizen whether or not transformational e-government results in there being no actual human beings to provide government services and we get locked into a despicable call-centre-in-Manila HELL as we attempt to communicate with and receive services from our governments. But that is not the privacy issue.

The privacy issue is that the technological and automation revolution envisioned does not work unless it is supported by giant, linked databases containing colossal and unprecedented amounts of personal and sensitive information on all citizens.

And this is the big idea that has captivated many governments – ours included.

As with most of our “innovative models” in governance and bureaucracy, this originated elsewhere. Don’t be fooled by the “Made in Canada” rhetoric; we are consistently importing our policies and practices from elsewhere. The unintended benefit this provides for those of us concerned about policies and practices is that it allows us to “see ahead” to where the policies lead, and to be able to refute the argument that the government’s good intentions will necessarily lead to good outcomes.

The model for the Database Nation is the UK. Just this week, some of the most respected information policy analysts and academics in the UK released a report on the UK’s “transformational government”. Reporting on 46 public-sector databases, the expert panel found that:

- A quarter of the databases reviewed are almost certainly illegal under human rights or data protection laws;
- A further 50% have significant problems with privacy and effectiveness and could fall foul of a legal challenge;
- Fewer than 15% of the public-databases reviewed were effective, proportionate and necessary, with a proper legal basis for any privacy intrusions;
- The benefits claimed for data-sharing are often illusory;
- That data-sharing can harm the vulnerable, not least by leading to discrimination and stigmatization; and
- The UK government spends over 16 billion pounds *per year* on information technology, yet only 30% of government IT projects succeed.

The Executive Summary notes that:

[T]he emphasis on data capture, form-filling, mechanical assessment and profiling damages professional responsibility and alienates citizens from the state. Over two-thirds of the UK population no longer trusts the government with their personal data.

None of this is particularly surprising to anyone who knows how surveillance mad the UK has become. This is, after all, a government that has a massive National DNA database that the European Court of Human Rights has found illegal for holding the DNA of over half a million people who are innocent of all crimes and have not so much as received a caution. This includes more than 39,000 children.

This is also the government that holds a national index of all children in England and centrally records their every interaction with public services and, through a program called ONSET gathers information from many sources in order to do “risk assessments” to try to predict which children will commit crimes in the future.

I can't tell you how much I wish I were making this up.

But these horrendous examples were not what first brought my attention to “transformational government” in the UK. My first point of interest is one that all Canadians need to start paying some urgent attention to: centralized electronic health records. The UK has been a very aggressive pioneer in the realm of centralized patient health information. Despite a very concerted opposition by the British Medical Association which voted for non-cooperation on centralized electronic storage of records on the grounds that the system is unnecessary, unsecure and puts patient confidentiality at serious risk, the UK went ahead and designed a system to hold tens of millions of patient records in a massive concentration.

Dr. Helen Wallace of GeneWatch has noted that the ultimate plan for the UK's electronic medical records program involves linking all patient records with the national DNA database to allow Britain to take the lead in commercializing the human genome and use of all this confidential medical information for genetic and medical research, which would be achieved by the government sharing patient data with industry. Dr. Wallace points out the centralized medical data system is estimated to cost at least 11 billion pounds more than the localized system which was originally planned and that there was no government analysis of the cost-effectiveness, impact on health, or impact on the National Health Service ever undertaken to support the plan.

Within the last month, a heroic lobbying effort by British privacy and patient advocates and doctors just barely managed to beat back (at least for the time being) a sneaky provision in The Coroners and Justice Bill that would have allowed ministers to share any data – including genetic information and citizens' personal medical information – with *anyone*, public or private sector, domestic or foreign, without people's knowledge, let alone consent.

Other than to give you the heebie-jeebies, why am I telling you this?

Well. Many jurisdictions in Canada have already launched centralized electronic databases of medical information and BC's “e-health” launch is only a few weeks away.

Last spring, a small but insanely dogged group of privacy advocates miraculously managed to get the province's new "e-health" bill to include a requirement for some patient controls over who gets access to our medical information. And just so you are clear about the scope of the access, the plan is ultimately for a Pan-Canadian e-health record system. Canada Health InfoWay -- which is an organization which receives a lot of money from the federal government, but is not "government" for the purposes of access to information laws, so is completely unaccountable to citizens -- exists solely to promote centralized electronic health records, first provincially and ultimately linked so as to be accessible nation-wide.

The informal coalition of privacy-concerned organizations that took on the e-health bill lobbied for the inclusion of a right to make a disclosure directive to limit access to information about us on the provincial e-health system. We are now waiting to find out if this small victory will amount to anything at all.

The reason for the pessimism is Alberta.

Or rather, the cautionary tale that is Alberta.

Up until recently, the e-health system in Alberta required consideration of patients' wishes. That turned out to be a big hassle. So having already acquired the means of accessing most of the information, the government just rescinded any rights of the patient to attempt to direct who gets to see it.

And then they went further. The giant hoovering of private medical data wasn't just going to harvest information on hospital admissions, lab tests, diagnostic imaging, pharmacy use, etc. -- all which have very serious privacy implications. Alberta's Bill 42 would see the government of Alberta also harvesting patient information directly out of their physicians' offices, regardless of whether the patient consents to their information being forwarded to government databases. And for the physician who attempted to protect patient information by not disclosing it to the government? Fines ranging from \$200,000 to \$500,000.

This is very, very important for us to understand.

Alberta, I assure you, started out promising the kinds of patient confidentiality protections that we are being promised right now. As far as we can tell from experiences, both nationally and internationally, such promises generally prove worthless and are either quickly or incrementally eroded.

Which is why it is too early yet to be all fired-up excited that we have legislation that requires patient disclosure directives. What that actually amounts to and how long it lasts is anyone's guess at this point. We'll start to have an inkling when the regulations come out in June.

And what, incidentally, do we get in exchange for this massive Privacy-Chernobyl-Waiting-to-Happen that we, as a country, are investing billions in?

Well, that's an interesting question. I've asked that question of government repeatedly. And all I get are slogans and glossy brochures from IT firms that stand to make piles of cash from the venture. Those

who have searched for real evidence and hard data on the safety and efficiency improvements generated by giant databases of centralized medical records can tell you there really isn't any: a lot of "projections" – virtually no proof.

And watch out for the "stupid debate" on centralized electronic health records, the one where e-health proponents call you Luddite and rattle-off a hymn of praise for the many benefits of computers. Contrary to the ridiculous slander that we are constantly subjected to, health privacy advocates do not demand that all doctors write out their prescriptions with a quill and do their calculations on an abacus. Computers are very, very useful things. And we have no problems conceding that there are many benefits of computerization in health care.

But that's not what we are talking about. We are talking about a giant longitudinal database of the most sensitive citizen health information being made potentially accessible to tens of thousands of people.

Everyone agrees that it is important, for example that an urgent specialist's report get into the hands of your GP quickly. Computers will help you do that. But you don't need a giant longitudinal database to do that.

As the UK report on the Database State points out:

[T]here is a developing consensus among medical practitioners that for safety, privacy and system engineering reasons, we need to go back from the shared-record model to the traditional model of provider-specific records plus a messaging framework that will enable data to be passed from one provider to another when it is appropriate.

In other words, the data should be *pushed* from one health care provider to another. Not *pulled* from every health care provider into a massive database.

Why are we not building the right model?

Well, there's at least two reasons that I know of and they're both terrible.

The first is the IT industry-fuelled PR campaign of electronic health records as a cost-saver and therefore the savior of the health care system. Industry Canada, in some inadvertently revealing documents, discussed the wide-spread *perception* that e-health could be a cost-saver as the main driver of that industry's continued growth.

Governments are very, very keen to be *seen* to be doing something to safeguard healthcare. And they've latched on to e-health in spite of the growing evidence of its colossal costs and failure to deliver the promised benefits.

The second reason is that this is ultimately the thin edge of the wedge. BC's electronic health information infrastructure is meant to anchor an integration project called the Information Access Layer, which includes the Integrated Case Management Project. This is a massive information-sharing project meant to encompass the entirety of social services in British Columbia and to link information about us

from the Ministries of Employment and Income Assistance, Children and Family Development, Health, Education, Justice and the private sectors contractors for all of the above. The government has already issued an RFP, (a Request for Proposals) for this project.

This comes straight out of the playbook of Database Nation and holds all of the dangers inherent in that vision.

If you are a young mother who has some involvement with the Ministry of Children and Families, are you going to seek help for post-partum depression knowing full well that your confidential medical information is going straight to the Ministry? How long will it be at this rate before we are profiling our 'at risk' children for future criminality?

Privacy, we are increasingly being told is the enemy of safety and the enemy of protecting children and other vulnerable people. Except within the most narrowly-drawn of exceptions, this is an invidious lie.

Privacy is the traditional friend of healthcare, friend of social services and the friend of medical research.

The paradigm shift we are seeing right now is nothing less than a complete remodeling of the relationship between the citizen and the state and its practical effects are guaranteed to be disastrous.

And don't even get me started on the fatuous and technologically moronic promises that the databases will be secure. There are instructive lessons yet again from the UK, which has even had to stop *pretending* that it can protect data in the face of tens of millions of records lost or compromised and, just recently, the Prime Minister's own medical data illegally accessed.

As Ross Anderson, Professor of Security Engineering at Cambridge wrote in the Feb. 2008 edition of "The Economist":

Patient data held at a GP practice may be vulnerable to a security lapse on the premises, but the damage will be limited. You can have security, or functionality, or scale -- you can even have any two of these. But you can't have all three, and the government will eventually be forced to admit this. In the meantime, billions of pounds are being wasted on gigantic systems projects that usually don't work and that place citizens' privacy and safety at risk when they do.

There is much, much more to say on this subject.

Please stay tuned to our website and newsletter for information on the campaign to educate British Columbians about electronic health information systems and some practical tools for safeguarding your health information.