Citizens @ the Fringes: How e-Government Initiatives in British Columbia Are Displacing Citizens' Rights and Participation

MICHEAL VONN*

> '[B]ig data is like big sugar. The more ubiquitous, abundant, pleasurable, efficient and profitable it is, the more we want it. And sometimes, the more we want it, the more blinded we are by its consequences.
>
> We stand at the precipice of what one might call the 'late onset diabetes' of the information age. And we should be doing much more to prevent it.'[1]

Introduction

Edward Snowden's revelations shone a global spotlight on national security surveillance networks and how they tap into private sector internet and telecommunications services. Other global surveillance trends, such as the movement to aggregate and apply data analytics to citizens' personal information collected and used in the provision of ordinary government services, are comparatively little known.

The movement to transform the delivery of public services through the use of information technology has been highly controversial from the perspectives of privacy and human rights advocates.[2] Branded under many monikers, including 'e-government', 'horizontal government', 'linked-up government', and 'transformational

* Policy Director of the British Columbia Civil Liberties Association, Advisory Board Member of Privacy International.

[1] Ian Kerr, (giving evidence) Parliament of Canada, Standing Committee on Access to Information, Privacy and Ethics (HC Issue No 45, 12 June 2012).

[2] See, e.g., Ross Anderson and others, *Database State: A Report Commissioned by the Joseph Rowntree Reform Trust Ltd* (Joseph Rowntree Reform Trust Ltd 2009).

government', these reforms have also been severely criticized due to costly systems failures.[3]

However, the promises of 'open government', data analytics, and 'the Big Data Revolution', are being used to re-varnish the reputation of e-government. In British Columbia (BC), the e-government initiative has been dubbed 'Citizens @ The Centre: B.C. Government 2.0'. Its stated aim is to empower citizens both by transforming government services through freer sharing of citizens' information, and also by supporting citizens' digital engagement, by using, for example, data analytics on open government data and increasing dialogue and participation with government through online means.[4] In essence, it is a general freeing of data: government freer to use citizens' data and citizens' freer to use government's data. Cost-savings and actual money-making are meant to flow from this arrangement. At the October 10-11, 2013 conference 'Privacy and Access 20/20: A New Vision for Information Rights', Andrew Wilkinson, British Columbia's Minister of Technology, Innovation and Citizens' Services, spoke confidently about the government's on-going commitment to mobilizing data sets available to the government as tools of economic development.

This paper is a brief overview of some of the legal and policy issues raised by the e-government reforms in British Columbia. It argues that, contrary to the stated aims of the programme, both citizens' rights and options for meaningful participation and engagement are being eroded by these developments.

[3] See Paul Christopher Webster, 'Centralized, Nationwide Electronic Health Records Schemes Under Assault' (2011) 183(15) CMAJ E1105; citing the UK Public Administration Select Committee, *Government and IT—'A Recipe for Rip-Offs': Time for a New Approach* (HC 2010-11, 715-I) which 'concluded that the government essentially does not know how to develop information technology systems or judiciously shop for either hardware or software. "IT procurement has too often resulted in late, over budget IT systems that are not fit for purpose"'.

[4] BC Public Service, 'Citizens @ the Centre: B.C. Government 2.0: A Transformation and Technology Strategy for the BC Public Service' (*Government of British Columbia*) <http://www.gov.bc.ca/citz/citizens_engagement/gov20.pdf> accessed 2 September 2014.

British Columbia: The Best Place on Earth (to Realize the Promise of 'Big Data')

In 2005, the government of British Columbia launched its 'Best Place on Earth' slogan and set out its 'Five Great Goals for a Golden Decade'. The slogan did not last long,[5] but at least some of the 'Great Goals' and their principles remained intact, including the government's belief that 'a citizen-centred service approach should underpin the design and delivery of public services.'[6]

The Integrated Case Management (ICM) system for social services provision was meant to lay the groundwork for transforming service delivery in the social services sector and wider all-sector reform. The government's stated rationales for 'leveraging information sharing' included citizens' demands for convenient, high quality and accessible services and the need to do more with less. In its submission to the Special Committee reviewing the provincial public sector privacy and information laws, the government stated that:

> This change in approach to service delivery includes an increasing move to horizontal and integrated program delivery models to more effectively serve citizens and achieve better outcomes for clients. The transformation of government service delivery is also a response to demographic pressures requiring government to deliver quality services with fewer staff by implementing innovative programs and leveraging information technology.[7]

---

[5] Bob Mackin, 'BC No Longer Calls Self "Best Place on Earth" (*The Tyee*, 4 October 2011) <http://thetyee.ca/Mediacheck/2011/10/04/BC-Best-Place-On-Earth> accessed 2 September 2014.

[6] Gordon Campbell, 'Letter from the Premier: Towards a Golden Decade. Strategic Plan Update 2005/06 – 2007/08' (*Government of British Columbia*, September 2005) <www.bcbudget.gov.bc.ca/2005_Sept_Update/stplan/default.htm> accessed 2 September 2014.

[7] Government of British Columbia, 'Government Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act' (*Government of British Columbia*, 15 March 2010) ii <www.leg.bc.ca/cmt/39thparl/session-2/foi/submissions/organizations/BC_Government.pdf> accessed 2 September 2014.

The government also called for amendments to the privacy legislation in addressing 'barriers' to better service delivery:

> British Columbia is not alone in addressing issues related to the effectiveness of information sharing to provide better services to citizens. Many jurisdictions, including commonwealth countries and European nations have recently initiated legislative amendment and policy reform processes to facilitate personal information flows designed to improve the effectiveness and efficiency of government services and service delivery to citizens.[8]

But opinions varied as to whether these reforms needed to be sped up or slowed down. At the same time that the government was arguing for increased ability to share personal information within government, the Information and Privacy Commissioner for British Columbia was calling for a moratorium on data sharing initiatives 'until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing.'[9]

And the controversy extended beyond personal information held within government. The ICM is populated by data from various government ministries and also, from their private sector contractors, including community-based charities and non-profits delivering health and counselling services, and shelter and emergency services for those fleeing family violence. As pointed out in a seminal report on the ICM prepared by the BC Freedom of Information and Privacy Association, the new model takes individuals' personal data out of the private sector and commandeers it for government databases:

> ICM has the potential to transform [the culture of the independent community service sector] from one where helping people in distress is paramount to one where

[8] ibid.

[9] Office of the Information and Privacy Commissioner of British Columbia, 'Submission of the A/Information and Privacy Commissioner to the Special Committee to Review the Freedom of Information and Protection of Privacy Act' (*Information and Privacy Commissioner of British Columbia*, 15 March 2010) 12 <http://fipa.bc.ca/library/REVIEW_OF_BC_FOIPP_ACT-2009-2010/OIPC%20FIPPA_Rvw_Submission(15Mar2010).pdf> accessed 2 September 2014.

> organizations are de facto agents of the state, with the function of funnelling their clients' most intimate personal information to the provincial bureaucracy.[10]

This is not an exclusive feature of the ICM. Data transfer from private to public sector is occurring in all spheres where e-government initiatives span private contractors, including healthcare. In BC, health information administrators have the power under legislation to collect identifiable patient information from both public and private sector sources.

> One of the critical features of the *E-health Act* is the authorization for a massive transfer of private sector data, which is governed by the *Personal Information Protection Act*[11] ('PIPA') into the government's [Health Information Banks], which are governed by the *Freedom of Information and Protection of Privacy Act*[12] ('FOIPPA'). In British Columbia, the first stage in this massive data transfer into government databases is taking our personal health information from public and private-sector medical laboratories and putting it into the first designated HIB, which is the Patient Lab Information System.[13]

The implications for individuals' privacy are that their personal information moves from a high level of legislated privacy protection to a low level of legislated privacy protection. From one in which, subject to some exceptions (PIPA s. 12), consent is required for disclosure (PIPA s. 6) and the private sector actor must consider 'what a reasonable person would consider appropriate in the circumstances' (PIPA s. 4(1)), to a legislative scheme that does not

---

[10] British Columbia Freedom of Information and Privacy Association (BC FIPA), 'Culture of Care… or Culture of Surveillance? Personal Privacy and the BC Government's Integrated Case Management System: Legal, Ethical and Procedural Implications for Independent Community Service Organizations' (BC FIPA, March 2010) <https://fipa.bc.ca/wordpress/wp-content/uploads/2014/03/Culture_of_Care_or_Culture_of_Surveillance_March_2010.pdf> accessed 2 September 2014.

[11] 2003 (Canada).

[12] 1990 (Canada).

[13] Micheal Vonn, 'The Real Impact of e-Health' (2009) 67 The Advocate 753, 753-754.

require consent for use or disclosures and allows for (increasingly) broad uses and disclosures of personal data throughout government.

Additionally, this significant downgrading of privacy rights and loss of the ability to control the disclosure of personal information happens generally without notice to the individual. For example, the privacy policy of the Canadian Medical Association states that physicians have an obligation to inform patients that when the patient's information flows into an electronic health record system the physician cannot control access or guarantee confidentiality,[14] however, one would be hard pressed to find the patient in Canada who has been warned that this is so.

It is important to note that the issue is not that information is held electronically. The issue is centralization and transfer of control. To the citizen receiving services it may initially look no different—a service provider is using a computer to call up the file containing their personal information. But in one scenario, the service provider has control of the data and the obligation, with few exceptions, not to disclose it without consent. In the other scenario, the government has control of the data, which it centralizes and makes available through thousands of access points on the basis of access permissions decided by the government, not the citizen or the service provider.

In the case of private sector medical laboratories, this data transfer is authorized by the E-health (Personal Health Information Access and Protection of Privacy) Act 2008 (Canada). But in the case of social services contractors, the question of legal authority is highly dubious. Private sector contractors are governed by PIPA, but many of their government service contracts provide that the public sector privacy legislation applies to their clients' personal information. Service providers that receive needed funds from government contracts are in a poor negotiating position with respect to such problematic contract provisions. Although there is a strong legal argument that you cannot 'contract out of statute', the reality is that very few organizations can afford to jeopardize needed government contracts.

[14] Canadian Medical Association, 'Principles for the Protection of Patient Personal Health Information' (*Canadian Medical Association*, 2011) <http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf> accessed 2 September 2014.

Thus, there is little actual challenge on the legal issue, despite the recommendations of the BC FIPA report:

> The primary legal obligations of ICSOs [independent community service organizations] as defined under PIPA cannot be circumvented in consequence of actions or decisions by any external source, including government. ICSOs contracted to perform work for a government are not 'agents' of the crown, and the [FOIPPA] requirements faced by government are not somehow transferable to ICSOs in such a way that they vitiate or obviate PIPA requirements. For government to attempt to impose [FOIPPA] requirements onto community organizations through contract language is legally problematic, especially if and where the government seeks to impose [FOIPPA] requirements as a means of 'trumping' and thus avoiding the PIPA requirements to which the organizations are subject.[15]

This is not to say that all private sector contractors are failing to defend the privacy rights of their clients and patients. The research undertaken for BC FIPA's report showed that confidentiality was identified as 'very important' by all of the surveyed service providers.[16] And the serious ramifications of failures to maintain confidentiality have been the focus of concerted advocacy in some sectors, most pointedly in the transition house sector.

> Because of the clear connection between data safety and the safety of women and children threatened by violence, transition houses and counselling programs have a long and important history of paper-based, client-controlled, data minimized files and community coordination to ensure effective referrals without data centralization. This critical safety work will be undermined by forced disclosures that are integrated into a vast database system accessible from thousands of access points. Effective safety plans for women and children are simply not possible within a system that mandates disclosures that cannot be

[15] BC FIPA (n 10) 45.

[16] ibid 22.

> safeguarded against abusers' networks. Service providers are already tracking cases in which the ICM will jeopardize the safety of women and children fleeing violence. It is clear that no responsible government would allow this type of wide-spread dissemination of data for those in the witness protection program, and yet this is the system that will be mandated for women and children fleeing violence.[17]

But advocacy efforts have had very limited success and e-government data centralization programmes are continuing to roll out with exceedingly little attention paid to the evidence that there are serious harms to the course being navigated. See for example, the entirely predictable results of research from the BC Centre for Disease Control showing that 31% of patients would be less likely to test for sexually transmitted infections and HIV if that information were made available as part of the provincial electronic health records system.[18]

If private sector community contractors are ill-resourced to challenge the government over contractual provisions that affect the privacy of their clients, individual clients and patients are even less resourced to challenge their diminishing privacy rights under e-government data centralization and dissemination. Legal challenges are prohibitively costly and privacy protections under the existing provincial privacy legislation are increasingly limited, as a series of amendments have been enacted to facilitate greater data dissemination without consent, and thus yesterday's privacy act violation becomes today's privacy act compliance.[19]

---

[17] Letter from BCCLA Policy Director Micheal Vonn to Representative for Children and Youth, Province of British Columbia, Mary Ellen Turpel-Lafond (1 December 2010) (on file with author).

[18] Darlene Taylor, 'Client Perspectives on Electronic Health Records in a BCCDC STI Clinic' (*Smart Sex Resource*, 13 February 2014); See also, Wendy Armstrong, 'Getting Lost in Doing Good: A Societal Reality Check' in Colleen M Flood (ed) *Data Data Everywhere: Access and Accountability?* (McGill-Queens University Press 2011).

[19] BC FIPA, 'Piecemeal Repeal of FIPPA?' (*BC FIPA*, 20 June 2012) <https://fipa.bc.ca/piecemeal-repeal-of-fippa-4/> accessed 21 November 2014.

While statutory privacy rights have repeatedly been affirmed as enjoying a 'quasi-constitutional' status,[20] it is difficult to understand how this heightened status actually manifests in terms of rights protections. Even before the many enabling amendments to weaken statutory privacy protections, there were calls (unheeded) to go beyond statute and have the BC government draft a constitutional question regarding the ICM system and refer the matter to the BC Supreme Court, pursuant to the Constitutional Question Act[21] for an opinion on its constitutionality.[22]

In Canada there is a constitutional right to privacy that is protected by sections 7 and 8 of the Canadian Charter of Rights and Freedoms,[23] which provide that:

> 7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.
>
> 8 Everyone has the right to be secure against unreasonable search or seizure.

These rights are 'subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society', as provided in section 1 of the Charter.

The Supreme Court of Canada has long affirmed that the Charter protects 'a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.'[24]

In a constitutional case with respect to an e-government programme, the issue would doubtless turn on the section 1 analysis, which is the government's justifications for the programme and the court's

---

[20] See, e.g., *Lavigne v Canada (Office of the Commissioner of Official Languages)* 2002 SCC 53, para 24.

[21] RSBC 1996, ch 68.

[22] BC FIPA (n 10) 44.

[23] Constitution Act 1982 (Canada).

[24] *R v Plant* [1993] 3 SCR 281, 293.

weighing of the proper balance between achieving the legitimate aims of the government and protecting Charter rights.[25]

The evidence that would be marshalled for a constitutional case would be instructive, as the aims of e-government programmes are typically framed in broad terms with very little specificity—'responsiveness', 'effectiveness', 'engagement', etc. Many of these claims are contested. This includes seemingly 'intuitive' benefits such as the claim that shared databases and economies of scale automatically increase 'efficiency'. This is not proving to be so in many sectors from banking[26] to health services.[27]

In addition to the debate about whether the assumptions of the model itself are supported by evidence, concerns continue to grow with respect to huge financial costs and the detrimental effects of failed attempts to implement workable systems and maintain appropriate security.[28]

While the broader debate continues on the question of whether vast centralized data systems are a desirable and/or workable model for government service delivery, BC's e-government developments have recently spawned new legal questions and privacy challenges.

[25] *Alberta v Hutterian Brethern of Wilson Colony* [2009] SCC 37.

[26] For instance, see Robert R Kerton, 'Can Consumer Bank on Mergers?' (*Policy Options*, March 2003) <http://policyoptions.irpp.org/issues/bank-mergers/can-consumers-bank-on-mergers> accessed 2 September 2014: 'In fact, much evidence exists from studies on bank mergers elsewhere, to show that, over a certain size level, economies of scale are either absent or unimportant.'

[27] In this context, see Trisha Greenhalgh and others, *The Devil's in the Detail: Final Report of the Independent Evaluation of the Summary Care Record and HealthSpace Programmes* (University College London 2010) 11: 'Thus, in contrast to expectations expressed by many stakeholders that the [Summary Care Record] would bring clear, easily defined and readily measurable benefits, we found that when benefits occurred, they were subtle, hard to articulate and difficult to isolate out from other aspects of the consultation.'

[28] See Kate Milberry and Christopher Parsons, 'A National ID Card by Stealth? The BC Services Card: Privacy Risks, Opportunities and Alternatives' (*BCCLA*, 2013) 26 <http://bccla.org/wp-content/uploads/2013/10/2013-National-ID-Card-by-Stealth.pdf> accessed 2 September 2014.

Tokenization as the Proposed Solution for Off-Shoring Data Systems

British Columbia's public sector privacy legislation provides that a public body 'must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada' (FOIPPA, s. 30.1). This restriction, which prevents government from using foreign-based cloud applications for personal information, is meant to safeguard data against third-party disclosure, and in particular, against access by foreign governments and their agents through means like the USA PATRIOT Act.[29] The BC government has recently proposed using a process called tokenization to de-identify data so that it no longer constitutes 'personal information' for the purposes of FOIPPA, thus allowing government to store databases containing British Columbians' personal information outside of Canada.

In an internal memorandum, the Associate Deputy Minister and Government Chief Information Officer of BC reported that a contract had been signed with a vendor for ministries to use this 'new solution' to address the 'data-residency' issue. The memorandum states that:

> While the signing of this contract is a significant step forward in providing cost effective application hosting options for ministries, it does not mean that ministries may freely implement this service without appropriate privacy standards and security reviews. The use of foreign-based services are still subject to the legislative and policy requirements for a Privacy Impact Assessment and Security Threat and Risk Assessment, and the configuration of these applications and the means through which the residency-based requirements of FOIPPA are met must still be addressed.[30]

[29] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

[30] Memorandum prepared by Bette-Jo Hughes, Associate Deputy Minister and Government Chief Information Officer, Province of British Columbia to Ministry Assistant Deputy Ministers and Ministry Chief Information Officers, regarding Data Residency and Tokenization (2 October 2013).

Some guidance by the Information and Privacy Commissioner for British Columbia was issued with respect to the government's proposal.

> Tokenization is a process whereby information in a record is replaced by a randomly-generated token and the token acts as placeholder for the information in the stored record. A token generally consists of a randomly-generated value (whether alphabetical, numerical, symbol or other value). A log of the replaced information is maintained that links the information to the token. This log, or 'crosswalk table', is used to replace the token with the original information in order to access that information.
>
> …
>
> Based on the information that government has provided to my Office, it appears to me that tokenized information is not personal information if the following two key assumptions are met:
>
> 1. The information stored outside of Canada is adequately tokenized such that it is not re-identifiable without use of the crosswalk table; and
> 2. The crosswalk table is stored in Canada and is not accessible outside of Canada. [31]

As acknowledged by the Commissioner, much turns on the 'adequacy' of the tokenization. In the programme that will pilot this new approach, which is a programme for adults with developmental disabilities, the government is proposing only to tokenize information that it believes has the potential to identify an individual. The Commissioner's view is that:

> Where government chooses to only partially tokenize records stored outside of Canada, the un-tokenized

<http://docs.openinfo.gov.bc.ca/D11384614A_Response_Package_CTZ-2014-00009.PDF> accessed 2 September 2014.

[31] Public Comment by Elizabeth Denham, Information and Privacy Commissioner for British Columbia, 'Updated Guidance on the Storage of Information Outside of Canada by Public Bodies' (16 June 2014) <www.oipc.bc.ca/news-events/public-comment.aspx> accessed 2 September 2014.

> information must be analysed in advance to ensure that it is not capable of re-identification. While the un-tokenized information itself may not be sufficient to enable identification, it is possible that, depending on the nature of the information, indirect identifiers may be combined such that the individual that the information is about may be identified. [32]

The Commissioner states that her office is committed to working with 'an expert in re-identification' in order to review these specific concerns. The Commissioner also notes the 'far-reaching implications' of any unauthorized access to the crosswalk table which is the key to re-identification of the partially tokenized records.[33]

It is outside the scope of this paper to discuss the security and re-identification potential of mixed tokenized and un-tokenized fields in a given record or the legal and physical security of a tokenization crosswalk table. Critically, such discussions are beyond the scope of anyone who is not an expert in the field—i.e., the kind of person who the Office of the Information and Privacy Commissioner says that it will need to work with in order to review specific concerns. This raises the question: how are such specific concerns to be raised? How are individuals to hold public bodies accountable for their information practices in this regard? While the Information and Privacy Commissioner has a range of powers, including the power to conduct investigations and audits (FOIPPA, s. 42(1)(a)) and to hold inquiries (s. 56), much of the work of the office is generated from individuals' complaints which the Commissioner may investigate (s. 42(2)). And individuals are increasingly devoid of the information that would make them capable of exercising their rights under the Act.

As an example, the pilot programme for tokenization, Services to Adults with Developmental Disabilities (STADD), uses an integrated service delivery model involving different ministries and private sector contractors to address complex care needs. One of the aims of the integrated service model is 'enhanced data capture, management

[32] ibid 4.

[33] ibid 6.

and sharing.'[34] The STADD: Integrated Service Delivery Model report of 2013 acknowledges that '[i]ssues regarding data collection, storage, retrieval, and sharing require definition, clarification, and solution.'[35] Many of the service providers involved in the programme work with the Integrated Case Management (ICM) system, although strategic decisions about the use of ICM by the involved service providers had not been made at the time of the report[36] and the discussion of launching the programme for 'early implementation sites' states that this launch 'would not use ICM system platform, would have to be small and manageable (e.g. on Excel) and incorporated later.'[37] A document prepared for prospective contractors does not describe the data integration tool(s) except as a 'centrally accessible, standardized and comprehensive Common Assessment Platform.'[38]

As is evident, a client of this programme, or her guardian, would have considerable difficulty just determining who held and had access to the broad array of their sensitive health, education and family information that is shared within this particular service network. The public bodies involved have a range of obligations in relation to safeguarding personal data, but especially with regards to obligations like the provision of 'reasonable security' (FOIPPA, s. 30) and notification of unauthorized disclosure (s. 30.5), the possibility that a complaints-driven compliance model can ensure rights protection is increasingly faint. The system is too complex and the individual whose personal information is at issue cannot meaningfully see into the system, and if they could, they would not

[34] Government of British Columbia, 'Services to Adults with Developmental Disabilities: Integrated Service Delivery Model Version 1.0 Draft for Discussion' (*Government of British Columbia*, April 2013) 4 <www2.gov.bc.ca/assets/gov/topic/D53478E6C207D4FEEE8B245A3994CA26/integrated_service_delivery_model__report/service_delivery_model.pdf> accessed 2 September 2014.

[35] ibid 28.

[36] ibid 31.

[37] ibid 71.

[38] British Columbia Ministry of Social Development and Social Innovation, 'Services to Adults with Developmental Disabilities (STADD) Integrated Network Support Model—Early Implementation Sites Request for Expression of Interest' (*Government of British Columbia*, July 2013) <www.sd.gov.bc.ca/pwd/docs/isst-eis-eoi.pdf> accessed 2 September 2014.

have the requisite expertise to make an assessment (i.e. on whether a given level of tokenization constitutes de facto de-identification). Increasingly complex data integration and security processes like tokenization insulate data systems from the complaints of individuals and restricts oversight to specialists hired by commissioners' offices. Citizens have a legislative right to lodge a complaint, but increasingly, they have little practical ability to do so.

Using ID Management as a Whip to Further Centralization

As described by Minister Wilkinson at the 20/20 conference, a new BC Services Card is envisioned by the government as anchoring its evolving 'digital service delivery environment.' The Services Card is a new provincial ID that replaces expiring drivers' licenses and can be combined with the card that provides access to health services. BC is pioneering the use of a federated identity management system that is meant to be interoperable with the federal system and throughout the provincial system, as well as working for both commercial and e-commerce transactions.

The BC Services Card is a key component of the Province's e-government vision. There are indications that citizens are concerned about many aspects of the Services Card. The report of the BC Services Card User Panel (35 randomly selected British Columbians who spent more than 40 hours learning about the Services Card and drafting recommendations) repeatedly cited privacy and surveillance concerns, calling for 'strong, ongoing and independent oversight to safeguard the privacy of BC residents and to ensure that the best available data storage and management practices are consistently applied across government' and endorsed explicit (not implied) consent for transferring data between government agencies.[39]

At the same time that the Services Card was being introduced, the government was scrambling to fix another key component of the e-government programme. The province was forced to replace a

[39] British Columbia Ministry of Technology, Innovation and Citizens' Services, 'Recommendations from the B.C. Services Card User Panel' (*Government of British Columbia*, December 2013) <www.gov.bc.ca/citz/down/DigitalServicesConsultation_appendix2.pdf> accessed 2 September 2014.

province-wide student information system (BCeSIS) that was 'not meeting the business, technical or operational needs of BC and is not a viable future alternative.' [40] Almost $100 million had been spent on the unworkable system, which is being replaced with a new, substantially similar, provincial system called MyEducation BC.

Education Ministry officials confirmed that '[school districts] are not required to use a provincially mandated solution' and the School District of Saanich decided against using MyEducation BC. It invested about $1.5 million to develop an open-source student information system, contending that their made-in-BC product would be responsive to the needs of educators, because the users were actually building the software, which would be continually updated and still provide huge cost savings.[41] Additionally, Saanich's openStudent system would collect 'only a fraction' of the data that would be captured by the government's system:

> While developing openStudent, Ferrie [IT director for the Saanich School District] said they analysed the information BCeSIS was designed to capture and found that over 70 percent seemed superfluous to BC's educators and education system, so they built openStudent 'leaner'. [42]

But the School District of Saanich was compelled to abandon openStudent after Ministry of Education officials warned that the school district would have to make openStudent compatible with the new BC Services Card at a cost of millions of dollars. The requirement that student data systems be compatible with the Services Card was contained in the Request for Proposals, but the school district was not told that it would cost so much. Nor were they told why it would cost so much or provided with any technical

[40] Gartner Inc, 'A Report for BC Ministry of Education: Review of Student Information System' (*Gartner*, 12 September 2011) <www.bced.gov.bc.ca/pubs/review_of_student_information_systems.pdf> accessed 2 September 2014.

[41] Lindsay Kines, 'Saanich School District Builds Own Software to Handle Student Data, Defies Doubters' (*Times Colonist*, 20 January 2013) <www.timescolonist.com/news/local/saanich-school-district-builds-own-software-to-handle-student-data-defies-doubters-1.51944> accessed 2 September 2014.

[42] Robert Wipond, 'Dangerous Linkages' (*Focus Magazine*, May 2014) <http://focusonline.ca/?q=node/723> accessed 2 September 2014.

specifications that would clarify the requirements or the costs.[43] Subsequently, the school district accessed documents under a freedom of information request that showed that the Education Ministry had granted the MyEducation BC system a five-year exemption (with option for extension) on the Services Card requirement. The Saanich school board issued a statement stating that at no time was Saanich offered a similar exemption.[44]

The BC government has been accused of 'putting up roadblocks' to the development of openStudent.[45] In the RFP for the new student information system the government describes itself as 'highly motivated to ensure that School Districts adopt the [contracted for, province-wide] Service' and promises that 'senior executives at the Ministry, as well as the SIS-ESC responsible for this procurement are committed to encourage all School Districts onto the Service, as quickly as feasible.' [46] While technically not mandating the centralized system in which the government controls the data capture, the government expressly committed to getting all school districts onto the system, and will likely succeed as individual school districts are unsupported in developing their own systems.

In this case, the costs of unspecified integration with the Services Card, a key piece of e-government architecture, was used to effectively discourage or disqualify a decentralized, locally-controlled, less privacy-invasive alternative.

e-Government: The Democratic Deficit

While the increased capture and centralization of citizens' data may be motivated at least in part by a desire for better service provision, it nevertheless has the effect of increasing surveillance, concentrating

[43] ibid.

[44] Lindsay Kines, 'B.C. Misled Saanich School Board: Documents' (*Times Colonist*, June 4, 2014) <www.timescolonist.com/news/local/b-c-misled-saanich-school-board-documents-1.1115787> accessed 21 November 2014.

[45] Wipond (n 42).

[46] Government of British Columbia, 'Request for Proposals Student Information Service' (*Government of British Columbia*, 7 December 2012) 19 <www.bcedplan.ca/actions/technology/doc/sis-rfp-information.pdf> accessed 2 September 2014.

power, and diminishing rights. This aspect of e-government initiatives continues to foster controversy and legal debates, particularly in relation to the overlap of the public and private spheres of regulation and the question of constitutional rights.

The e-government re-brand in BC—'Citizens @ the Centre'—tries to ally itself with the popular notion of online communities and social media creating progressive and democratic change. Defining principles include to 'empower citizens to create value from open government data', to 'encourage collaboration in the public service because it is integral to delivery of quality services to citizens', to encourage citizens' participation, and their ability to 'interact with their government more directly in a dialogue about their communities and their futures'.[47]

These principles appear to reflect the robust notion of democracy described by Kristin Ross: the capacity of ordinary people to discover modes of action for realizing common concerns.[48] However, in almost every aspect of the e-government developments in BC, the opposite is occurring. Citizens are finding themselves disempowered.

Citizens are increasingly unable to control dissemination of their personal information. Government is increasingly insulated from citizen complaints about the management of individuals' personal data because no one outside of an increasingly small set of experts can understand the system sufficiently to effectively raise concerns. Almost no citizen or community group is sufficiently resourced to bring a constitutional challenge and the government shows no interest in referring a constitutional question for guidance on its reforms. Community-based organizations and other private sector service providers are challenged to resist the government capture of their patients'/clients' data, either because it is legislated or they cannot jeopardize needed government funding. Individuals are unlikely to have notice of the loss of their privacy protections in this regard or have meaningful alternatives. And exemplary participation and digital citizenship, such as the Saanich School District's responding directly to the education community's needs with an open source system, are being effectively shut down.

---

[47] BC Public Service (n 4).

[48] Kristen Ross, 'Democracy for Sale' in *Democracy in What State?* (William McCuaig tr, Columbia University Press 2011).

It is a brief snapshot, but nevertheless a sharp illustration that it is citizens' valuable data and not citizens themselves that are '@ the Centre' of these developments.