

**SEEING THROUGH THE CLOUD: COMMENTARY**

Responses to *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World* (2015), also available online at ecommoutsourcing.ischool.utoronto.ca/final-report/commentary.

Table of Contents

Colin Bennett, Professor, Department of Political Science, University of Victoria .................................................................1
Heather Black, former Assistant Privacy Commissioner for Canada .............................................................................................................2
Avner Levin, Chair, Law and Business Department, Ted Rogers School of Management at Ryerson University and Director of the Privacy Institute ........................................................................................................3
David Lyon, Professor, Department of Sociology, Queens University .........................................................................................................4
Vincent Mosco, Professor Emeritus of Sociology, Queen’s University and former Canada Research Chair in Communication and Society .........................................................................................................................5
Marc Rotenberg, Executive Director, Electronic Privacy Information Center (EPIC) ..................................................................................5
James L. Turk, Distinguished Visiting Professor, Ryerson University ........................................................................................................6
Konrad von Finckenstein, Q.C, Former Justice of the Federal Court of Canada, Commissioner of Competition, Former Chair of the Canadian Radio-television and Telecommunications Commission ................................................6

**Colin Bennett, Professor, Department of Political Science, University of Victoria**

The Report “Seeing through the Cloud” should remind us what a fundamentally misleading concept “cloud-computing” actually is. The constant pressure to outsource to “cloud” services for economic reasons entails huge implications for national sovereignty, privacy, intellectual property and other values, as documented in this report. The implications are particularly pressing for Canada, whose economy has been so inextricably linked to that of the United States. Yet, most organizations and individuals give little thought to how and where their data might be stored and processed. They should. Based on detailed legal analysis, careful empirical investigation into outsourcing by Canadian universities, this report reminds us that jurisdiction matters, the routing of communications matters, and national laws still matter. Behind all the hype about “borderless worlds” and the “cloud” lie a range of crucial questions concerning what Canadian organizations can, and should, do to protect the personal data under their control.

Colin Bennett is a professor in the Department of Political Science at the University of Victoria. His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published six books, including *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, 2008) and *Transparent Lives: Surveillance in Canada* (AUP, 2014), as well as policy reports on privacy protection for Canadian and international agencies.
Heather Black, Former Assistant Privacy Commissioner for Canada

I have followed with interest the ongoing debate on the outsourcing of universities’ email systems and I have also noted the universities’ reliance on the 2005 PIPEDA case involving CIBC Visa. It is important to place that finding in context which involved the transfer for processing of the Visa transactions of Canadians to a US processor. The metadata in question included names with associated billing addresses, billing amounts and the names of the providers of the goods and services being billed for. In short the information was not particularly sensitive.

PIPEDA requires that when information is being transferred for processing an organization must ensure that the information is provided with a “comparable level” of protection that it is afforded under PIPEDA. In the course of arriving at a finding in the CIBC Visa case, the Office of the Privacy Commissioner of Canada applied what has come to be called a “similar risk” analysis. Simply put, is the information of individual Canadians at a greater risk, a lesser risk or a similar risk when it becomes subject to the laws of another jurisdiction, such as the US? On balance the thinking at the time was that the laws of Canada and the US were more or less comparable and that the CIBC could not have done anything further to protect the information once it left Canada.

In their excellent paper on Why Jurisdiction Still Matters, Lisa Austin and Daniel Carens-Nedelsky have argued that the “similar risk” analysis as applied in the CIBC Visa case is wrong and that it should not be relied upon by the universities. While I totally agree with the second part of that premise, I do not necessarily think that the analysis model itself is wrong but that as the paper argues it did not go far enough. In light of the Snowden revelations I believe it would be foolish indeed to blindly follow the CIBC Visa “precedent” especially when the personal information at stake is something as sensitive as emails. It is necessary now to go beyond a comparison of the Patriot Act with Canadian laws as they were at the time and move to a more complete analysis of the legal and constitutional regimes in both countries.

Heather Black practised law in the federal Department of Justice from 1976 to 2000, specialising in commercial, and information and privacy law. Beginning in 1982, she worked on the implementation of the federal Access to Information and Privacy Acts. In the mid-nineties Heather began work with Stephanie Perrin on the project that ultimately culminated in the drafting and passage of the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000. That year she moved to the Office of the Privacy Commissioner of Canada (OPC), becoming General Counsel at the OPC a year later and in 2003 Assistant Commissioner with primary responsibility for private sector privacy. Heather co-authored The Personal Information Protection and Electronic Documents Act: an Annotated Guide with Stephanie Perrin, David Flaherty and Murray Rankin, published in 2001 by Irwin Law. Heather retired from the public service in 2007 and has since been working as a consultant, including being a member of the External Advisory Board for the Office of the Information and Privacy Commissioner of British Columbia.
Avner Levin, Chair, Law and Business Department, Ted Rogers School of Management at Ryerson University and Director of the Privacy Institute

The recently released research report “Seeing Through the Cloud” provides powerful and timely counterarguments to a recent arbitral decision on a grievance brought forward by the union representing Dalhousie University’s faculty members against the university’s administration for its decision to outsource the university’s communications to Microsoft.

Nova Scotia’s Personal Information International Disclosure Protection Act (PIIDPA, not to be confused with the federal PIPEDA) was passed to limit the ability of public bodies to outsource personal information on the basis of concerns very similar to those found in “Seeing Through the Cloud”. The Act contains several limiting measures, including the stipulation (in Section 5) that personal information should only be stored and accessed within Canada, and the prohibition (in Section 8) on the international disclosure of personal information. PIIDPA does permit the head of a public body to allow storage or access outside of Canada, “if the head considers the storage or access is to meet the necessary requirements of the public body’s operation.” Similarly, the Act provides for a list of exceptions to the general prohibition on international disclosure.

Unfortunately, despite the stated purpose of PIIDPA, the arbitrator found that the outsourcing to Microsoft falls within the exceptions to Sections 5 and 8. The arbitrator found that Dalhousie’s decision was reasonable since it was arrived at through a process of deliberation in which several operational requirements (including costs) were assessed and found necessary, as per the language of the exemption. The arbitrator found that “cost played a role in [Dalhousie’s] decision, [but] it was by no means the only factor.” Among some of the other requirements the arbitrator listed “robustness, functionality and enhanced security.”

Here is one point where “Seeing Through the Cloud” explains why the analysis of the arbitrator, and the university, is ultimately lacking. The report argues convincingly that the debate over outsourcing is, crucially, a constitutional one. While no constitutional right is absolute there is a great distance between the careful constitutional analysis taken by the courts when they evaluate whether rights should be circumscribed, and the operational analysis conducted by the university and endorsed by the arbitrator.

The arbitrator also found that storage outside of Canada does not amount to disclosure. In arriving at his finding the arbitrator conducted a linguistic analysis of “disclosure” and an analysis of the relationship between the various relevant sections of PIIDPA. The arbitrator did not mention the massive NSA surveillance programs uncovered by Snowden and it is worth noting that PIIDPA was originally passed in 2006, in reaction to the USA PATRIOT Act but without, obviously, awareness of the extent of the NSA’s activities. In my opinion our current knowledge of the NSA’s mass surveillance should prompt decision makers to proceed with more, not less, caution, when authorizing outsourcing and so the arbitrator should have interpreted disclosure in light of American practices and in a manner significantly more protective of Canadian privacy.

Finally, the arbitrator bolstered his substantive findings with some general observations on the security and risks associated with electronic storage and communications. On the format of e-mail the arbitrator stated that “email communications are far from being secure, even when hosted within Canada... Certainly, any person who entrusts personal information to email, particularly their work email, cannot do so with a high expectation of privacy.” Here is a second point where the arbitrator could have benefited from the excellent “similar risk” analysis in which the report clearly and carefully lay out the differences between the United States and Canada. This thorough analysis stands in stark contrast to the generalizing and incorrect observation of the decision.
Of course, the arbitrator, Dalhousie and its faculty members did not have the benefit of reading the report and its analysis of outsourcing throughout the grievance. Now that the report is public, courts and other arbitrators that may be called upon to decide similar disputes would be well advised to carefully consider whether, in the cloud-piercing light provided by this report, there is any basis to agree with the Dalhousie decision.

Dr. Avner Levin is a Professor at the Ted Rogers School of Management, and Chair of the Law & Business Department. He heads Ryerson University’s Law Research Centre which focuses on research related to law and legal education. He is also the Director of the Privacy and Cyber Crime Institute, a centre for research related to privacy and cybercrime. During the 2012-2013 academic year Professor Levin served as Ryerson University's Interim Vice-Provost of Faculty Affairs and as Interim Assistant Vice-President of Human Resources.

Professor Levin’s research interests include the protection and legal regulation of personal and private information, both locally and internationally. Among his recent research areas are social media, online advertising, the workplace, mobile devices, corporate risk management, electronic health records and the smart electricity grid. He has been a recipient of funding from the Office of the Privacy Commissioner of Canada, Public Safety Canada and Industry Canada.

David Lyon, Professor, Department of Sociology, Queens University

This is a model of good report-writing. It states clearly and unequivocally the issues regarding cloud services that are increasingly used by universities and other organizations for eCommunications and demonstrates that the logic justifying their choices is frequently under-informed and flawed. This puts many ordinary members of such organizations at risk of significant privacy breaches that are far more than ‘private troubles’—they are public issues ranging from appropriate confidentiality of documents to democratic participation. The report is both technically and legally literate and relies on evidence and careful argument to make its case. The key finding is that local jurisdictions do create different situations—the idea that ‘similar risks’ occur wherever you live is simply misleading. This is not an argument against using new digital communications but rather a plea that the policies that shape their use be recognized and reformed to offer genuine protections where they are most needed. Lastly, the report also offers ways of engaging these issues, so often treated as ‘beyond our reach’ in some supposed global cyberspace, in our own local situations. You don’t have to be an Edward Snowden to make a difference.

David Lyon is director of the Surveillance Studies Centre, Queen’s Research Chair in Surveillance Studies, and professor in the Department of Sociology and the Faculty of Law at Queen’s University. Some of his recent books are The Routledge Handbook of Surveillance Studies (2012), Transparent Lives: Surveillance in Canada (AUP, 2014) and Surveillance after Snowden (Wiley, 2015). He is a cofounder of the journal Surveillance and Society and the Surveillance Studies Network.
Vincent Mosco, Professor Emeritus of Sociology, Queen’s University and former Canada Research Chair in Communication and Society

This project makes an important contribution to Canadian research and policy analysis on a significant, but poorly understood, area of the online world. As it convincingly demonstrates, there are significant privacy implications in the movement of data to the Cloud and while it is sometimes less expensive to locate data outside Canada, there is considerably greater privacy protection for data that remains in Canada. In order to save money, institutions like universities are placing the records of employees and students at great risk by moving it to foreign servers.

The report is all the more important as we move to what I call the Next Internet, which combines Cloud computing, Big Data analytics, and the Internet of Things. The world of decentralized servers based in thousands of IT centers is giving way to large Cloud data centers run by companies based in the US (Amazon, Microsoft, Google) and China (Alibaba, Baidu, Tencent) which profit by storing, processing, and, increasingly, marketing data. Security is a serious issue as was demonstrated in 2015 when, the U.S. government reported that hackers had stolen the personnel records of 22.1 million federal employees, contractors, and their families and friends who provided information for background checks. The growth of Big Data analysis expands the universe of commercial potential in Cloud-stored data. Companies and government agencies, especially military and intelligence bodies, are expanding their capabilities in building the apparatus of digital positivism. Reliance on so-called predictive algorithms expands profit and control, but is fraught with problems, especially when bad data are trusted to make big decisions. Finally, there is the Internet of Things, which connects objects and people and promises an exponential expansion in commercial and surveillance opportunities.

The security problems identified in this report will also grow substantially unless Canada establishes an appropriate national regulatory regime. In the meantime, it would be wise to stop putting at risk data on Canadian citizens by subjecting it to the seriously flawed regime of the Next Internet.

Dr. Vincent Mosco (PhD Harvard) is Professor Emeritus of Sociology at Queen’s University where he was Canada Research Chair in Communication and Society and head of the Department of Sociology. His most recent book To the Cloud: Big Data in a Turbulent World, was named a 2014 Outstanding Academic Title by Choice: Current Reviews for Academic Libraries. Dr. Mosco’s latest project addresses The Next Internet: The Cloud, Big Data, and the Internet of Things.

Marc Rotenberg, Executive Director, Electronic Privacy Information Center (EPIC)

Perrin and her co-authors make a powerful argument that the adoption of cloud based services, particularly for business and government, is a risky proposition. Until baseline privacy safeguards are put in place, the wise move is to keep data close to home.

Marc Rotenberg is Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, DC. He teaches information privacy law at Georgetown University Law Center and has testified before Congress on many issues, including access to information, encryption policy, consumer protection, computer security, and communications privacy. He testified
before the 9-11 Commission on “Security and Liberty: Protecting Privacy, Preventing Terrorism.” He has served on several national and international advisory panels, including the expert panels on Cryptography Policy and Computer Security for the OECD, the Legal Experts on Cyberspace Law for UNESCO, and the Countering Spam program of the ITU.

James L. Turk, Distinguished Visiting Professor, Ryerson University

Heidi Bohaker and colleagues’ report, Seeing Through the Cloud, provides a vital antidote to the misinformed thinking that has allowed the outsourcing of academic staff email and other eCommunications at a growing number of Canadian universities. In an increasingly digital society, it has become too easy to abandon any notion that privacy can be protected and therefore that it is important to protect. But some aspects of privacy are essential. One of those is intellectual privacy—protecting from surveillance the generation of ideas before they are ready for public distribution. In universities, whose public mission is the advancement of knowledge and education of students, this has been long recognized through the concept of academic freedom. But that academic freedom is fundamentally undermined if emails, preliminary drafts of papers and lectures, or other exchanges of ideas become subject to surveillance, or even the realistic possibility of surveillance. The effect is chilling and harmful. But that is precisely what happens when universities outsource eCommunications to Microsoft or Google. Seeing Through the Cloud dismantles the justifications for such outsourcing—showing them to be misinformed and invalid. It offers useful recommendations for Canada’s universities, governments, and privacy commissioners. I can only hope they read this report and are guided by its sound advice.

James L. Turk is Distinguished Visiting Professor at Ryerson University and Director of the Ryerson’s Centre for Free Expression. For the past 16 years, he was the Executive Director of the Canadian Association of University Teachers. His most recent book is Academic Freedom in Conflict: The struggle over free speech rights in the university (Lorimer, 2014).

Konrad von Finckenstein, Q.C, Former Justice of the Federal Court of Canada, Commissioner of Competition, Former Chair of the Canadian Radio-television and Telecommunications Commission

I enjoyed reading the “Seeing through the clouds” report. Not only is it insightful, full of pertinent information, but is also clearly written and all findings are well supported. The report convincingly establishes why outsourcing can jeopardize privacy of data, why the ‘similar risk ’ analysis is deficient, why the privacy impact assessments conducted by universities are insufficient, and how data whether stored abroad or in transit can be accessed by the US under present US legislation.

It also raises important questions rarely addressed elsewhere such as:

…we noted a lack of clarity around the question of metadata. Is metadata in fact Customer data? Who owns the data generated by users in the course of using the software? Are companies in fact free to mine that data and/or sell that data to third parties? Will the Internet of Things bring fresh threats to this situation? When a customer...
ends their contractual relationship with the vendor, is the metadata returned along with the customer data? Does the vendor get to retain copies? These questions are unanswered.

I certainly agree with your conclusions:

We need a much broader policy debate, both within Canada and internationally, to ensure that the benefits of new communications technologies do not come at the cost of losing the human rights we fought so hard for in the last century. We encourage readers of this report to become engaged with these issues we have discussed here, and press politicians at all levels for legal reform and better public policy.

The recommendations at the end of your report are very commendable but I am afraid a bit over optimistic and unlikely to be followed. For instance, I do not see Parliament following your suggestions:

1. To enhance and clarify data protection across Canada, we encourage legislators to actively engage in law reform in the area of transborder dataflow.
2. To reduce the transit of domestic Internet traffic through the US and therefore to capture by the NSA’s UPSTREAM program, legislators should enact requirements that telecommunications carriers route domestic Internet traffic within Canada, such as via public Internet exchange points (IXPs)

More precise, more concrete and limited recommendations would in my view be more likely to be received positively.

However the main goal of the report is obviously to bring the issue of the ‘cloud’ to the attention of the public and organizations who use them. In that you have succeeded brilliantly. It is a frightening picture that you paint and it makes a strong argument for why one should not resort to cloud storage merely for the sake of cost efficiency. The report certainly points out the dangers and shows some steps that should be taken to minimize risks.

I hope this report serves as a call to action and more research on this field, and will spur the search for more precise solutions.

The Honourable Konrad von Finckenstein, Q.C. is an arbitrator of complex Canadian and international business disputes in both institutional and ad hoc settings. He has been in public service for nearly 40 years, and has been extensively involved in the negotiation and settlement of a wide variety of high-profile disputes since the 1980’s.

Justice von Finckenstein has held a number of prominent positions, including Justice of the Federal Court of Canada, Commissioner of Competition, and Chair of the Canadian Radio-television and Telecommunications Commission, where he acquired broad experience in matters involving dispute resolution, business and commercial law, international trade, competition, telecommunications, and administrative law.