

Chapter 51

Cloud Computing and Gov 2.0: Traditionalism or Transformation across the Canadian Public Sector?

Jeffrey Roy

School of Public Administration, Dalhousie University, Canada

ABSTRACT

This article seeks to dissect the evolution of digital governance within the Canadian public sector at an expansionary time for cloud computing and wider reforms often referred to as Gov 2.0. Beyond infrastructure, the notion of the cloud may also be viewed as a proxy for a wider societal transformation that, in turn, impacts government both administratively and politically. This wider transformational nonetheless faces tensions between traditional proprietary concepts and mindsets and newer emerging models of open source and shared openness. The future of the Canadian public sector requires a careful navigation and blending of these two worldviews. While some observers may prefer to decouple cloud computing from new governance capacities associated with Gov 2.0 (viewing the cloud instead strictly through a prism of internal architecture and infrastructure), the evidence presented in this article suggests that both directions are intimately related in shaping the public sector going forward.

1. INTRODUCTION

The purpose of this article is to dissect, assess, and better understand the evolution of digital governance within the Canadian public sector at an expansionary time for both cloud computing solutions and wider reforms often referred to as Gov 2.0. Both directions are tied to the advent of the Internet and virtualization on the one hand, and on the other hand the increasingly networked patterns of governance structurally and culturally challenging traditional government pillars of hier-

archical control and proprietary notions of ownership in terms of information and infrastructure.

Governments around the world are thus actively studying and pursuing (to varying degrees, depending on the jurisdiction) cloud computing solutions for infrastructure refurbishment. The importance of doing so is underscored by two recent and inter-related developments germane to IT governance within the Canadian public sector at the federal level: first, an April 2010 Auditor General's report lamenting the general state of disrepair of antiquated, legacy systems across the

DOI: 10.4018/978-1-4666-6539-2.ch051

Government of Canada (underpinning billions of dollars of service processing and delivery); and secondly, the 2011 formation of Shared Services Canada, an internal agency meant to coordinate, to some degree consolidate, and upgrade the shared IT infrastructure for the federal government as a whole. In line with other likeminded democracies such as the US, the UK, and Australia, Shared Services Canada (SSC) is now tentatively exploring the deployment of cloud-based solutions as its efforts take shape. Accentuating the importance of such matters, a more recent report by the Auditor General in October 2012 cited significant weaknesses in cyber-security within Government of Canada operations (directly relevant since the safeguarding, storing, and sharing of personal data and corporate information flows are central factors in discussions and debates pertaining to cloud computing feasibility and desirability), while a major data breach would be revealed early in 2013.¹

Beyond such critical internal matters pertaining to infrastructure, the notion of the cloud may also be viewed as a proxy for a wider societal transformation that, in turn, impacts government both administratively and politically. As Young puts it, the cloud as a symbolic basis of a wider virtual universe driven by a myriad of smaller and more powerful and mobile computing devices, a penchant to share more and more personal information online – especially via social media, and a new form of enhanced and shared networked intelligence (Young, 2012). This wider transformational is nonetheless partial and contested – rooted within tensions between traditional proprietary concepts and mindsets on the one hand, and newer emerging models of open source and shared openness (often associated, but not synonymous with cloud computing models as discussed below). For governments, the advent of so-called ‘Gov 2.0’ is very much predicated upon this wider notion of a cloud as a more open, networked, and participative architecture for not only digital infrastructure but also organizational and societal governance

(Roy 2013b). The resulting implications not only impact individual government levels (such as and perhaps notably the federal government and its aforementioned reforms) but also the public sector as a whole with respect to local and provincial jurisdictions and the widening interdependence of all such levels in a cloud-driven and increasingly mobile era (ibid.).

In exploring cloud computing infrastructure as well as the wider implications of cloud-inspired governance, this article is organized as follows. Following this introduction, section two explains the origins of cloud computing in today’s virtual environment and the prospective benefits and risks for government. Shifting to a more empirical perspective, section three presents an exploratory case study of the Canadian public sector as a whole – encompassing examples and initiatives from all government levels, both individually and in terms of their shared efforts.² Section four then draws from this case study the most lessons and implications for both cloud computing deployment within the wider pursuit of Gov 2.0. The article then concludes with a brief summary of the main argumentation and key lessons of this undertaking.

2. THE EMERGENCE OF CLOUD COMPUTING: BENEFITS AND RISKS

As a new form of digital infrastructure, cloud computing is intertwined with virtualization and the emergence of the Internet, defined as follows by Wyld: ‘The term “cloud computing” has at its core a single element: computing services are delivered over the Internet, on demand, from a remote location, rather than residing on one’s own desktop, laptop, mobile device, or even on an organization’s servers (p.6 Wyld, 2010). Closely tied to virtualization on the one hand, and a commoditization of many forms of IT services on the other hand, many observers speak of cloud computing as a form of utility computing – accessing and paying for infrastructure developed, residing, and

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cloud-computing-and-gov-20/119899

Related Content

Fake Review Detection Using Machine Learning Techniques

Abhinandan V., Aishwarya C. A. and Arshiya Sultana (2020). *International Journal of Fog Computing* (pp. 46-54).

www.irma-international.org/article/fake-review-detection-using-machine-learning-techniques/266476

Fog Computing Qos Review and Open Challenges

R. Babu, K. Jayashree and R. Abirami (2018). *International Journal of Fog Computing* (pp. 109-118).

www.irma-international.org/article/fog-computing-qos-review-and-open-challenges/210568

Anomaly Detection in Cloud Computing and Internet of Things Environments: Latest Technologies

Rachid Cherkaoui, Mostapha Zbakh, An Braeken and Abdellah Touhafi (2018). *Cloud Computing Technologies for Green Enterprises* (pp. 251-265).

www.irma-international.org/chapter/anomaly-detection-in-cloud-computing-and-internet-of-things-environments/189377

A Review of Quality of Service in Fog Computing for the Internet of Things

William Tichaona Vambe, Chii Chang and Khulumani Sibanda (2020). *International Journal of Fog Computing* (pp. 22-40).

www.irma-international.org/article/a-review-of-quality-of-service-in-fog-computing-for-the-internet-of-things/245708

Analyzing Virtualization Vulnerabilities and Design a Secure Cloud Environment to Prevent From XSS Attack

Nitin Nagar and Ugrasen Suman (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 824-838).

www.irma-international.org/chapter/analyzing-virtualization-vulnerabilities-and-design-a-secure-cloud-environment-to-prevent-from-xss-attack/224608