Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Protecting digital identity in the cloud: Regulating cross border data disclosure

*Clare Sullivan**

School of Law, University of South Australia, Adelaide, Australia

Keywords:
Cross border data regulation
Cloud computing
Digital identity
Regulation of data disclosure
EU
US
Australia

ABSTRACT

Widespread use of cloud computing and other off-shore hosting and processing arrangements make regulation of cross border data one of the most significant issues for regulators around the world. Cloud computing has made data storage and access cost effective but it has changed the nature of cross border data. Now data does not have to be stored or processed in another country or transferred across a national border in the traditional sense, to be what we consider to be cross border data. Nevertheless, the notion of physical borders and transfers still pervades thinking on this subject. The European Commission ("EC") is proposing a new global standard for data transfer to ensure a level of protection for data transferred out of the EU similar to that within the EU. This paper examines the two major international schemes regulating cross-border data, the EU approach and the US approach, and the new EC and US proposals for a global standard. These approaches which are all based on data transfer are contrasted with the new Australian approach which regulates disclosure. The relative merits of the EU, US and Australian approaches are examined in the context of digital identity, rather than just data privacy which is the usual focus, because of the growing significance of digital identity, especially to an individual's ability to be recognized and to transact. The set of information required for transactions which invariably consists of full name, date of birth, gender and a piece of what is referred to as identifying information, has specific functions which transform it from mere information. As is explained in this article, as a set, it literally enables the system to transact. For this reason, it is the most important, and most vulnerable, part of digital identity. Yet while it is deserving of most protection, its significance has been largely underappreciated. This article considers the issues posed by cross border data regulation in the context of cloud computing, with a focus on transaction identity and the other personal information which make up an individual's digital identity. The author argues that the growing commercial and legal importance of digital identity and its inherent vulnerabilities mandate the need for its more effective protection which is provided by regulation of disclosure, not just transfer.

* School of Law Division of Business, University of South Australia, Law Building, George Street, City West Campus, Adelaide, South Australia.
E-mail address: clare.sullivan@unisa.edu.au.
0267-3649/$ – see front matter © 2014 Clare Sullivan. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2014.01.004

1. Introduction

In launching the proposed US Consumer Bill of Rights in 2012, President Obama made the point that Americans can't wait any longer for clear rules that ensure their personal data/information[1] is safe online:

> *Every day, millions of Americans shop, sell, bank, learn, talk and work online. At the turn of the century, online retail sales were around $20 billion in the United States, now they're nearing $200 billion," said Secretary Bryson in announcing the Consumer Bill of Rights. "The Internet has become an engine of innovation, business growth, and job creation…*[2]
>
> *That's why an online privacy Bill of Rights is so important.*[3]

However, there has been even more fundamental change recently. Cloud computing has changed the nature of cross border data regulation. Off-shore data had mostly been an issue in relation to large multinational corporations, especially US multinationals, but now off-shore data services are used by organizations, large and small, around the world. Cloud computing has made data storage and access cost effective and as a consequence, it has changed the nature of cross border data.

As observed by Viviane Reding Vice-President of the EC, EU Justice Commissioner:

> *Our world is no longer defined by physical borders. Data races from Barcelona to Bangalore. It is processed in Dublin, stored in California and accessed in Milan. In the digital age, the transfer of data to third countries has become an important part of daily life. And this affects both businesses and citizens.*[4]

Cloud computing is commonly used to refer to network-based services which to the user, give the appearance of being provided by a hardware server. However instead of a physical i.e. a hardware server, the server is simulated by software running on one or more machines, hence the reference to a cloud.[5] In essence, it is Internet-based computing whereby services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet.[6]

The advantage of cloud computing is that the virtual servers do not physically exist so they can be quickly and easily moved around and scaled up or down without affecting the end-user. Cloud computing does away with the constraints and costs of the traditional computing environment which is based on physical servers, and because of its flexibility, cloud computing has been embraced by government and businesses.

The range of cloud computing services is highlighted by the Article 29 Working Party on the Protection of individuals with regard to the Processing of Personal Data (Article 29 Working Party)[7] in its opinion on Cloud Computing adopted on 1 July 2012[8]:

> *There is a wide gamut of services offered by cloud providers ranging from virtual processing systems (which replace and/or work alongside conventional servers under the direct control of the controller) to services supporting application development and advanced hosting, up to web-based software solutions that can replace applications conventionally installed on the personal computers of end-users. This includes text processing applications, agendas and calendars, filing systems for online document storage and outsourced email solutions.*

As a consequence, data does not actually have to be stored or processed in another country or transferred across a national border in the traditional sense to be what we consider to be cross border data. Yet the notion of physical borders and transfers is evident in the focus on transfer in the EU proposal for reform of cross border data regulation and in the preferred US approach. In turn, this focus on transfer is influencing the reform of the two other major data transfer schemes, the EU's Binding Corporate Rules framework (BCR) and Asia Pacific Economic Cooperation's (APEC) Cross Border Privacy Rules System (CBPR) which are following similar approach to that

[1] In this article the "data" includes information and vice versa, unless otherwise indicated. This is also the approach typically followed in Directives and legislation.

[2] The White House, "*We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*" <www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights> at 29 September 2013.

[3] Ibid.

[4] Viviane Reding Vice-President of the EC, EU Justice Commissioner Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing, IAPP Europe Data Protection Congress Paris, 29 November 2011.

[5] The Cloud is an enabler. Mobile IT, social IT, and big data, for example are all cloud based.

[6] The accepted official definition of cloud computing is that of the National Institute of Standards and Technology ("NIST"), an agency of the US Department of Commerce published in September 2011. After, in its own words, "years in the works and 15 drafts," the final NIST definition is: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction," See, NIST, "*The NIST Definition of Cloud Computing*" <www.nist.gov/itl/csd/cloud-102511.cfm> at 24 September 2013. See also the definition used by the Article 29 Working Party on the Protection of individuals with regard to the Processing of Personal Data: "[C]loud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space." See, Article 29 Data Protection Working Party, "*Opinion 05/2012 on Cloud Computing*, 4.

[7] The Article 29 Working Party is an independent advisory body on data protection and privacy, set up under Article 29 of the *Data Protection Directive 95/46/EC*. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the EC. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[8] Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing, 4.