

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

Digital citizenship and the right to digital identity under international law

Clare Sullivan *

Law Center, Georgetown University, Washington, DC, USA

A B S T R A C T

Keywords:

Digital identity
Digital citizenship
Right to identity
Right to privacy

Australia has formally recognized the importance of digital identity and has raised the issue of reciprocal rights and duties between the government and its citizens. Australia is the first country to articulate digital citizenship in these terms.

This paper considers the respective rights and duties of government and citizens that could be included in a digital citizenship charter, and the likely legal implications. The paper explores these aspects in relation to digital identity because of its increasing commercial and legal importance.

The author argues that considering the consequences for individuals, the right to identity, as an international fundamental human right, should now be recognized and protected in relation to digital identity. The argument is presented that recognition and protection of this right is an essential component of a model of accountable and responsible digital citizenship. While the paper uses the Australian concept of digital citizenship as the basis for the discussion, the issues are relevant to all jurisdictions implementing e-government initiatives that require an individual to use digital identity for transactions.

© 2016 Clare Sullivan. Published by Elsevier Ltd. All rights reserved.

1. Introduction

A specific digital identity for government dealings is now emerging as governments around the world¹ move their services and transactions on-line. Digital identity, as used in this article, consists of the digitally recorded information about a natural person, which is recorded under the particular e-government

scheme. This digital identity is generally required for services ranging from social security benefits and employment assistance to health care and tax filing.² Thus, digital identity is now the primary means by which a natural person can access these services.³

This transition to this new scheme is underway in the United States, Australia and many Asian countries, but is most advanced in European countries, with GOV.UK⁴ and e-Estonia being

* Law Center, Georgetown University, 600 New Jersey Avenue NW, Washington, DC 20001, USA.

E-mail address: cls268@law.georgetown.edu.

¹ The new scheme being rolled out in India is the most recent example of a comprehensive scheme. See IGovernment, 'India plans multi-purpose national ID card for citizens' <igovernment.in> at 24 August 2013. However, most governments around the world are incrementally implementing similar schemes that require a person to register and use a digital identity to access and use government services.

² While it may seem that it is still possible for an individual to transact outside the new digital identity system, this is usually not the case. For example, in Australia, a paper tax return can still be lodged rather than using the e-Tax filing portal. However, the information in the document is scanned into, and processed by, the digital system.

³ Consequently, this article focuses on the consequences for individuals i.e. natural persons.

⁴ GOV.UK uses a single on-line portal to provide access to a range of government services. In many respects GOV.UK follows the model used by the advanced e-economy of Estonia. See e-estonia.com – The digital Society.

<http://dx.doi.org/10.1016/j.clsr.2016.02.001>

0267-3649/© 2016 Clare Sullivan. Published by Elsevier Ltd. All rights reserved.

examples.⁵ Estonia has moved all services to digital delivery while in other countries like the United States and Australia, the move has been more gradual and incremental. Irrespective of how the scheme is established and marketed, if an individual has a digital identity to transact under the scheme, it is a digital identity scheme, and that definition is used in this article.

Of the countries that are incrementally implementing these schemes, Australia is notable for its candour about the impact on individuals. The Australian government has unequivocally stated that Australia is moving to what it calls “digital citizenship”.⁶ The Australian government acknowledges the importance of digital identity and the significant implications in the event of it being compromised:

In an era where our online identity is central to accessing information and services, ensuring the integrity of that identity is increasingly important. The loss or compromise of our online identity can have wide-ranging implications, including financial loss, emotional distress and reputational damage.⁷

Significantly, the Australian government also states that:

... there would be value in revisiting the distribution of responsibility among individuals, businesses and governments ... Developing a common understanding of a model of accountable and responsible digital citizenship – a digital social contract – may need to be part of the debate about Australia’s digital future.⁸

It is against this background that this article examines what a digital social contact should include with regard to digital identity. This article focuses on rights of an individual in his/her digital identity because of its commercial and personal significance. A human right to identity arises under international law. The argument presented in this article is that in the context of a government scheme that requires use of digital identity to transact, this right to identity now takes specific form as the right of an individual to an accurate, functional and unique digital identity.

2. The significance of digital identity

The full implications of digital identity are becoming apparent as governments around the world move services and transactions⁹ on-line.¹⁰ A natural person must use this assigned

digital identity to transact under this type of scheme. This is a fundamentally different way of transacting and it is elevating digital identity to an unprecedented level of personal, commercial, and legal significance.

These schemes are necessarily based on the premise of one person: one digital identity. Digitalization of government services and transactions is driven by the need to reduce costs and to increase efficiency in service delivery, but most importantly, by the need to reduce fraud. As a consequence, an individual can legitimately have only one digital identity under this type of scheme. The move to one person : one identity under this type of scheme is a major change, especially for common law jurisdictions, which unlike civil legal systems such as those based on Dutch and German legal doctrines, have not traditionally recognized identity as a legal concept.¹¹

There are also broader ramifications. The digital identity required for government services will likely set the standard for transactions with the private sector. It is an outcome that is almost inevitable¹² from a practical point of view unless there are reasons to doubt the accuracy and integrity of the registered digital identity;¹³ and that has been the experience internationally to date.¹⁴ This means, in effect, that the digital identity for government transactions would become the primary means by which an individual can enter into all commercial transactions.

Digital identity in this context has specific composition and transactional functions, which make its accuracy and integrity critical, yet system design makes this identity vulnerable to system error. In this article, system error is used in its widest sense to describe any malfunction whereby an otherwise authentic and valid digital identity is not recognized by the system. A malfunction may be spontaneous or the result of all or part of an individual’s digital identity being used by another person. In most instances, the latter will involve dishonesty, but not always.¹⁵

Digital identity and its susceptibility to system error fundamentally change the balance of responsibility and accountability between government and citizens. Individuals, the most vulnerable sector with comparably less access to resources and information, are most affected when the system does not operate as intended as a result of fraud or

⁵ The scheme may be formally established as such from the outset, as was done in Estonia and as is now being implemented in India, but in many countries, the scheme is phased-in gradually through subtle, incremental change. This is the approach in Australia and the United States, for example.

⁶ Australian government, “Connecting with Confidence: Optimising Australia’s Digital Future” A Public Discussion Paper (2011).

⁷ Ibid, 10.

⁸ Ibid.

⁹ A transaction in this context is any dealing for which an individual is required to use digital identity. A transaction may be between an individual and a government department or agency or with a private sector entity if that is permitted under the scheme. A transaction can range from an enquiry to a contract.

¹⁰ Recall that digital identity is all the information digitally recorded about an individual i.e. a natural person – that is accessible under the particular scheme. In this article, ‘Information’ includes ‘data,’ unless otherwise indicated.

¹¹ One person : one identity has also not been a requirement for private schemes like Visa credit and debit card transactions.

¹² Unless there are questions about the integrity of the government-assigned and registered digital identity.

¹³ This is a feature of similar schemes in other countries. It is a stated feature of the new national identity scheme being rolled out in India, and it was a feature of the scheme planned for the United Kingdom, which was extensively documented. Although the full scheme was not implemented in the United Kingdom as planned, the United Kingdom scheme is the model for the new Indian now being rolled out. See for example, United Kingdom Information Commissioner, “The Identity Cards Bill—The Information Commissioner’s Concerns (June 2005)” < ico.gov.uk > at 10 May 2006.

¹⁴ The advanced e-economy of Estonia is a notable example.

¹⁵ Another person may use an individual’s identity accidentally such as by inadvertently keying-in the wrong information, though this would be a comparatively rare occurrence.

Download English Version:

<https://daneshyari.com/en/article/467445>

Download Persian Version:

<https://daneshyari.com/article/467445>

[Daneshyari.com](https://daneshyari.com)