Editorial

Rebecca Wong*

Nottingham Law School
Burton Street, Nottingham
NG1 4BU, UK
E-mail: R.Wong@ntu.ac.uk

Joseph Savirimuthu*

Liverpool Law School
University of Liverpool
Liverpool, L69 7ZS, UK
E-mail: J.Savirimuthu@Liverpool.ac.uk
*Corresponding authors

Biographical notes: Dr. Rebecca Wong is a Senior Lecturer of Law at the Nottingham Law School, Nottingham Trent University, UK, with teaching and research interests in tort, intellectual property, data protection and cyberlaw. Her main areas of specialisation are in data protection and privacy. She holds an LLB (1998), MSc (2000), LLM (2001), PCHE (2004) and a PhD (University of Sheffield, 2007) in Data Protection. She has written widely on privacy and data protection and her recent publications include *Data Protection Online: Alternative Approaches to Sensitive Data*, 2007, *International Journal of Commercial Law and Technology*, Vol. 2, No. 1, pp.9–16 (reprinted in *Journal of Internet Law*, March 2007 and *ICFAI Cyberlaw*, May 2007) and 'Demystifying clickstream data: a European and US perspective', *Emory International Law Review*, Vol. 20, No. 2, pp.563–590 (2006).

Joseph Savirimuthu is a Lecturer of Law at the Liverpool Law School, the University of Liverpool, UK. His teaching and research areas include internet regulation and governance, internet child safety and information security. He holds an LLB (1987), an LLM in International Business Law (1988), a Diploma in Legal Practice (1997), a PGCE (2004) and Certificate in Internet Child Safety (2007). He is also a Consultant with an online mediation company and a firm of copyright, patents and trademark attorneys. His recent publications include *P2P@softwar(e).com: Or the Art of Cyberspace 3.0* (2007), *DRMs, RFID and Disruptive Code: Architecture, Dystopia and Eunomics* (2006), *Reflections on the Google Print Library Project* (2006) and *'Open Source, Code and The Architecture: It's the Memes Stupi'* (2005).

1 Introduction

With over 1.4 billion users of the internet, the management as well as the control of information flows has attracted the interest of organisations, industries, governments, and privacy advocates. Identity management systems enable users to control their personal

information when accessing online services. From the perspective of service providers, identity management systems offer two key benefits. First, they are useful as systems for authentication. Second, users do not have to create multiple accounts when accessing particular websites. What are the privacy implications arising from the growing use of federated identity management systems? We can approach this question differently. What are the privacy risks confronting users when disclosing information to service providers? Consider as an example the information that users now disclose when accessing application platforms on social networking sites or setting up accounts on websites. As 'digital subjects', do privacy values and principles continue to be relevant? A digital subject, as defined by Kim Cameron, is:[1]

> "A person or thing represented or existing in the digital realm which is being described or dealt with."

It is entitled to certain constitutional guarantees relating to the individual's privacy. Do we conceptualise 'identity' and 'privacy' differently? Having clear ideas about the goals and policies of identity management systems is relevant to an understanding of what privacy means in the digital environment. We can, as an example, consider the context in which the European Data Protection Directive 95/46/EC was passed. How would these policy-makers now view logistical, cultural and legal issues regarding the collection and storage of identifiable personal data by social networking sites, Google and Yahoo!? This special issue focuses on privacy and its intersections with information technology and associated social and technology trends.

Part 1 consists of contributions from international legal scholars and practitioners on various topics concerning the individual's identity, in particular, the implications of the use of digital rights management software on privacy, location-based identity, identity cards and avatars.

Part 2 is devoted to analysing the paradox of identity management systems. Given the broad reach of the issues raised by identity management systems, the focus and the analysis of the topics in the Special Issue is modest. There are many issues and topics that continue to pose ongoing governance challenges. The contributions in the Special Issue aim to facilitate debate, and encourage much needed research and analysis of the paradox of identity management systems. Any further analysis and debate cannot ignore a central concern facing all stakeholders in the age of information flows – in the digital environment, privacy once lost cannot be erased from the collective memory of the internet.

We hope that the discussion in both issues will serve as a platform to heighten awareness and further research into the importance of 'identity' and 'privacy' amongst policy-makers and industry.

Note

1 http://www.identityblog.com/stories/2004/12/09/thelaws.html