Editorial

Abhilash Nair

The second Issue of 2015 is a collection of four thought provoking articles. The overarching theme of this issue is privacy and data protection, albeit approached from different perspectives and contexts. The Issue also contains an article that encapsulates the theme of cybercrime from an enforcement perspective, offering a useful contribution to the discussion in this highly topical area.

The debate surrounding privacy in the context of social networking sites has been fairly polarised with strong arguments mooted on both sides of the spectrum. People share large amounts of personal information online often without thinking about its potential implications for privacy and in some cases, safety. Bessant, in her insightful article considers a very important issue: what happens when an individual posts photographs of others online? Citing the example of parents taking photograph of children at school events, she analyses the efficaciousness of the current data protection laws as well as the impending European level General Data Protection Regulation in protecting personal data.

Esayas undertakes a useful analysis of the role of anonymised and pseudonymised data in the wider data privacy discourse by examining the current and proposed EU data privacy rules. The article identifies how anonymisation and pseudonymisation can serve as a safe harbour from the application of data privacy rules in its entirety or, in some cases, partially. It then goes on to argue that it could also constitute the mandated requirements for compliance with data privacy obligations such as data security. The article persuasively takes the discussion forward beyond its current focus within existing literature on the technical aspects and the rather limited legal discourse, by providing an in-depth analysis and contextualising it within the existing and proposed EU data privacy rules.

Staying on the theme of privacy, Spahiu comments on the decision of the Court of Justice of the European Union in the Google Spain case (case c-131/12). Spahiu argues that the decision does not necessarily imply a victory for the 'right to be forgotten' over the 'right to know', but reinforces the protection of private interest where the public interest is absent. She goes on to state that the decision has far reaching consequences by bringing personal data protection to a whole new level that may have a significant impact in the future regulation of internet companies.

On a separate theme of cybercrime, Calcara *et al* analyses the advantages and limits of the use of social media and computer technology in cyber policing. Using the example of the Finnish Internet Police (Nettipoliisi), they evaluate the potential of social media for virtual community policing and as a medium of carrying out ordinary police work. The article raises interesting questions as to whether it is possible to create a new type of law enforcement service appropriate for cyberspace with similar functions and powers of 'regular' police. The authors argue rather persuasively that the Nettipoliisi offers a good model for other countries to follow for effective policing of cyberspace.

All of the above articles are timely and topical in the context of the current discourse on internet law and regulation. They offer a lot of food for thought, and we leave it to the readers to ponder on how these arguments influence and shape the future debate on our rights and freedoms in cyberspace.