Summary of Proceedings

Jessie Blackbourn*

The IACL Working Group on Constitutional Responses to Terrorism held its 2012 Workshop in Sydney, hosted by the Australian Research C Laureate Project on Anti-Terrorism Laws and the Democratic Challenge and the Gilbert + Tobin Centre of Public Law at the University of New South Wales. It was held over two days on 13 and 14 December, and was attended by participants from Asia, Australasia, Europe, and South and North America. The Workshop addressed the impact of post-9/11 surveillance practices on constitutionalist principles.

Session 1: Surveillance, Counter-Terrorism and Constitutional Law – A Review

The first session of the conference introduced participants to a variety of significant themes and issues relating to contemporary surveillance practices and constitutionalist principles. The presentations and subsequent discussion centred on the balance between security and liberty in the particular context of the intrusions that anti-terrorism surveillance makes into the right to privacy. Presenters and participants discussed a number of important issues in the debate, including the question of what constitutes privacy; what limitations could or should be placed on privacy; how should ‘reasonableness’ in the right to privacy context be conceived, and by whom; and how have new technologies challenged traditional conceptualisations of the right to privacy. David Cole offered three approaches that might benefit the US in protecting privacy in the face of new technologies: redefining the concept of privacy to take into account new technologies, such as the ability to mass mine, collate and analyse vast reams of data; introducing a ‘least restrictive means’ test; and establishing an office of privacy commissioner or independent reviewer of state surveillance practices. Conor Gearty’s paper focused on how the debate between liberty and security has skewed our conception of democracy so much that democratic states have been allowed to carry out surveillance practices that would not previously been acceptable in a civil liberties-respecting society. Acknowledging this could lead to some form of resistance and

* Postdoctoral Research Fellow, ARC Laureate Project Anti-Terrorism Laws and the Democratic Challenge, Gilbert + Tobin Centre of Public Law, The University of New South Wales.
contestation. These themes of contestation, new technologies, and balancing rights with security continued throughout the workshop.

**Session 2: Migration & Harmonisation**

The three papers in session two took up some of the key themes identified by the two papers in the first session. Cian Murphy’s presentation looked at the extent to which the US and EU have shared surveillance policy, in particular with relation to border security and lists of Passenger Name Records on flights terminating in the US. The paper highlighted the clash between the US desire for security and the EU’s guarantees of privacy in its data protection laws. Murphy drew out this theme of balancing rights and liberty further, arguing that there is a different conceptualisation of privacy rights in the US, where they are based on liberty, in comparison to the EU, which focuses on dignity. The issue of migration also arose in Akiko Ejima’s paper, which drew attention to the role of US counter-terrorism policy in shaping Japan’s post-9/11 surveillance practices. Drawing on one of the other workshop themes, Ejima highlighted that the lack of domestic resistance to Japan’s new anti-terrorism laws was a result of their focus on foreigners, not on Japanese citizens, emphasising the ‘us versus them’ nature of surveillance practices that arose in many of the other presentations. The final paper in this session, which was delivered by Gregory Hagen and Maureen Duffy, argued that the conflicting outcomes of similar cases concerning surveillance practices before the US and Canadian Supreme Courts can be seen as a product of the differing approaches that the courts take to constitutional interpretation (for example, the adoption of a ‘living tree’ approach in Canada). The paper also reflected on one of the workshop’s key themes, that of how it is to be determined whether an intrusion into the right to privacy by the state is ‘reasonable’. They argued that the parameters of privacy have changed with emerging technologies and this prompted a discussion on whether the law needs to catch up with to surveillance practices.

**Session 3: Surveillance Regimes – From the National to the Local**

The three papers in session three examined the ways in which states have responded to terrorism through the use of new technological surveillance practices. In particular, the presentations asked who is doing the surveilling and who is being surveilled? The session included two interesting and novel jurisdictions: India and China. Ujjwal Singh described how the Indian state had introduced a range of
new surveillance practices in the past decade, whilst simultaneously lowering human rights protections regarding the use of those practices. He revealed how the practice of intercepting communications had been removed from counter-terrorism legislation and inserted into the permanent Indian criminal law, highlighting another one of the themes of the workshop: function creep. Fu Hualing’s paper on surveillance practices in China revealed the extent to which the Chinese state has reconceptualised security into an ‘all-risks’ approach. This was also examined by Clive Walker in his presentation on local surveillance in UK counter-terrorism practices. Whilst the Chinese state has taken an authoritarian view to an all-risks strategy, the UK has, conversely, attempted to police and surveil terrorism at the local level using the same strategy. These papers posed a number of interesting questions, for example: whether it is better to have laws that breach the right to privacy, or not to have such laws at all; whether surveillance practices are legitimate or even legal; and whether those who practice surveillance can be held to account. These papers also opened up discussion into possible avenues for contestation of surveillance practices.

Session 4: Emerging Models of Surveillance

Day two of the workshop commenced with a paper by Nicola McGarrity and George Williams which outlined the way in which new categories of powers have been bestowed on Australia’s intelligence agencies in the aftermath of 9/11. The presentation highlighted one of the workshop’s key themes; that there has been a seepage of law enforcement powers into intelligence agencies without a concurrent seepage of protections against these powers. Their claim that Australia was an outlier in comparison to four other jurisdictions in this regard (Canada, Israel, New Zealand and the UK) led to a lively discussion as to whether Australia was as unique as they suggested, or whether other states’ law enforcement and intelligence agencies held similar, but unlegislated, powers. Merris Amos also warned against the possibility of function creep in her paper, arguing that the normalisation of surveillance, such as the extensive use of CCTV cameras in the UK, makes it easier to introduce new practices of surveillance. In her presentation, Fiona de Londras highlighted the role of private actors in counter-terrorism surveillance, questioning their impact on constitutionalism in general, defined broadly as power that is limited, transparent and accountable. She argued that privatisation hides surveillance practices from the public, and that those hidden practices cannot be contested. Both de Londras and Amos also addressed
in their papers one of the key questions that arose throughout the workshop, that of who is being surveilled. Amos argued that some are the subject of more surveillance than others, such as migrants at borders, protestors and young black and Asian males; however, de Londras pointed out that the danger in buying into the ‘us’ versus ‘them’ theory is that in reality, with the emergence of new technological models of surveillance, ‘we’ are all being surveilled.

**Session 5: The Constitutional Challenges of Technology**

Session five began with a presentation by Jens Kremer which identified some of the new surveillance technologies currently in use by states, as well as where the future of surveillance lies. Kremer highlighted the important difference in the various processes of surveillance, arguing that the use of mass surveillance systems might not necessarily infringe a person’s right to privacy, but that those rights are likely to be engaged when data from mass surveillance systems is stored, mined, collated, compared, altered, erased or disseminated. The paper highlighted the necessity for these surveillance practices to be contained within the democratic process, in particular by judicial and democratic review, in order to fulfil minimum standards of transparency and accountability. Vanessa MacDonnell’s paper also examined accountability and transparency, but from the interesting angle of popular constitutionalism. MacDonnell explored the example of popular resistance to the enactment of Bill C-30 in Canada (requiring telecommunication service providers to build interception capability into their systems), and argued that popular resistance can shift constitutional meanings. The discussion that followed questioned the extent to which resistance to Bill C-30 can be seen as an expression of popular constitutionalism, rather than simply another political protest movement or, indeed, ‘mob rule’, and raised an interesting issue about whether and how the effects of popular constitutionalism can be limited to movements that are ‘positive’ rather than those that aim to limit rights further. The final paper in the session looked at how the European Union has dealt with emerging technologies in the field of surveillance. It also looked at the issue of transparency and accountability, and its authors, Monica den Boer and Flora Goudappel argued that these have been upheld at the national level, not by the EU, because that organisation is not equipped to deal with these issues at the European level. The workshop theme of balancing rights with security was raised again during the discussion, questioning how the EU
could balance its purpose as a rights protector against its introduction of a range of new anti-terrorism surveillance measures in the aftermath of 9/11.

**Session 6: Surveillance and the Rule of Law**

The final session of the conference commenced with a presentation by the Honourable **Anthony Whealy** QC, former justice of the New South Wales Supreme Court, in which he outlined the various methods by which a judge could ensure that a defendant’s right to a fair trial would not be infringed by new technological surveillance practices. The subsequent discussion centred on his personal experience of balancing these issues in the courtroom, and gave practical form to many of the theoretical concerns that had arisen in earlier presentations. His presentation was complemented by **David Scharia**’s. The latter paper was based on interviews with relevant agencies in a range of jurisdictions, and highlighted the international trend towards the bringing together of prosecutors and intelligence agencies to avoid some of the problems of using intelligence as evidence in court proceedings. For example, the conducting of joint training sessions and the involvement of prosecutors to advise intelligence agencies as to how to collect intelligence such that it will be admissible. Some concerns were raised about the extent to which this trend might taint the prosecutorial process with ‘intelligence values’. The third paper in this session, by **Federico Fabbrini** and **Mathias Vermeulen**, looked at a particular example of how the US Supreme Court and the European Court of Human Rights have approached the right to privacy in the context of police use of GPS surveillance technology – in *Jones* and *Uzun*. Despite the similar facts, the two courts disagreed on whether the defendant’s right to privacy had been curtailed by the extended use of surveillance, and it was suggested in the following discussion that this might have been due of differing conceptions of privacy in the European Convention on Human Rights and the US Bill of Rights.