Regulation, ‘Red Tape’ and the ‘War on Terror’:
Exploring the regulatory aftermath of September 11th

Associate Professor Fiona Haines, School of Social and Political Sciences,
University of Melbourne

Email: fhaines@unimelb.edu.au

Law and Society Association Australia and New Zealand (LSAANZ) Conference
2008 ‘W(h)ither Human Rights’
10-12 December
University of Sydney
Abstract

To date, public debate around human rights and counterterrorism within Australia has focused on changes to criminal law and enforcement that threaten civil liberties. Yet concerns also arise with general security measures concerned with reducing the risk of terrorist attacks at our ports, airports and major infrastructure. New regulatory responsibilities require sites to identify possible methods of attack and to put in place comprehensive risk reduction measures. At ports and airports, tailored security plans, access control regimes, accompanied by screening and monitoring technology, are considered most appropriate to protect both the public and the infrastructure itself. Such measures may well assist in allaying public anxieties about their security from unprovoked and deadly attack. However, this approach is costly and resources used in this way need to be weighed carefully against its effectiveness in increasing security. Despite their initial appeal, security plans and other regulatory initiatives may provide only a limited salve to public anxieties around security. Whilst some level of screening and emergency planning at our ports and airports is appropriate, ever increasing levels of intrusion and resources divert both attention and resources from other initiatives based on tolerance and respect for human integrity that arguably do more to enhance our overall security and wellbeing.

Key words: terrorism, security, risk, regulation.
Introduction

Security and the role of the state in protecting both citizens and non-citizens from arbitrary violence lies at the heart of debates about human rights and civil liberties (Steiner and Alston 2000). How security is provided and whose security is protected from such violence can reveal tensions between victims groups, state authorities (including police and the military) and government concerning what constitutes ‘appropriate’ state action (Carroll 2006; Cox 2004; Humphrey and Valverde 2007). The Australian government response to the terrorist attacks of September 11th 2001 in the United States, for example, has generated significant debate around the protection of human rights in the face of significantly increased police and law enforcement powers (Williams 2003) whilst at the same time proving electorally popular.

Less discussion, however, has been directed at the significant level of resources and heightened level of surveillance that takes place in public spaces, for example at our ports and airports as part of the Australian response to the ‘War on Terror’. Yet the implications of heightened general monitoring and surveillance are significant. In his 1988 finding following the Coronial Inquiry into the Queen Street massacre in Melbourne, the (then) Coroner Hal Hallenstein voiced concern with suggestions that heightened surveillance and monitoring of ‘critical infrastructure’ should be used to protect the community:

To use these (past) events as a standard would not be reasonable and would require application of security measures akin to a permanent stage of siege. It is possible to effect such security measures, but it is neither practical nor reasonable in the ordinary world.

In this paper I ask: What is reasonable in terms of security measures designed to protect us against terrorist attacks? What risk reduction is possible through screening and access controls – and what is not? And critically, what are some of the dangers associated with the dramatic tightening of security regulations, both in terms of reshaping our perceptions of what is reasonable in terms of general surveillance and in terms of the resources expended? Can such measures protect us from attack in the manner suggested by government or do they create a false sense of security that may lead to a continual escalation of measures that have the potential to fundamentally affect human and societal integrity? The paper is informed by ARC funded research into regulatory reform within Australia following the terrorist attacks in the United States on September 11th, 2001.

Terrorist attacks, victimization and heightened fear

Violence aimed at creating terror generates strong emotional responses, heightened levels of fear, anger and anxiety amongst affected communities, irrespective of whether such violence takes place in the context of war or peace, or is perpetuated by government or non-government actors (Carroll 2006; Huddy, Feldman, Capelos and Provost 2002; Humphrey and Valverde 2007; Lerner, Gonzalez, Small and Fischhoff 2003; Spalek 2006). Finding a way through such emotional trauma is central to human wellbeing, a process that involves re-establishing autonomy, finding meaning in the face of tragedy and reasserting personal, and in some cases, territorial control (Spalek 2006).
In the aftermath of high-profile disasters and catastrophes political reform agendas transform these private emotional anxieties and uncertainties into public policy and legal reform. Within a human rights framework attention understandably is focussed on trials or truth commissions. Less discussed are regulatory reforms aimed at preventing a recurrence of catastrophe (Boin and t'Hart 2003; Haines 2009). Yet, there is value in scrutinising such reforms to assess their impact on the nature of our society. In Australia, as in other western societies, regulatory reform is a central feature of contemporary means of recovery from crises (Hancher and Moran 1998), including acts of mass violence, and formed a significant part of Australia’s response to September 11th.

**Regulation as the response to the threat of terrorism**

Regulatory reform can reduce the likelihood of disaster (Reason 1997). Indeed, our current way of life would be impossible without robust regulatory frameworks underpinned by comprehensive risk management processes. But, useful as they are, regulations themselves can also cause problems. Whilst they appeal to our pragmatic, rational selves it is clear that both *when* we regulate and *how* we regulate are fundamentally shaped by political interests, particular values and dreaded fears (Beck 1992; Sunstein 2003; 2005). Incidents that evoke fear or dread, (and this is specifically what a terrorist attack sets out to do) pose particular challenges for a regulatory approach (Haines, Sutton and Platania-Phung 2008; Sunstein 2003). Such regulations can also be costly with benefits and costs unevenly distributed through the population (Sunstein 2005).

The new counterterrorism regulatory regimes in Australia are both extensive and intensive. They require active and ongoing commitment to risk reduction by regulated sites. Security regulations pertaining to ports and airports are ‘co-regulatory’ (Ayres and Braithwaite 1992; Haines 2009) with the regulator, the Office of Transport Security (OTS) developing site specific regulatory requirements in partnership with individual sites. Ports and airports are required to submit to the OTS a detailed security plan based on an assessment and management plan for security risks within the particular location, with designated secure areas that allow only those with the proper security identification card (ASIC or MISC) to enter unaccompanied, together with development of emergency procedures should an attack occur. Finally strict reporting requirements of suspicious occurrences to the OTS are required. Plans are subject to an audit and review procedure by the OTS that may result in additional measures required of sites.

The stringency of requirements, the breadth of their coverage and the rapidity of multiple waves of reform all are noteworthy. In the aviation area, there are two acts: *Aviation Transport Security Act* (2004) as well as the *Aviation Transport Security (Consequential Amendments and Transitional Provisions) Act* 2004, acts underpinned by *Aviation Transport Security Regulations* (2005). In the Maritime area there is the *Maritime Transport and Offshore Facilities Security Act* (2003) also underpinned by regulations. In addition there are considerable international regulatory obligations. For example the current Australian regime must comply with reforms to the International Maritime Organization regulatory regime, in particular amendments to the *Safety of Life at Sea Convention, 1974* (SOLAS Convention) that followed September 11th, and the introduction of the *International Ship and Port Facility Security Code* (ISPS Code).
Commonwealth legislation has undergone multiple revisions. In the aviation area, the Aviation Transport Security Act has been amended four times since 2004. The *Aviation Transport Security (Consequential Amendments and Transitional Provisions) Act 2004* has been amended once. The Aviation Transport Security Regulations have been amended six times since coming into force in October 2005. In the Marine area, the Act has been amended once since 2003, and the regulations six times since 2004.

The costs associated with these reforms are considerable. In 2007 the (then) Attorney General stated that Australia had spent more than $8 billion on security-related measures since 2001 and had budgeted for $10.4 billion for the 10 years to 2010-2011 (Brew 2007), although actual amounts expended may be around $3 billion less (Yates 2007). Annual reports from the OTS with responsibility for security activities at ports, airports and offshore oil platforms for the financial years 2003-4 to 2006-7 revealed a total cost of $219.6 million with costs increasing between $10 and $15 million in each of the three years. The costs for industry are also high. Interviews with airports and analysis of documents revealed that it was not only the costs of new technology, such as explosion detection devices (around $60,000), metal detectors (around $70,000) or x-ray machines (around $100,000) that were extensive (Hall 2007) but ancillary costs such as renovations to accommodate the technology and employment of additional security personnel that could add up to $700,000 in additional costs per annum for each x-ray machine.

These costs to industry, though, are unevenly distributed. For example, airports have a security ranking, based on an assessment of the security risk they face. Airport managers were very aware of the possibility of losing custom and revenue should they be considered at enhanced risk by the regulator. Those designated as counter-terrorist first response (CTFR) faced significantly higher costs, costs ultimately passed on to their customers. Where competition between airports was intense, CTFR airports stood to lose business affecting both their own staff and local communities. There are ongoing debates about who should pay such costs. The government’s preferred argument is that this is simply a cost of doing business. Industry response is that this is a general threat, and so it needs to be a shared burden (Hall 2007).

It is important to clarify here that “industry” represents multiple entities, not all of whom are large and well-resourced. Ports and airports, for example, are run by cities and shires, by not-for-profit entities as well as by private companies. For cities and not-for-profit entities the aim of the service is to support the trade and industry and public needs of a given area, not to make money from the particular activities. In rural and remote areas, too, increased security requirements stretch already tight budgets that can threaten services to local communities.

**Sensible Regulation?**

Highlighting these costs illustrates why it is important to question recourse to tighter and tighter regulation as the preferred method to alleviate public concern. A typical method of questioning the addition of more ‘red tape’ is to call for a more rigorous cost/benefit analysis based on sound data that can inform a considered response (Sunstein 2005; Regulation Taskforce 2006). Assessing costs and benefits seems a logical way to determine the level of security regulation that the public should be asked to fund.
However, the reality of a rigorous cost benefit analysis in the area of counter-terrorism regulation is fanciful. Estimated costs of the impact of an attack might be possible (Yates 2006) but determining the probability with any reasonable degree of certainty is not. Because probability is not able to be calculated, then assessing the benefits and costs of a particular regulatory initiative also is not possible. Interviews with sites revealed a high degree of ambivalence about the possibility of detecting a determined terrorist, irrespective of the level of regulation imposed. Whilst the airports and ports interviewed were confident about their compliance with OTS requirements, they were less sure that compliance had significantly reduced the risk of attack. They recognized the challenge posed by those determined to infiltrate their site and understood well their own particular vulnerabilities.

The security regulators interviewed acknowledged the difficulty, if not impossibility of quantitatively assessing costs and benefits of security regimes. However, they argued that the level of security required was still justified. The OTS based its views on a version of the precautionary principle, namely, that in the face of uncertainty and potentially irreversible harm more regulation is always warranted. Further they argued that the perception of ‘lax security’ might place business at risk making Australia less attractive for needed investment. It was clear, too, through the interviews that threats by the United States to disallow ‘unsafe’ ships entry to US ports was taken very seriously indeed and provided strong motivation to increase regulatory demands on ports in particular. In the absence of accurate assessment of costs what was increasingly relied on was the public, political and business perception of the benefits of enhanced security.

There is a further problem with a risk management/regulatory approach to reducing the risk of a terrorist attack. Regulation is both site and risk specific. But overall reduction cannot work this way, since the potential hazards and potential sites are inexhaustible. Those who were more confident of their level of risk either because of their security measures or by virtue of their marginally level of threat of attack conceded that the real problem lay in displacement of risk of attack to ever ‘softer’ targets. There are the problems of when to stop extending the regulatory regime. What is a weapon? Initially sharp objects including nail clippers were considered potential weapons. Recent regulations have added shampoo, hair gel and toothpaste to this list. Which buildings are at risk, in which city and at what time? Is it Sydney, Canberra, or Melbourne? Is it the port, the airport – or the train station? What chemicals are dangerous? Petrol or LPG tankers? What about liquid chlorine, since releasing the valve on a chlorine tanker in a densely populated area could cause significant harm and the transport of chlorine common?

Conclusion

In short, a terrorist attack is not like an industrial explosion, an earthquake or a cyclone. It is designed to inspire terror, it is intentional and strategic. Minimizing these risks, if done systematically and comprehensively, would be both prohibitively costly and create a fundamentally different society to the society we currently have, it would, in Hallenstein’s terms create ‘a permanent state of siege’. Our current regulations are neither systematic nor comprehensive but shaped by social, political and economic realities (Haines, et al. 2008). Airports have experienced the most dramatic changes. Ports with other locations follow a fair way behind. Yet, there is little reason for this distinction in
any rational evaluation of the risk to Australia. In Australia, shopping malls, particular
during peak sale times, night clubs or packed city beaches in summer make an equally
logical target for attack. The point here is not to inspire fear but to point to the limitations
of a regulatory approach to the problem of terrorism, and to highlight the significant costs
that are associated with what, by all accounts, can only ever be a partial protection.

Given the limited potential for a bureaucratic assessment of the effectiveness of counter-
terrorism regulation there is an urgent need for an alternative method to shift from
reaction to reflection. This reflection must allow us, as a community, to consider what
else might calm our fears around terrorism, arguably in a more robust way. If the
response to terrorism is one of fear, anger, suspicion and avoidance of people and places,
policies need to address our fear, anger and suspicion without promising what cannot be
delivered or fundamentally reshaping what we consider a ‘civil’ society. Funds could be
well spent that allow greater communication and understanding between the diverse
communities in our midst (see for example Borradori 2003). Community infrastructure
and creative local policies, alternative sites of education and communication that enhance
our common humanity make sense.

Let us suppose, for a moment, that Australia will at some time experience the horror of a
terrorist attack. Arguably, this is as likely whether our country pursues an extensive
tightening of control over public space or balances the regulatory impulse with a genuine
attempt to invest resources into policies that replace fear and suspicion with increased
understanding and tolerance. Neither approach can promise a society free from
experiencing the horror of indiscriminate and intentional killing. Clearly, if an attack
occurs, the pain and grief in the immediate aftermath would be equally as intense.

Yet both leave different legacies. In learning from the event, those who experience loss
draw on different societal cues. In the first, victims and their families may rightly feel
betrayed by the (now) empty promise of security and understandably push harder for
greater levels of surveillance, tighter controls and technology measures that themselves
pose threats to our individual and collective integrity. The second, if done well, may
create the space for a different meaning to emerge, anger against those who threaten
vibrant communities and a strong respect for difference, with a determination that those
who wish to inspire fear between neighbours will not succeed.
References


---

1 Material for this paper is principally drawn from research regarding the response to terrorism following September 11th 2001, part of an ARC discovery project entitled “Never again? The nature and effectiveness of Australian regulatory responses to terrorism, the Esso Longford Explosion and the collapse of HIH Insurance”. Interviews were undertaken with relevant regulators: Office of Transport Security (OTS) housed within the Commonwealth Department of Transport and Regional Affairs (DOTARS) later renamed the Department of Infrastructure, Transport, Regional Development and Local Government (DITRDLG) and the Australian Customs Service (Customs). The Australian Federal Police refused a request for formal interview but did meet informally to provide some understanding of the regulatory reforms that pertained to ports and airports. Case studies were then undertaken. There were five airports and three ports in the case study sample, one of each in NSW and the NT, and three airports and one port in Victoria. Airports and ports varied from large facilities with extensive international demands for trade and passenger movements...
to small regional sites with domestic concerns. Case studies were comprised of between one and five interviews on site (depending on the level of access provided) and analyses of annual reports and written documentation provided by the sites’ managers. In the case of airports too, there was analysis of government enquiries where airport management had been required to appear before committees.

This can reach down to the level of reporting doors open into secure areas for example.

One remote site, for example, stated their greatest threat of a breach of the fence around the airport was from local wild buffalo.

This includes the most recent introduction of screening equipment that is able to digitally strip an individual naked.