empowered to search anyone for merely being in the security zone. This will in practice authorise arbitrary searches for those who 'look like a terrorist' and normalise discriminatory practices of racial profiling.

Criminalising charity

The *Criminal Code* (Cth) presently provides for 'financing of terrorism' offences, which make punishable by life imprisonment the provision or collection of funds by a person who is reckless as to whether the funds will be used to facilitate a 'terrorist act'. The Bill extends the operation of these offences to those who collect funds either directly or indirectly for or on behalf of a terrorist organisation. Well-intentioned charitable work could easily fall foul of the extended offence.

A host of other measures in the Bill operate to give unaccountable and unjustifiable power to police and the executive. The AFP will have extensive powers to compel production of personal and private documents without judicial supervision. ASIO search and monitoring warrants have been extended to double and in some circumstances triple duration of operation of time from 28 to 90 days, and from 90 days to six months.[16] This excessive extension erodes key safeguards against 'fishing expeditions' and reduces the degree of oversight to which ASIO is currently subject.

Conclusion

The proposed laws place serious limitations on existing rights and freedoms that underpin Australian democracy including:

- the presumption of innocence
- the right to privacy
- everyone's right to be considered equal before the law
- everyone's right to freedom of political and religious association and belief.

The Bill contains inadequate details about the limitations on the scope of the laws, the circumstances in which they could be employed and who will possess the powers to exercise them. In spite of the announcement of a 'potential terrorist threat' just before the Bill's introduction, the government has not adequately explained why the current expansive counter-terrorism laws are insufficient to deal with such a threat and how these measures, with their severe curtailment of rights and freedoms are proportionate to the current threat. It is worth nothing that the National Counter-Terrorism Alert Level has remained at 'medium' since September 2001. This means that the government has assessed that a 'terrorist attack *could* occur'. It does not mean that a 'terrorist attack is *likely*' ('high' level of threat) or that a 'terrorist attack is *imminent* or *has occurred*' (extreme level of threat).

The proposed 10-year sunset clause does not constitute accountability and should be set at most at three years with full open parliamentary review, as was the case with the *Australian Security Intelligence Organisation Amendment (Terrorism) Act 2003* (Cth). While some minor amendments have been made, the lack of meaningful judicial safeguards leaves the Bill open to misuse. A focus of concern on judicial oversight, however, obscures the primary objection that these laws are draconian measures. At their core, the laws transform basic assumptions about what constitutes criminality. Presumptions of guilt based on category and association favour the targeting of political opinion and behaviour deemed as 'suspicious' by ASIO, the police and the executive. While the government argues Muslim communities are not being targeted, the laws create discretionary mechanisms that will in practice mean that chiefly Muslim and Arab individuals and communities will be at risk of being racially and religiously profiled.

ANNIE PETTITT and **VICKI SENTAS** are doctoral students in the Department of Criminal Justice and Criminology, Monash University.*

16. For example, the duration of search warrants is extended from 28 days to 90 days, and warrants for the inspection of postal articles and delivery services from 90 days to 6 months: Anti-Terrorism Bill (No 2) 2005 Schedule 10.

* The authors are two of the co-authors of *Laws for Insecurity?* Annie is also co-convenor of the National Human Rights Network of the National Association of Community Legal Centres and Vicki is spokesperson on terrorism laws for the Federation of Community Legal Centres (Victoria).

Useful websites
http://amcran.org
http://www.civilrightsnetwork.org

WORKPLACE SURVEILLANCE

A proposed regulatory model for Victoria

PRIYA SARATCHANDRAN reports on the VLRC's report into privacy and workplace surveillance, and its proposed Workplace Privacy Act.

Almost daily, there are media reports of privacy invasions in many spheres of public life, including the workplace. The modern labour force has changed and now includes multiple, global, mobile, and cyber workplaces. A parallel development has been the rapid advance of surveillance technologies, which are more available and affordable to employers than ever.

The 'creeping' of surveillance into the workplace raises fundamental questions about workers' rights to autonomy and dignity, and the kind of workplaces our society finds acceptable.[1]

The widespread use of surveillance and other privacy-invasive practices in the workplace was the subject of the Victorian Law Reform Commission's workplace

REFERENCES

1. For a detailed discussion see Kate Foord, *Defining Privacy* (2002).

privacy reference, which concluded in October 2005. This was the first inquiry of its kind in the world. The Victorian Attorney General asked the Commission to consider the benefits and risks posed by a wide range of potentially privacy-invasive practices in Victoria. As well as surveillance, medical, alcohol and drug, psychological and genetic testing, and searching of workers, were considered. This article focuses on the recommendations on surveillance.

The Commission adopted a human rights framework in conceptualising privacy.[2] However, like other human rights, privacy is not an absolute right. For example, federal and state anti-discrimination legislation does not provide for absolute rights, but rights subject to certain exceptions. Workplace privacy is no different. The workplace is a site of complex, often competing, interests.

Consultations revealed that employers use surveillance to protect property and control computer equipment, measure performance and productivity, reduce the risk of legal liability, gather evidence relevant to legal issues and maintain safety and security.[3]

Unions told us that the use of such practices led to concerns about workers' autonomy and dignity being undermined, lack of transparency about what/why practices were being used, practical difficulties in a worker's ability to withhold consent to such practices, the blurring of the distinction between workers' private and working lives, and potential discrimination.[4]

Surveillance practices

The Commission defined 'surveillance' to include audio and video surveillance, email and internet monitoring and tracking.

While Victorian surveillance legislation covers video, audio and tracking surveillance, these practices can be used by employers with the consent of workers.[5] In the context of unequal bargaining power within the workplace, the ability of workers to genuinely consent is questionable. Furthermore, the legislation only protects activities that are considered 'private' — a concept that is open to interpretation in the workplace context. Protections relating to monitoring by employers of Internet and email use are virtually non-existent in Victoria, and application of relevant federal laws is uncertain. There is also confusion about whether biometrics and other technologies are covered by state surveillance laws. Limited information-privacy protections exist for certain workers, but such legislation does not address the employers' use of the practice in the first place.

Commission's findings[6]

The Commission found that the existing legal regime was inadequate in balancing the interests of workers and employers. The patchy nature of existing laws and the permeation of various technologies into the market had resulted in lack of guidance for employers and workers. The Commission also had concerns about the overall social effect of technology on workers' lives and rejected the notion that worker consent was a sufficient safeguard.

Proposed regulatory regime[7]

The Commission recommended that a Workplace Privacy Act be enacted and administered by an independent regulator. The main concepts underpinning the proposed regulatory model were the need to balance the interests of workers and employers and to match the regulatory response to the seriousness of the privacy intrusion.

In the Commission's draft Bill, an obligation is placed on employers not to unreasonably breach the privacy of workers while they are engaged in work-related activities. A set of principles is included to clarify the nature of the obligation. This includes establishing that the use of a practice is for a purpose directly connected to the business and is proportionate to the risk being managed. Adequate safeguards must be instituted and workers must be informed and consulted.

The principles are supplemented by codes of practice. Such codes set out the practical detail for employers and workers on how practices should be used. If a worker makes a complaint about an employer's use of a practice, compliance with an advisory code can be a defence to the claim. For example, overt surveillance will be covered by advisory codes of practice.

Because covert surveillance was seen as a more serious invasion of privacy — due to the element of 'entrapment' of workers — it will be covered by a mandatory code. While the Commission acknowledges that certain forms of overt surveillance can be oppressively used, covert surveillance does not give workers the opportunity to modify or change their behaviour. Employers must comply with the requirements of a mandatory code in order to defend a complaint.

In Victoria, there are few restraints on employers surveilling workers, even when they are not working. The Commission regards invasions of privacy in the non-work-related context as a serious invasion of privacy, and has recommended that prior authorisation from the regulator must be sought by employers in such circumstances. This means that in the absence of an authorisation, surveillance of workers when they are not working is prohibited.

The Commission has included home-based work in its definition of 'non-work related', given that privacy intrusions into a worker's home, and particularly of other household members, would represent a serious privacy intrusion. The one exception to this is using the employer's communication system from home (or wherever it is located). This will be treated as a work-related activity because legal liability for discrimination, harassment and copyright breaches may still attach to an employer through the misuse of its communication system.

The Commission has also imposed a complete ban on the surveillance of workers in toilets, washrooms,

2. For detail on the Commission's 'human rights approach', see Victorian Law Reform Commission, *Workplace Privacy Options Paper* (2004) paras 1.5–1.6.

3. For employer perspectives see ibid paras 3.9–3.47.

4. For worker perspectives see ibid paras 3.52–3.101.

5. For detail on the regulation of such practices see ibid ch 2.

6. For detail on the Commission's findings see Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005) ch 2 <www.lawreform.vic.gov.au> at 29 November 2005.

7. For detail on the proposed regulatory regime and draft Bill see ibid ch 3 & 4, Appendix 5.