Law Protecting citizens from threats such as terrorism can lead governments to impinge on civil liberties, so proper oversight is more vital than ever, writes **James Renwick**.

Safety vs freedom: getting the security balance right

Tensions. The ACT Court of Appeal has overturned a secrecy order in the trial of lawyer Bernard Collaery
PHOTO: ALEX ELLINGHAUSEN

Alexander Hamilton is now famous because of the award-winning musical that bears his name. But as a key founder of the United States constitutional system he wrote in the Federalist Papers a prediction which resonates today: "Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates ... To be more safe [nations] ... become willing to run the risk of being less free."

In the 20 years since 9/11, Australia has enacted over 130 pieces of national security legislation. Many of those laws created new criminal offences and exceptional investigative powers. While often controversial in principle and almost always contestable as to their terms, they seem to have become permanent.

So where does Australia now sit on the spectrum between safety and freedom?

The essential task in a democracy of defining then maintaining the legal, human rights and ethical boundaries of this new frontier in the law is hard.

Determining whether a law is necessary and proportionate given actual or reasonably likely threats is challenging because key threats, while serious if carried out, are complex and often opaque.

These laws create significant issues for each branch of government – including the courts – and for society as a whole.

At the time of 9/11, Australia had few national security laws and no counter-terrorism laws. Since then, over 130 of them have been enacted and 92 people have been convicted of terrorism-related offences. Since September 2014, when the national terrorism threat level was raised, 143 people have been charged as a result of 70 counter-terrorism related operations in Australia.

The laws were often made in response to some of the most shocking events of our times, such as the destruction of the twin towers, the Bali bombings, the 2014 Lindt cafe siege in Sydney and the mosque shootings in Christchurch in 2019. They also followed unsettling revelations of espionage and foreign interference in recent years.

The Australian approach of legislating in response to a significant terrorist attack differs from Britain, which is more likely to focus on strengthening the enforcement of existing laws.

The time spent on considering laws in draft before they are enacted in Australia is also becoming ever shorter. The original anti-terrorism laws in 2002 took many months to be considered before enactment. The law preventing live-streaming of terrorist acts introduced after the Christchurch massacre took a week or so. Speed in passing laws can sometimes be necessary but it brings risks of error and overreach.

The most recent laws focus on the dual nature of the internet: it is essential for full participation in our society for lawful ends, but it is also increasingly used by criminals, hostile nation states and their proxies.

As Sir David Omand, the former head of Britain's electronic intelligence agency GCHQ has said: "The Internet, and the World Wide Web that it carries, were not originally designed with security in mind, and many seek to exploit this weakness for their own antisocial, criminal, or aggressive ends." Hence, the need for laws to protect critical infrastructure, or warrants to authorise computer access, data disruption, or network takeover.

Both in the UK and in Australia, the primary threat of terrorism was and remains radical Islamism. But radical right-wing terrorism activity has now almost caught up. It also seems likely that the COVID-19 lockdowns will leave some of those experiencing social isolation and financial hardship more susceptible to radicalisation online.

A significant trend is for terrorism to be planned and carried out by lone actors rather than as part of a co-ordinated group, although sometimes these individuals simply assert that they are acting in the name of an existing terrorist group.

And rather than bombs and firearms, attacks increasingly involve the use by lone actors of an everyday item, such as a knife or a car, to randomly murder people or to maim them. But the future may include directed acts of bio-terrorism (such as the UK's Salisbury Novichok poisonings), or disruption to critical infrastructure such as a telecommunications or electricity network.

The time between an offender's deciding to conduct an attack and acting on that decision has markedly decreased from a decade ago, making the work of police and intelligence agencies far more difficult.

Take the 2017 London Westminster Bridge attack where, without warning, the attacker drove his car at high speed across that bridge injuring 50 people, five of whom later died, before crashing his car at New Palace Yard, stabbing a police officer to death, and then being shot dead himself. The entire attack took 82 seconds.

The New Zealand supermarket attack last month involved a closely monitored person still being able to take a knife from a super-

market shelf and injure seven people before being swiftly shot dead.

The spectre of a simultaneous terrorism attack on more than one target – of which the 2015 Paris "Bataclan" triple attack remains one of the worst examples – is of great concern to police and intelligence authorities and one for which they must prepare.

And although espionage is hardly new, its scale and scope together with foreign interference against Australian interests have been described as "unprecedented", and the new laws are evidently being used to confront these activities.

But these laws can be challenging to justify publicly. Espionage and illegal foreign interference is clandestine and attributing hostile acts to a particular foreign state or its proxy may be technically difficult. Even if that can be done, it may be undesirable to identify the offending because it will cause a diplomatic rift or because this will reveal our counter-espionage capacities in a way which weakens them.

There are serious challenges which test even the most senior judges in both Australia and the UK. These include:

Publicity: If the terrorist act has taken place (rather than being stopped in the planning stage), there may be much unavoidable and adverse publicity and the jury needs to be firmly but carefully instructed to put that aside to ensure a fair trial;

Complexity and volume of material: The Crown material will often include immense quantities of metadata, video, emails, and other electronic materials which, to complicate matters further, may be encrypted or in a language other than English;

Adequacy of disclosure: A frequent argument in criminal trials is whether the Crown has disclosed to the accused all that it should have, for example, material that runs counter to the prosecution case or which might mean the jury doesn't accept the evidence of a prosecution witness. As Sir Brian Leveson, when President of the Queen's Bench Division and Head of Criminal Justice, said: "Technology serves an increasingly vital function in our society, but these facilities have created one of the greatest challenges ever to be faced by the criminal justice system: that of disclosure."

Court Closure: The English court system, like ours, is designed for openness, but it is often necessary to protect secret intelligence and police sources and methods, to rule on immunity (and exclude material) or to make non-publication and court closure orders for evidence. But as (former justice and Inspector-General of Intelligence and Security) the late Margaret Stone wrote: "The tension between secret intelligence and civil rights and liberties is not reconcilable; inevitably, secrecy threatens rights, and rights weaken secrecy."

The decision of the ACT Court of Appeal last week in the prosecution of Bernard Collaery is a recent example of the tensions at work. The judgment summary states: "The open hearing of criminal trials was important because it deterred political prosecutions, allowed the public to scrutinise the actions of prosecutors, and permitted the public to properly assess the conduct of the accused person."

Hence, its apparent decision (reasons are not yet available) that there will be a "risk" but not a "significant risk" of "prejudice to national security" if certain matters are revealed.

Australian judges face additional problems. Some are inherent in the federal system. This relies upon criminal trials of federal offences in state courts "picking up" differing state laws about criminal practice and procedure, even though, as former Justice Michael Kirby writes, a federal offence is, in effect, an offence against the whole Australian community. It can be difficult to work out which state laws are picked up, and federal trials can look quite different depending upon where an accused is tried.

And because there are no federal jails, there are differences in how terrorist offenders are dealt with: one state disperses them among the general prison population, another puts them all in a "supermax".

And Australia's excessively complex sentencing laws greatly extend the length of remarks on sentence and provide more scope for arguing error on appeal. The UK's sentencing laws appear far simpler but no less effective than our own.

Former UK Reviewer Lord David Anderson QC has said: "Public consent to intrusive laws depends on people trusting the authorities, both to keep them safe and not to spy needlessly on them ... Trust in powerful institutions depends not only on those institutions behaving themselves (though that is an essential prerequisite), but on there being mechanisms to verify that they have done so."

On public trust, the UK and Australia have a similar approach. In addition to the indispensable role of our independent judiciaries in conducting criminal trials, and the vital work of an alert and thoughtful media, each country has three key types of oversight: the parliamentary committees, the intelligence service overseers, and the independent legislation monitors/reviewers.

The key parliamentary committees are the UK's Intelligence and Security Committee and the Australian Parliamentary Joint Committee on Intelligence and Security. In contrast to the UK, the PJCIS includes senior national security shadow ministers who are thereby better prepared to assume such ministerial roles on any change of government. Its workload is heavy: at least 25 reports finalised in the current Australian Parliament, and a dozen live inquiries, against a background of constant urgency.

Inevitably, secrecy threatens rights, and rights weaken secrecy.

The late Margaret Stone, former Inspector-General of Intelligence and Security

The UK has the Independent Reviewer of Terrorism Legislation, and in Australia the Independent National Security Legislation Monitor (INSLM). Each measures the operation of such laws against standards of necessity, proportionality and human rights, and regularly reports to the government. In Australia the INSLM has royal commission powers, seeing everything of relevance regardless of security classification, holds public inquiries and provides reports which must be promptly tabled in Parliament.

Meanwhile, the IGIS deals with any complaints about the activities of Australia's intelligence community and has complete and constant access to relevant personnel, premises and information. Investigating complaints and regularly auditing the use of powers, it measures intelligence activities against standards of legality, human rights and propriety.

The IGIS is rightly regarded as a vital means of retaining public trust, and although it has recently expanded its personnel and reach, it is slightly different to its main UK counterpart, the UK's Investigatory Powers Commissioner's Office (IPCO).

IPCO is not only the auditor of the covert use of investigatory powers, (although complaints go to a Tribunal) but, under a *double lock* system, must approve the most intrusive search warrants by testing them for necessity and proportionality. IPCO consists of senior retired judges who have access to the best technical advice.

In contrast, in Australia, search warrants (except for ASIO, whose warrants are issued by an increasingly busy Attorney-General) are issued by equally busy judges and tribunal members. By a thin constitutional fiction, they are said to issue them in their personal capacity, and in fact get no assistance from the court or tribunal of which they are part.

They act randomly and infrequently and, as a result, have no capacity to build up expertise in particular types of warrants or technology. They also have no access to specialist technical advice and, save for the rare judges with computer science degrees, must find it very difficult to understand whether what is proposed will minimise impacts on legitimate uses of a mobile device, computer or network, or to shape the terms of the warrants to best maintain the protections available to important interests such as privacy, legal advice, parliamentary privilege or journalism.

And keep in mind what technology can reveal: obviously, readable content and images on our mobile devices reveal much about our daily interactions and thoughts. But don't forget metadata – a 2018 US Supreme Court case said metadata did not only reveal where the phone user had been, and what he had searched for on the internet, but through it, the user's "familial, political, professional, religious, and sexual associations".

Lest Hamilton be proved right, national security law, its content, boundaries and oversight, should remain a concern for all of us – whether lawmaker, legal professional or interested member of the public – and so the important output of the oversight bodies in the UK and Australia deserve greater attention. R

Dr James Renwick CSC SC is a Sydney barrister, an Honorary Professor at the ANU and a former Independent National Security Legislation Monitor (2017-2020). At the request of the General Editor Justice Francois Kunc, he was Guest Editor of the ALJ Special Edition on National Security and the Law published on Thursday by Thomson Reuters.

Journal. The special national security issue of the *Australian Law Journal* (left).