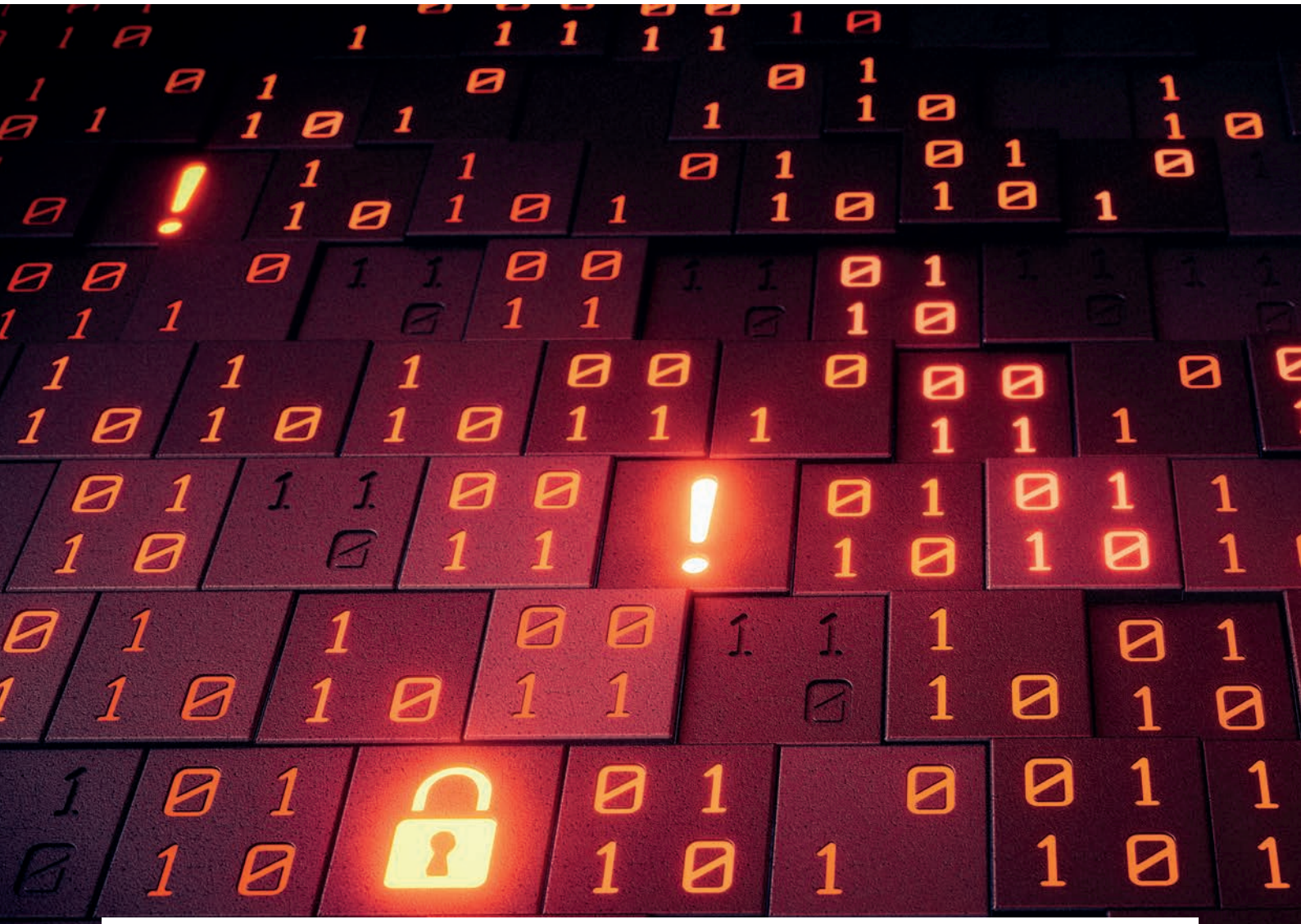

Legal hacking – why not?

BY PROFESSOR BRIAN MARTIN, EMERITUS PROFESSOR, UNIVERSITY OF WOLLONGONG, AND AISA MEMBER

A new law gives police extraordinary powers for disruptive hacking, which will harm security and Australian businesses.

Brian Martin

Imagine that you are tasked with purchasing database software for your organisation. Two promising options are from Belarus and Belgium. The Belarus product is cheaper, but then you learn that Belarus is a dictatorship that spies on its citizens. You worry that the Belarus software may not be totally secure, so opt for the Belgian product.

Government repression can be bad for business. The *Defence Trade Controls Act 2012* has severe controls over Australian military-related and dual-use research, including computing research. It allows the Department of Defence to take over intellectual property. High-tech entrepreneur Brendan Jones was one target; he ended up leaving the country.[1]

Then came the law enabling Australian agencies to demand access to encrypted communications. This was opposed by the tech sector on the grounds that customers would not trust Australian products to be secure. Industry pleas were ignored.

The latest law is the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021, which was recently passed.[2] It enables the Australian Federal Police and the Australian Criminal Intelligence Commission to obtain warrants to access the accounts of targets – including email and social media – and to add, change or delete data. Remarkably, this legalises what might otherwise be called malicious or black-hat hacking.

This hacking law was passed with support from both major parties. There was limited consultation, and advice from expert bodies was ignored.

The danger to the tech industry is obvious. Whatever the intent of the law, and however it is used, the perception will be that Australian products cannot be trusted. Software might have been tampered with, databases might be corrupted and back doors might have been inserted. Because accounts can be commandeered, even the authenticity of messages may be in doubt. These worries might be unwarranted, but, like the hypothetical Belarus example, perception can be just as influential as reality.

It is well-documented that police with access to databases on citizens can be bribed, often on a regular basis, by private investigators seeking information. And some police misuse their access for personal reasons – for example, to stalk an ex-partner. Imagine the attraction that hacking powers will create for mission creep and individual abuse.

TACTICS

Around the world, powerful perpetrators of injustice – for example, illegal surveillance, sexual harassment, police beatings and massacres – try to reduce public outrage about their actions.[3]

A crucial technique is cover-up. The hacking law provides severe penalties for revealing any operations. When people don't know what agencies are doing, they won't be upset.

Another outrage-reduction technique is reframing: namely, describing the action in a favourable way. The rationale for the hacking law is to counter criminal activities, such as paedophile rings – surely a worthy goal. This distracts attention from the lack of specificity in the law – it can be used more widely.

A third technique is devaluation. The government's rhetoric suggests that anyone opposed to the law opposes action against criminals.

Then there is intimidation. Exposing hacking operations can lead to 10 years in prison. On top of this is a plausible fear that those who speak out might themselves become targets of surveillance.

The government has followed the playbook of other powerful perpetrators, and the damage to the tech industry is an afterthought. Implicitly, industry concerns are devalued – that is, if they receive any attention at all.

Looking at these methods to reduce outrage over injustice points to counter methods: expose the adverse actions, counter rationales, frame legal hacking as an injustice, have respected individuals and groups give credibility to concerns, and stand up to intimidation. There is an alternative. Like Brendan Jones, you can give up on Australia – or you can resist. Resistance against legislation that overreaches requires voices – particularly those from industry. This is exactly the sort of legislation that the Australian Information Security Association (AISA) – in partnership with its sister associations across the business community – should speak up against in public venues. •

A theoretical physicist by training, Brian Martin is Emeritus Professor of Social Sciences at the University of Wollongong, and the author of 20 books and hundreds of articles. He has a special interest in free speech and organisational dissent.

References

1 *Brendan Jones, 'Defence takes control over Australian research,'* Australasian Science, *April 2016*

2 *https://bit.ly/3pDrqPQ*

3 *'Backfire materials,' https://www.bmartin.cc/pubs/backfire.html*