Dutton’s Record: Building the Surveillance State in Australia

By Ugur Nedim
Asia-Pacific Research, June 01, 2022
Green Left 31 May 2022

Region: Oceania
Theme: Justice

***

*When **Peter Dutton** confirmed his candidacy for the leadership of the Liberal Party the public relations campaign to “soften” his image went into overdrive.*

The so-called “hard man” says he is keen to show the public “the rest of my character, the side my family, friends and colleagues see”.

As traditional Liberal voters turn away from the party, Dutton wants us to know what he believes in. “We aren’t the Moderate party. We aren’t the Conservative party. We are Liberals. We are the Liberal party. We believe in families – whatever their composition”, he said.

Dutton’s leadership of the Liberal Party is a concern given his demonstrated commitment to eroding democratic principles including: the separation of powers; basic civil rights such as privacy; personal freedom and free speech; government transparency and accountability; as well as suppressing dissent and prosecuting state crime and corruption.

It would require a thesis to adequately detail the dozens of pieces of rights-eroding laws and hundreds of amendments to existing laws championed by Dutton in his various portfolios as minister for immigration, home affairs and defence.

Below is a thumbnail sketch of the slippery slope into authoritarianism, in which Dutton has played an instrumental part.

Building the surveillance state

Supporters of civil liberties, such as Edward Snowden, sometimes use the phrase “without

privacy, there is no freedom" when discussing the proliferation of state surveillance in modern societies.

The ability to freely communicate without arbitrary monitoring and a fear of prosecution is essential to a healthy democracy.

However, supporters of privacy-eroding laws, under the guise of protection against perceived and, often exaggerated, threats will often use phrases such as "you have nothing to fear if you have nothing to hide".

The "need" to protect us against terrorists has been used to justify many laws which have turned Australia into one which has the most pervasive surveillance laws of any Western democracy.

When Snowden exposed the United States National Security Agency's illegal surveillance of its own citizens, the Coalition government passed many draconian laws giving the state and its agents more powers. Dutton played an integral role in their formulation, advocacy and passage into law.

Without a national bill or charter of rights there has been little to stand in the way of these laws being enacted.

These laws include:

1. Compelling internet service providers to store user data and hand it over on request.

The meta-data retention laws, passed in 2015, were marketed as necessary to protect against the threat of terrorism.

They require internet and phone service providers (ISPs) to store your personal data for two years and make it available to a range of law enforcement agencies without those agencies having to obtain a warrant.

Similar laws were proposed, but rejected, in Britain due to their arbitrary and pervasive nature. They have not been enacted in any other Western country.

You don't have to be suspected of an offence for authorities to access and monitor at least two years of a range of your personal data.

Meta-data includes: telephone records; the time and length of phone calls; the internet protocol addresses (IP addresses) of computers from which messages are received or sent; location of parties making phone calls; to and from email addresses on emails; logs of visitors to chat rooms online; status of chat sites — whether they are active and how many people are participating; chat aliases or identifiers (the name a person uses in a chat room online); start and finish times of internet sessions; the location of an individual involved in communications, and the name of the application someone uses online and when, where and for how long used.

Meta data does not encompass the actual content of communications and ISPs have made it clear that filtering content, such as text in SMS transmissions, and emails for such a large number of users would be a mammoth and potentially impossible task.

The concern is that all of a user's requested data would be provided to authorities and there is currently no information regarding whether or not this is happening.

There is no evidence to date that the laws have proven to be an effective mechanism against terrorists. There is, however, evidence that the laws are being used by a range of agencies not involved in the detection or prosecution of terrorism; agencies that can apply under the laws to access the personal data.

It was revealed that in 2018 more than 60 government agencies applied to the Attorney-General for metadata access. The list included the Australian Taxation Office, Department of Human Services and even local councils. Bankstown Council applied for metadata access in an attempt to catch illegal rubbish dumpers and those who breach by-laws. That access was granted.

The Queensland Police Service used the scheme to access the metadata of cadets in an attempt to determine whether they were sleeping with one another, or faking sick days.

The Australian Federal Police (AFP) has used meta-data laws to access information given to journalists and even doctors to identify their sources — whistleblowers who expose crime and misconduct within government agencies.

Indeed, the AFP admitted in 2019 to accessing the meta-data of 20,000 people over the previous 12 months — without having to inform its targets, let alone justify its conduct.

2. Compelling technology companies to provide encryption keys to access user data

In another unprecedented move, Dutton championed laws enacted in 2017 which compel technology companies, such as Facebook, Google and Apple, to surrender their encryption keys to the accounts of Australian individuals and organisations upon service of a warrant and to even alter, or delete, the information.

The laws were passed with little public scrutiny, and have since been used to access the accounts of not only individuals, but news organisations.

The laws were condemned here as well as overseas, with *ABC* News executive editor John Lyons tweeting during the 2019 raids of its Sydney office: "I'm still staggered by the power of this warrant. It allows the AFP to 'copy, delete or alter' material in the ABC's computers. All Australians, please think about that: as of this moment, the AFP has the power to delete material in the ABC's computers. Australia 2019."

A group of United Nations special rapporteurs expressed concern the law would "disproportionately chill the work of media outlets and journalists by exposing human rights campaigners, activists and academics to criminal charges and, in doing do, contravene the International Covenant on Civil and Political Rights".

3. Increased search, seizure, detention and compelled disclosure powers at the border

Dutton played a pivotal role in the enactment of the *Australian Border Force Act* in 2015, which gave officers of the Australian Border Force (ABF) frighteningly broad and indeterminate powers "to do all things necessary or convenient to be done for or in

connection with the performance of his or her duties". This includes broadened powers to search and detain travellers and to seize their personal items.

Dutton oversaw amendments in 2018 which made it a crime, punishable by up to five years in prison, for such persons to decline to provide passwords to their smartphones, computers or other electronic devices – enabling access to all the private information.

That same year, Australia made headlines when dual British and Australian citizen, 46-year software developer Nathan Hague, was detained for 90 minutes and had his devices seized at Sydney Airport, without being given a reason.

The devices were returned weeks later without further action being taken against him. Authorities refused to provide information about whether the digital data was copied and stored as the legislation permits.

An incensed Hague told the media at the time: "I have nothing to hide, but I value my privacy".

4. Accessing overseas data

Home Affairs Minister Dutton in 2020 ensured the enactment of laws to empower the Australian Security Intelligence Organisation (ASIO) to access the data of Australians stored overseas while, at the same time, allowing other members of the Five Eyes Alliance to have access to that data.

The laws established a regime of international production orders, which allow agents to directly require foreign designated communication providers to hand over stored communications and data, and even enable direct wiretapping.

According to Civil Liberties Australia CEO Bill Rowlings: "We've had nearly 20 years of draconian laws — many totally over the top – and most absolutely slashing personal privacy … Dutton and the henchmen have all the laws they need already. This is overkill … Without a federal charter of rights, there has been nothing protecting the basic rights of individual Australians."

That's the overriding problem: Australia is the only Western democracy without a national bill or charter of rights that could obstruct such intrusive invasions of privacy.

5. Identify and disrupt – power to hack accounts and delete, add or alter data

Described as "the nail in the coffin of democracy", so-called "identify and disrupt" laws enacted last December 3 are perhaps Dutton's pièce de résistance in terms of surveillance legislation.

The laws give the AFP and Australian Criminal Intelligence Commission the power to collect intelligence online, including over the dark web, disrupt online activity by manipulating data and even to take over a person's online account – locking them out of it –to "gather evidence".

Again, this is unprecedented in the West. Authorities can now legally hack and enter accounts and essentially do whatever they please with the data contained therein — including delete, add or alter content.

The potential implications are frightening.

Rowlings said: “The new laws allow faceless federal agents to ‘target and destroy’ people, under what is officially called the *Identify and Disrupt Bill*. This awful law multiplies tenfold the powers and reach of government intrusion. Police have such an appalling record throughout Australia of planting evidence and wrongly locking up people for years and decades. Why wouldn’t they plant more ‘evidence’ to suit themselves now they are permitted to do that officially?”

Slippery slide into authoritarianism

These are just five of many surveillance laws overseen by the Liberal Party’s new leader.

The rapid degeneration into such a pervasive regime of surveillance — often under the threat of criminal sanctions — would have been the envy of past dictators.

It could not have been foreseen by authors such as George Orwell. Indeed, the “Thought Police” in Orwell’s iconic novel *1984*, published in 1949, would have relished the ability to arbitrarily monitor and intercept information transmitted through and recorded on devices as integral to our daily lives as mobile phones and computers have become.

As Rowlings said: “The police and spooks of Australia now have more powers and can reach further inside people’s lives and minds than the notorious Stasi of East Germany ever could.”

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

***Ugur Nedim** is a partner of Sydney Criminal Lawyers where a longer version of this article first appeared.*

Featured image is from Green Left

Articles by: **Ugur Nedim**