Proposed: Australia's Anti Mass Surveillance Policy

Terrorism and criminal organisations are real problems. However, the government's response to indiscriminately spy on Australians is disproportionate to the risk. Likewise, the government's mass surveillance laws enable warrantless access to data, grant the government access to private organisations' networks and IT systems, and enable to government to take over Australians' online accounts.

End Mass Surveillance

Government mass surveillance has steadily grown, especially after 9/11. Mass surveillance laws aren't justified, are often rushed through parliament without scrutiny, and treat Australians as guilty without evidence. These laws concentrate too much power in the hands of government.

- **Abolish mass surveillance laws.** Mass surveillance laws are unnecessary & steadily grow, especially after terrorist attacks. When the next terror attack happens, governments demand even more power.
- **Stop government hacking and seizure.** The government can add, copy, delete or alter data on Australians' devices, take over online accounts, and gain access to private networks. These powers are unnecessary and enable the government to plant evidence on Australians.
- **Devolution of surveillance laws to states and territories.** After 9/11, surveillance laws were federalised, granting the federal government too much power over Australians. A return to states and territories handling surveillance laws distributes and dilutes power, ensuring Australians aren't indiscriminately targeted.
- **Stop the collection of metadata.** Despite government promises, metadata collection has expanded to local councils. The collection of metadata treats Australians as guilty without having committed a crime.
- **Ensure warrants for targeted surveillance of individual Australians.** Surveillance must only occur after a warrant has been approved for specific individuals. The judicial system is an important bulwark against government overreach.
- **No cash bans.** Cash bans enable government surveillance by forcing Australians to pay for goods and services with traceable bank-issued payment methods (e.g., debit cards). To protect privacy, Australians must be able to trade with each other without government surveillance.

Freedom of Speech

Freedom of speech is one of the most fundamental rights. Attacks on encryption from government occur regularly. In order to hold politicians to account, Australians must be able to talk to each other without the government knowing who is talking to whom and about which subjects.

- **Abandon 100 points of ID for SIM cards.** The 100 point requirement for SIM cards is disproportionate to the risk. The US and UK have no such requirement, and Australians must be able to talk to each other without the government knowing.
- **Abandon consideration of 100 points of ID for social media and other Internet services.** The government is considering requiring Australians to prove their identity for online services. This will limit whistleblowers, those who face repercussions for speaking out, and create a culture of fear rather than allowing anonymous accounts.
- **Stop attacks on encryption.** The government -- along with the US, UK, Canada, and NZ -- continually attempts to undermine encryption through laws that can weaken security & by promoting backdoors. Australians must be able to talk to each other without the government knowing.
- **Stop the government from deplatforming speakers.** In 2019, the Australian Signals Directorate banned two speakers at the Australian Cyber Conference. It's inappropriate for intelligence agencies to ban speakers who are presenting about mass surveillance and whistleblowing. The government deplatforming speakers is a direct attack on free speech and must not be tolerated.
- **Protect the media and whistleblowers.** The media and whistleblowers must not suffer police raids for reporting on intelligence agencies. Police raids have happened multiple times in the last few years.
- **Stop police from forcing Australians to unlock their devices and hand over their encryption keys, passwords.** Police must not be able to compel speech or require Australians to incriminate themselves. Likewise, police access to devices opens the possibility of indiscriminate access to Australians' data.

Freedom of Movement

Freedom of movement is one of the most fundamental rights, enabling Australians to move freely around the country. However, the government continually adds more and more technology to track Australians.

- **Stop monitoring Australians.** Police departments have continually expanded their means to monitor Australians' movement. This includes drones, helicopters, and specialist surveillance equipment. This technology undermines the right to protest, is open to abuse, and indiscriminately targets Australians.

- **Reduce CCTV.** Limit the number of CCTV cameras in public areas (e.g., public transport).
- **Reduce ANPR.** ANPR – automatic number plate recognition – tracks Australians' vehicles on the road. The government should reduce the number of government-run ANPR cameras. Private toll road operators – leasing roads from governments – must provide anonymous payment options in order not to be tracked.

Limit Government Data Collection

The government collects more and more data on Australians every year. The danger is government misusing the data, using the data to target Australians, and foreign governments acquiring the data to target Australians.

- **No digital identity laws.** Australians should be free to buy and sell and contract with each other, and free to move around and communicate with each other, without having to "show their papers" and without intrusive governments tracking their every move.
- **Abandon the census.** The census is outdated, unnecessary, and often collects data that the government already has.
- **Decommission MyHealthRecord, limit online services.** The government's controversial MyHealthRecord is both ineffective and unnecessarily grants the government access to Australians' medical data. Likewise, the increase of online services and integration of online services (e.g., myGov with Medicare, the ATO) creates a one-stop-shop for access to Australians' data.
- **Stop collecting unnecessary data.** Historically government-collected data has been used by foreign governments to target people. The government must stop collecting unnecessary data (e.g., religious affiliation, ethnicity).
- **Stop collecting unnecessary biometric data.** The government has begun collecting biometric data such as voice records. Such biometric data is unnecessary and could be used by the government to impersonate Australians.
- **Limit data sharing between and within governments.** Government data sharing between governments and within government departments enables the government to collect, correlate, and create a picture of Australians' entire lives. Governments and government departments must remain islands of disconnected information.

Government Reform

The government cannot protect its own networks and systems, yet spends time and money on the mass surveillance of Australians. Likewise, the government's main cyber security function is run by intelligence agencies, which is a clear conflict of interest.

- **Focus government on improving its own cyber security.** The government regularly fails its own cyber security audits. Improvement is required to avoid foreign governments compromising government systems. The effort the government spends spying on Australians is better spent protecting Australians.
- **Distance government from private organisations.** The metadata retention law has enabled more co-operation between private organisations and the government to spy on Australians. The government must distance itself from private organisations, and automated systems to request Australians' data from private organisations must be decommisioned.
- **Prevent intelligence agencies from interfering with, and providing services to, private organisations.** The ASD is lobbying to take over private companies' networks and IT systems to respond to cyber security attacks. Likewise, the ASD offers services to private organisations, sponsors private organisations, and runs the Australian Cyber Security Centre. Intelligence agencies must not be involved with private organisations.
- **Separate the government's cyber security and intelligence agencies.** The Australian Cyber Security Centre is part of the ASD. However, the ACSC employees intelligence officers & have an inherent conflict of interest. The ASD's focus is to spy on foreign entities, and hence security vulnerabilities will likely be horded to use against foreign entities instead of reported to Australians.
- **No government involvement in cyber security research / encryption research.** Historically, governments have suppressed private organisations' encryption research and attempted to back door encryption. The private sector must lead the way on security and privacy technology.

International Involvement

The government belongs to the Five Eyes spy network that was brought to the public's attention by Edward Snowden. Australia's government must take the lead by advocating the end of mass surveillance and government attacks on encryption. Likewise, the government must protect Australians form other countries' mass surveillance of Australians.

- **Free Julian Assange.** Julian Assange alerted the world to the dangerous power of the state in the age of the Internet. We will advocate for his immediate release and repatriation.

- **End government advocacy of mass surveillance.** The government must take the international lead in its advocacy of ending mass surveillance across the world.
- **End government involvement in international mass surveillance programmes.** End government involvement in mass surveillance programmes with other counties.
- **Advocate the end of governments' attacks on encryption.** The government's stance on encryption must be that citizens have the right to speak to each other without their government knowing.
- **Protect Australians from other governments' mass surveillance.** The government must do a better job not using datacentres and IT equipment manufactured by hostile nations. Likewise, the government must protect Australians against other countries' mass surveillance attempts of Australians.