



# STOPPING SURVEILLANCE OVERREACH WE ARE CITIZENS NOT SUSPECTS

*The Greens' plan to defend your privacy and rights online*

Our online privacy and rights are compromised by widespread warrantless surveillance. The Greens believe that the benefits of the internet can be available with personal privacy and civil rights intact but only if we balance freedom and security online, otherwise we risk losing both.

The Greens care about your privacy and rights online, campaigning with a broad coalition of organisations and the business community to successfully defeat the government's technically unfeasible and politically questionable mandatory internet filter.

As much as it is the Government's role to promote collective protection against identity theft, online crime and acts of political violence, Australian citizens have a legitimate expectation that the government will defend their democratic right to privacy, freedom of expression and freedom from arbitrary acts of state coercion.

This is especially the case when the blurring of terrorism with journalism, civil disobedience and healthy dissent has seen our security agencies and police forces deployed against climate change demonstrators, journalists, the occupy movement, anti-whaling campaigners and whistleblowers.

## > GET A WARRANT

Law enforcement and intelligence agencies need a warrant to enter our homes. They should also need one to access our telecommunications data. Because Australian law enforcement agencies were granted access to personal information about Australians 293,501 times throughout the 2011-12 year, without obtaining a warrant or having any judicial oversight, the Greens introduced the "Get a Warrant" bill into the parliament.

## > NO TO DATA RETENTION

The government proposed to retain data on all Australians for up to two years. Retaining all 'metadata' for all Australians, for years means that detailed locational data collected by phones, as well as information about every single social or business interaction online would be captured. This proposal was recently rejected by a parliamentary committee that received over 5,500 submissions, 98.9 per cent of which were opposed to the data retention proposal.

## > LIFE IN THE PRISM

While the old parties pretend nothing is happening, the world is in uproar about the US National Security Agency using the PRISM backdoor program to conduct warrantless surveillance through the servers of companies including Apple, Microsoft, Google and Facebook.

The Greens have demanded transparency about our government's complicity in the collection of private emails, audio and video chats, photographs, documents, connection logs and location data. The old parties wouldn't even support the Attorney General making a statement on the vulnerability of government information and Australians' legislated privacy protections.

In light of the PRISM scandal and the ongoing surveillance overreach, we need an overhaul of the information governments collect and share about us.

## > THE GREENS' PLAN

- **Include security agencies under the Telecommunications Interception and Access Act reporting requirements**
- **Require Mandatory Data Breach notifications by industry and government**
- **Require IT providers to inform customers of agreements to provide information to governments**
- **A Five Eyes agreement protecting privacy of citizens**
- **Bring security agencies within the ambit of the FOI Act**

Administrative costs for government to implement these policies will be absorbed by the relevant agencies, with a one off allocation of \$0.2 million for educational advertising.



## > INCLUDING SECURITY AGENCIES UNDER THE TIA ACT

Every year requests for telecommunications information and intercepts are increasing. The 2011-12 Telecommunications and Interception Access Act Annual Report showed that telecommunications data had been requested 240,000 times and the following year, 293,501 times.

ASIO and other intelligence and security agencies currently are not accountable through regular reporting under the Telecommunications Interception and Access Act. The Greens believe it is appropriate to include security agencies under the Telecommunications Interception and Access Act reporting requirements, similar to the reporting required from law enforcement agencies. Including them would improve accountability.

## > MANDATORY DATA BREACH NOTIFICATION

The Australian Greens believe that if a data breach occurs, the victim of that breach must be notified in order to minimise the harm caused and to restore the individual's control over their personal information.

The Greens support mandatory data breach legislation and propose to strengthen the *Privacy Amendments (Privacy Alerts) Bill 2013*, stating that mandatory data breach notifications would benefit both Australian consumers and industry stakeholders.

## > REQUIRE IT PROVIDERS TO INFORM CUSTOMERS OF THEIR AGREEMENTS WITH GOVERNMENTS

IT providers and carriage or carriage service providers including offshore companies operating in Australia should be required to advise customers of any agreements with foreign or domestic governments that may lead to or have led to the provision of either content or telecommunications data to government agencies.

These companies should be required to identify the agency, the date of the agreement, the relevant documentation and any follow-up documentation such as compliance reports, plus an annual report of how often information has been provided.

## > FIVE EYES AGREEMENT TO PROTECT THE PRIVACY OF CITIZENS

The governments USA, Canada, Australia, UK and NZ have an agreement to share information AUSCANNZUKUS, also known as Five Eyes.

The Greens believe that an agreement is needed among the five eyes cluster of countries sharing intelligence that any information held by the all partners on nationals of the other countries be stored only within the borders of that country and unless directly related to a national security operation or criminal trial, accessible only with the approval of the host government, with an annual report of how many requests for access have been made.

## > BRING SECURITY AGENCIES UNDER THE FREEDOM OF INFORMATION ACT

The 2011 reform of the FOI laws improved some aspects of the FOI framework in Australia but also opened major loopholes.

The Greens believe that ASIO, ASIS and others should be returned to the ambit of the FOI Act and the interpretation of national security as a ground for refusal FOI requests should be reviewed and narrowed.

The internet is the greatest information sharing tool and library in history. The democratisation of communications is leading to information sharing, scientific and technical innovation and the formation of a global civil society and that is extraordinarily valuable. The Greens believe that its potentials should be realised and will continue to resist it being transformed into an electronic panopticon surveillance tool.