Privacy and Security Services Policy

Vision

The Green Party envisions a National Security apparatus and Intelligence Community that provides a service that is in Aotearoa New Zealand's best interests and promotes democracy, non-violence, and justice.

Key Principles

1. Privacy and Security Services decision-making should align with the Key Principles of our Democracy and Constitutional Reform Policy, Defence and Peacekeeping Policy and Justice Policy.

Specific Policy Points

1. Security and Intelligence Agencies

There is significant concern with the activities of New Zealand's security and intelligence agencies (as established per the Security and Intelligence Act 2017) in terms of those agencies unreasonably interfering with a citizen's expression of personal opinion and freedom of association.

There is also significant concern with New Zealand's ongoing contribution of intelligence to mass-surveillance programmes and the militaries of other nations which contribute to human rights abuses.

A. Security Intelligence Service (SIS)

Before the SIS was established during the Cold War, its intelligence gathering functions were carried out by the police.

The Green Party believes that the SIS' history shows a disturbing pattern of spying on law-abiding political dissenters and people who hold different views on what is in the interests of Aotearoa New Zealand's 'international well-being or economic well-

being'. The SIS has done this in the name of protecting “national security”, New Zealand’s “international relations and well-being of New Zealand” – to quote from the objectives spelled out in the Intelligence and Security Act 2017. Such vague and undefined objectives, separated from any pursuit of criminality, have long been used to justify SIS surveillance on dissenters. The Green Party believes that what is good for New Zealand’s “international relations”, “national security”, or its “economic well-being” is politically contestable in a democracy, and shouldn’t be up to a secretive government agency to define.

Policy Positions

1.1. Tighten the definition of security in the relevant intelligence legislation to include only 'espionage, sabotage and terrorism'.

1.2. Instruct a Select Committee to review the security and intelligence agencies with a view to establish how existing and potential agencies could best contribute to Aotearoa New Zealand’s wellbeing and domestic and international law and order. As part of this review, the Select Committee would be asked to identify whether the functions of the security and intelligence agencies could be completed by other government agencies which have specific law and order functions, both nationally and internationally.

B. Government Communications Security Bureau (GCSB)

The GCSB is a signals intelligence organisation which spies on private electronic communications, including between New Zealanders and people in our neighbouring Pacific countries.

It is exempt from key provisions of the Privacy Act and the Crimes Act. The GCSB is linked with agencies in the United States, Britain, Canada and Australia: the Five Eyes network. The Green Party believes that it primarily operates in the interests of the United States and Britain, rather than for the benefit of Aotearoa New Zealand.

Policy Positions

1.3. Abolish the GCSB and establish an independent cybersecurity agency to adopt the useful cybersecurity function of the GCSB.

1.4. Withdraw Aotearoa New Zealand from the Five Eyes spying network

1.5. Close the satellite communications interception base at Waihopai and the signals intelligence base at Tangimoana.

C. Oversight and Scrutiny of Security and Intelligence Agencies

The Green Party believes that it is critical for democracy to be able to assure Aotearoa New Zealand's citizens, and those we wish to have international relationships with, that any action or expenditure on national security and intelligence matters can be scrutinised. The Green Party believes in Parliament's constitutional role in overseeing and examining all aspects of government agency activity and expenditure.

Parliament and its Select Committees is prevented from consideration or scrutiny of anything to do with intelligence and security agencies, including their operations and finances. Instead, these functions are held by a committee comprising the Prime Minister, the Leader of the Opposition and a small number of their nominees.

The position of Inspector-General of Intelligence and Security was created in 1996. The Inspector-General has limited powers to investigate the activities of intelligence and security agencies.

The Department of Prime Minister and Cabinet (DPMC) also contains security functions including in the National Assessments Bureau, Officials' Committee for Domestic and External Security Coordination, and Security and Intelligence Board.

Policy Positions

1.6. Replace the Intelligence and Security Committee with a true multi-party Select Committee, operating under parliamentary Select Committee rules, so that Parliament can scrutinise the intelligence and security activities of the Government. Such a Select Committee would not require approval from the SIS or GCSB Director to see "sensitive" information and, like all Select Committees, it would be able to scrutinise anything within its mandate, not excluding operations, all with an appropriate level of confidentiality.

1.7. Make the Inspector-General an officer of Parliament, with the recommendation for an appointment coming from the Officers of Parliament Committee, not from the Prime Minister, so they are truly an independent watchdog.

1.8. Repeal the Minister of Security and Intelligence's powers that limit the Inspector-General's ability to investigate and report on their own activities.

1.9. Extend the jurisdiction of the Inspector-General of Intelligence and Security to all agencies contributing to Aotearoa New Zealand's National Security

apparatus, including the New Zealand Defence Force and relevant parts of the Prime Minister and Cabinet, such as the National Assessments Bureau.

1.10. Review the functions of and need for the security agencies within the DPMC.

2. Freedom of Information

Access to official information is a cornerstone of an effective participatory democracy. The Green Party is committed to improving accessibility of public information.

Policy Positions

2.1. Reduce fees charged for public information and ensure that access to information has primacy over cost-recovery.

2.2. Ensure easy access to public information in cases involving public money or resource consents.

2.3. Ensure that all government information and advice is made available to the public archives after 25 years. The only documents exempt are those specifically restricted or withheld by the Chief Archivist on legitimate privacy grounds, not including political embarrassment for the government or departments.

3. Privacy and Surveillance

The Green Party is concerned that privacy is being undermined by intrusive personal surveillance activities such as the greater use of fingerprinting and biometrics for identification and tracking devices, the monitoring of electronic communications, expanded rights to search premises, and the greater use of computer databases to store and exchange personal information.

Digital services make the storage and correlation of personal data much more prevalent than it was in the past. The nature of the technology means that it is easy to gather and use information of all sorts, including accurate and inaccurate information. Once information is placed in a database it can last there indefinitely. This information should be collected, stored, and treated ethically, and access to this information by New Zealanders is paramount.

Policy Positions

3.1. Scrutinise closely any increase in state surveillance powers and information sharing between different state databases, and oppose any that are unwarranted.

3.2. Oppose the development of a universal identification card or system.

3.3. Adopt the New Zealand Privacy Charter.

3.4. Support a review of the Privacy Act 1993 and the Official Information Act 1982, to improve the public's access to information and ensure that there are effective review mechanisms in place for those who do not receive the requested information or the protection of their privacy.

3.5. Ensure judicial oversight, with full transparency, of government actions involving the surveillance of individuals, and also the designation of people as a threat to security.

3.6. Support amending the New Zealand Bill of Rights Act 1990 to specifically include a right to privacy.

3.7. Review controls on the sale of private information, the aggregation of information by private agencies, and the exchange of information between government agencies, to ensure consistency with the aims of the Privacy Act.

3.8. Regulate the use of tracking devices on products so that they don't intrude on people's privacy.

3.9. Promote and publicise the right of people to see the personal information held on them in state and other databases and to correct such information.

3.10. Ensure all government databases and, wherever possible, all other databases are kept in a New Zealand jurisdiction, not on an overseas site and that Aotearoa New Zealand privacy laws still apply where databases are kept on an overseas site.

3.11. Ensure that all data held by the state is stored on servers in Aotearoa New Zealand.

3.12. Ensure that data on alleged criminal behaviour is not accepted from a foreign agency unless its collection does not violate the Bill of Rights Act 1990 and other international rights agreements.

3.13. Ensure that any state agency, when sharing data with an overseas agency, has adequate guarantees as to the subsequent use of that information, and hold agency heads accountable, professionally and personally, for misuse of that information.

3.14. Support measures restricting the use of "profiling", the ranking of individuals for use in determining eligibility for health care, insurance, financial services, etc., because of the potential for this to raise issues of a lack of transparency, lack of accountability and discriminatory outcomes."

3.15. Make it illegal for people to be discriminated against on the basis of information they do not have access to, including information held in a confidential overseas database.

3.16. Review the Search and Surveillance Act, with the aim making it more difficult for enforcement agencies to search without a Court-ordered warrant.

3.17. Amend the Search and Surveillance Act to remove the right of the state to conduct video surveillance on private property without the permission of the property owner or lessee without clear police warranting authority, regular review of the authority, and public reports on use of video warrants.

3.18. Monitor and regulate the use of CCTV cameras and drone video cameras by public and private bodies and ensure that the information gathered from them is gathered and used legitimately and not counter to the public interest.

3.19. Ensure that data gathered from electronic payment systems is gathered and used legitimately and not counter to the public interest.

3.20. Support legislation and regulations restricting the use of biometric information (fingerprints, iris or face recognition, etc.), and any data bases of biometric information, by both private and public organisation.

3.21. Pass legislation to restrict the use of drones unless they have prior authorisation from the owner or lessee of the land they are flying over, or they are flying over public areas authorised by local or national authorities or otherwise have lawful excuse. Any such restrictions should be motivated both by the need to protect people's privacy, and the need to limit the annoyance and noise pollution caused by drones.

3.22. Uphold the principle that citizens cannot be legally required to answer questions or to self-incriminate, and flowing from that that they not be required to provide their passwords for electronic devices or computer systems.

3.23. Restrict the ability of border and law enforcement agencies to access computer devices, including smart phones. That there be a legal requirement that such access is granted only for serious crimes, and either on the production of a search warrant either before the search or, in exceptional circumstances, after the search. The search warrant should be specific as to what information can be searched for, for what purposes the information can be used, in recognition of the huge amount of personal information commonly stored on computer devices and smart phones.

3.24. Oppose any legal requirement on operators of computer system to weaken the security of their computers to enable state agencies to have a back-door entry.

3.25. Help ensure the security of computer systems, and the privacy of their users, by separating the state agencies having prime responsibility to protect computer system from those engaged in the surveillance of computer systems. Consequently, a new state cybersecurity agency should be established separate from what is presently the state's main cyber-surveillance agency, the Government Communications Security Bureau.

3.26. Oppose the hacking of computer systems by government agencies without the knowledge of the owner or operator except for law enforcement purposes, with clear police warranting authority, regular review of the authority, and public reports on use of these warrants.

3.27. Publicly call out corporations interfering in the privacy rights of New Zealanders, and impose punitive penalties against them.