

Review of the Search and Surveillance Act 2012 – Questions and Answers

The Act

Q. What does the Search and Surveillance Act do?

A. The Act outlines rules for how New Zealand Police and some other government agencies (like the Department of Internal Affairs and Inland Revenue) conduct searches and surveillance when investigating and prosecuting offences and when monitoring compliance with the law.

The Act does not apply to New Zealand's intelligence agencies (the Government Communications Security Bureau and the New Zealand Security Intelligence Service). Their search and surveillance powers are contained in the Intelligence and Security Act 2017.

Q. What is a search?

A. The Search and Surveillance Act does not define what a search is, but the courts have said that a search is a State intrusion on a person's "reasonable expectation of privacy". The most obvious example is the Police looking for evidence inside a person's home.

Q. What is surveillance?

A. Again, the Act does not define surveillance. Instead it provides rules for using interception, tracking and visual surveillance devices. Such devices can be used to monitor, observe and / or record activities of individuals.

Findings and recommendations in the report

Q. What is wrong with the current law?

A. Generally the Act is working well. However, the review identified two main problems. First, key aspects of search and surveillance law are contained in case law and are not evident on the face of the Act. Second, the Act has not kept pace with developments in technology.

Q. What do the Law Commission and the Ministry of Justice recommend?

A. The Report contains 67 recommendations, including recommendations concerning the underlying principles of the Act, the use of surveillance technology, searching electronic devices and Internet sites and conducting undercover operations. Many of the recommendations are designed to clarify the existing law rather than significantly change it.

Q. Will the recommendations expand police powers?

A. The review recommends that in some areas police powers should be expanded and that in other areas new restrictions should be put in place.

The recommendations that would expand police powers mainly relate to surveillance. The review recommends that:

- surveillance warrants should not just enable the use of devices, but should also be available in relation to other surveillance technology, including computer programs;

- data surveillance warrants should be available to enable police officers to undertake activities such as monitoring a person's web browser history or logging their keyboard strokes; and
- police officers should be able to conduct warrantless surveillance for a limited period of time in urgent situations.

Some of the new restrictions recommended in the report include:

- enforcement agencies should be required to publish policy statements explaining how and in what situations they use certain lawful investigatory techniques, such as undercover operations, CCTV use and social media monitoring;
- searches of electronic devices should only be permitted if a warrant has been obtained, except in urgent situations;
- warrants should be obtained before conducting some undercover operations and they should be subject to external auditing.

Q. Will the recommendations protect people's privacy?

A. Protecting privacy and enabling effective law enforcement were two of the main objectives for the review. Several recommendations promote greater transparency and therefore accountability around law enforcement practices. This includes recommendations for a new principles section, publicly available guidelines about certain activities and more extensive requirements for notifying people who are affected by searches.

Where the report recommends new powers, it also proposes safeguards to ensure privacy intrusions are minimised (such as requiring judicial authorisation for new surveillance techniques).

Q. Will the recommendations make it harder for police officers to do their jobs?

A. The report does recommend some new restrictions to ensure police exercise their powers in a manner that respects the privacy and human rights of individuals. The Law Commission and Ministry of Justice worked closely with Police and other enforcement agencies in developing these recommendations, and do not think they will prevent enforcement officers from doing their jobs effectively. In other areas the report recommends new powers for enforcement officers, to address difficulties they have encountered under the current law.

Q. What is happening with surveillance?

A. The review makes a number of recommendations that relate to surveillance. In order to update the Act to take account of new technology, the Report recommends that surveillance warrants should not just enable the use of devices, but should also be available for other surveillance technology (for example, computer programs) that can access the same information. The Report also recommends the Act should enable data surveillance. This could allow enforcement officers to obtain warrants to undertake activities such as monitoring a person's web browser history and logging their keyboard strokes. Other recommendations would allow enforcement officers to carry out warrantless surveillance in certain urgent situations where there is a compelling need to do so.

Q. What does the Report say about enforcement agencies searching:

a. Electronic devices, like my smartphone?

A. The review explains that electronic devices, like smartphones, have become increasingly prevalent and sophisticated since the Act was passed. The owners of such devices have a high privacy interest in their contents. To recognise this, the Report recommends that search warrants should be obtained before an enforcement officer searches the contents of such a device, unless it is an urgent situation.

b. Internet sites, like Facebook?

A. The Report highlights some difficulties with the provisions in the Act that govern searches of Internet sites, such as Facebook. There is currently some uncertainty in international law about whether enforcement officers are able to search information on an Internet site that is stored on a server in another jurisdiction. The provisions in the Act are also difficult to understand. The Report recommends that the government should consider acceding to a leading international agreement, the Budapest Convention, so that New Zealand can take part in finding a possible international solution to the problems associated with Internet searches. The Report also makes recommendations to improve the Act's provisions, to clarify their effect.

c. Customer records held by companies?

A. The report explains that there is uncertainty about how enforcement officers should obtain customer records from companies. The Act introduced a mechanism for obtaining these types of documents by compulsion – production orders – but it does not specify when enforcement officers should use production orders. The alternative is that enforcement officers can ask the companies to provide the information voluntarily. In order to promote consistency and to give greater guidance to enforcement officers and the general public, the Report recommends that there should be publicly available guidance on when enforcement officers should use a production order to obtain customer records from companies.

Q. What does the report recommend about undercover operations?

A. The report recommends that the Act should require agencies to publish policy statements on when and how they use undercover techniques, and to obtain warrants in certain circumstances. Undercover activity would also be subject to external auditing.

Q. Why does the Report recommend regulation of undercover operations?

A. The Act does not specifically regulate undercover operations. The review concludes that this is undesirable. Undercover operations have the potential to intrude on people's reasonable expectations of privacy and to involve undercover officers in conduct that would be unlawful if carried out by a member of the public. The Report concludes that we need more transparency and accountability to ensure that intrusive State activity accords with the rule of law, and to encourage public confidence in the integrity of the criminal justice system.

Q. Why does the Report distinguish between regulatory and law enforcement powers?

A. The Act applies to powers exercised for law enforcement purposes, as well as to some powers exercised for regulatory compliance purposes (for example, inspections by fisheries officers). Regulatory powers are often wider than law enforcement powers because people who choose to operate in a regulated industry are more likely to expect that their activities might be monitored. The review found that the rules in the Act, which were designed largely with law enforcement powers in mind, do not always fit well with regulatory powers. The report suggests that further work be done considering the extent to which regulatory powers should be covered by the Act.

The review process

Q. Why was the review carried out?

A. When Parliament passed the Search and Surveillance Act in 2012, it decided that the Law Commission and the Ministry of Justice should conduct a joint review of the Act between June 2016 and June 2017. The Act requires the review to look at how the provisions in the Act have operated in practice.

Q. Why did it take several months for the report to be released?

A. The Law Commission and the Ministry of Justice provided the report to the former Minister of Justice at the end of June 2017, as the Act required. However, it was not tabled in the House of Representatives before the election. Following the election, the new Minister of Justice needed time to consider the report before tabling it.

Q. What consultation did the Law Commission and Ministry of Justice undertake?

A. The Law Commission and the Ministry of Justice released an Issues Paper in November 2016 and received submissions from government agencies, interest groups and members of the public. The Commission and Ministry also engaged with a range of stakeholders throughout the review process. This included setting up and consulting with:

- an Expert Advisory Group, with members selected for their expertise in privacy law, human rights, criminal law, technology and digital security; and
- an Officials' Group, with representatives from many of the key law enforcement and regulatory agencies that exercise powers under the Act.

What happens next?

Q. Will there be future reviews?

A. The Act only required one review. However, as with all legislation it administers, the Ministry of Justice will continue to monitor the Act's effectiveness, including in light of any legislative changes resulting from this review. Some of the recommendations in the report also suggest further work be undertaken by the Ministry of Justice in certain areas, such as how the Act applies to regulatory agencies.

Q. What is the process for the Government to respond to the Report?

A. The Government will consider the recommendations in the report and decide whether to accept some or all of them. If it accepts the recommendations, it will need to introduce a Bill to Parliament to amend the Act.

Q. What is the timeframe for the Government's response? When will a Bill be introduced?

A. There is no statutory timeframe within which the Government must respond to this report. Because the review was a joint one between the Law Commission and the Ministry of Justice, the process for the Government response may differ from other Law Commission reports.