BUDDLEFINDLAY

Ministry of Justice and Law Commission report finds Search and Surveillance Act "has not kept pace with developments in technology"

Scott Barker, Seb Bisley, Willie Palmer, Susan Rowe, David Broadmore, Kelly Paterson, Peter Niven, Anita Birkinshaw, Bridie McKinnon, Oliver Gascoigne, Olly Peers

2 February 2018

The Search and Surveillance Act 2012 (Search and Surveillance Act) has not kept pace with developments in technology, according to a report published on Tuesday by the Ministry of Justice and Law Commission. The report also raises concerns that key aspects of case law, such as the protection of individuals from "unreasonable search and seizure", are not reflected in the Search and Surveillance Act.

The purpose of the Search and Surveillance Act is to "facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values". This purpose reflects the two sets of values that arise in the context of regulating search and surveillance powers: human rights values and law enforcement values.

The report contends that the Search and Surveillance Act has compromised both of these values in two important ways:

- Key aspects of search and surveillance law are contained in case law and are not evident on the face of the Search and Surveillance Act
- The Search and Surveillance Act has not kept pace with developments in technology.

While none of the report's recommendations propose a major overhaul, the report concludes that the Search and Surveillance Act requires amendment to reflect international trends in search and surveillance law.

The main recommendations include:

- Enacting a principles provision, based on relevant case law that is not evident on the face of the Search and Surveillance Act. This reflects the view that too much of the law in this area is contained in the jurisprudence surrounding section 21 of the NZBORA protecting individuals from "unreasonable search and seizure"
- Recommending that Chief Executives of enforcement agencies should be required to issue publicly available policy statements about certain investigative activities. When an investigative activity is lawful, there may still be doubt as to its reasonableness. These policy statements should promote certainty, transparency, and accountability
- Amending references of surveillance devices to "surveillance technology". This will ensure that warrants are both required and available under the surveillance device regime to carry out surveillance using intangible technologies (such as computer programmes) as well as devices, which carry an ordinary meaning of a tangible thing. This reflects advancements in technology and extends the availability of warrants to surveillance not previously covered by the regime
- Extending the surveillance warrant regime to enable data surveillance. Data surveillance includes logging a computer's keystrokes on a keyboard and monitoring web browsing history
- Assisting enforcement officers in obtaining password and encryption keys that are necessary to gain access to electronic devices by:
  - utilising keystroke logging technology
  - recommending the privilege against self-incrimination be limited to prevent an individual refusing a request to provide access information for a device
  - increasing the penalty for individuals refusing an enforcement agency access to their devices.

This report reflects international concern about the appropriate balance between intrusive surveillance powers, and corporate and personal privacy. Most recently, the Court of Appeal for England and Wales handed down a decision on 30 January 2018 in *Secretary of State for the Home Department v Watson MP* [2018] EWCA Civ 70 in which the Court ruled that the United Kingdom's Data Retention and Investigatory Powers Act 2014 (DRIPA) was inconsistent with EU law. That was because the DRIPA permitted the Government access to retained data for reasons not restricted solely to fighting

serious crime. While the DRIPA has since been replaced by the Investigatory Powers Act 2016, the Court's decision is expected to remain relevant to the powers under the new Act.

Similarly, legislative authorities both here and in the United States, have sought to expand and clarify the scope of surveillance powers. New Zealand did so by the enactment of the Intelligence and Security Act 2017. The United States, another Five Eyes Intelligence network member, did so by re-authorising the Foreign Intelligence Surveillance Act 1978 in January 2018 for a further six years.

These sorts of powers are contentious given the allegations made against MI5, MI6 and the GCHQ based on the release of internal documents. Those are agencies of the United Kingdom, which is also a Five Eyes Intelligence network member. The internal documents reveal that intelligence services in the United Kingdom have intercepted legally privileged communications between lawyers and their clients in sensitive security cases.

While these issues do not relate directly to the Search and Surveillance Act, they nonetheless inform the increasingly international and multi-jurisdictional context in which amendments to the Search and Surveillance Act ought to be considered.

As to the report, developments in technology appear to have heightened the public's interest in the privacy of their information and have created new challenges for effective law enforcement. Overall, the report's view is that the Search and Surveillance Act is generally working well, but some parts would benefit from clarification.

See the full report here.

Auckland

PwC Tower
188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659