SE16/2 **CROSS SCHEME**

ADDITIONAL ESTIMATES BRIEFING – FEBRUARY 2016

ACCESS TO TELECOMMUNICATIONS DATA BY THE CLEAN ENERGY REGULATOR

ISSUE

As of 13 October 2015, as a result of the implementations of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, the Clean Energy Regulator is no longer a designated 'enforcement agency' and does not have access to telecommunications data under the provisions of the *Telecommunications (Interception and Access) Act 1979 (*TIA Act).

HEADLINE STATEMENT

- The Clean Energy Regulator is no longer able to utilise the provisions of the TIA Act to access telecommunications data.
- The Clean Energy Regulator considers access to telecommunications data to be a valuable investigative tool.
- Recognising the importance of people's privacy, the Clean Energy Regulator utilises access to telecommunications data as a tool of last resort. The Clean Energy Regulator had implemented strict controls on the request for, and use of, telecommunications data.
- This has resulted in the Clean Energy Regulator only authorising access on four occasions relating to three investigations.
- While the rate of usage of telecommunications data in Clean Energy Regulator investigations is low, the loss of this tool is likely to result in some investigations not progressing to the extent that may have been possible.
- The Clean Energy Regulator is exploring other options, including the use of our existing coercive notice powers, to obtain access to telecommunications data.

TALKING POINTS

- The Chair and Chief Executive Officer of the Clean Energy Regulator wrote to the Attorney-General's Department on 12 June 2015, seeking continued access to telecommunications data. Preliminary advice is that the Attorney-General is not minded to expand the revised list of 'enforcement agencies'.
- The Clean Energy Regulator is responsible for administering climate change laws that contain offences with significant criminal and civil penalties. Circumstances giving rise to breaches of climate change laws often also provide evidence of offences under the *Criminal Code Act 1995*.
- Information obtained as a result of access to telecommunications data was not available through other means and enabled the Clean Energy Regulator to progress the relevant investigations.

- While the rate of usage of telecommunications data in Clean Energy Regulator investigations is low, the loss of this tool is likely to result in some investigations not progressing to the extent that may have been possible.
- The Clean Energy Regulator is exploring other options for gaining access to telecommunications data. These options include requesting the assistance of a defined 'enforcement agency' or utilising the provisions of our existing coercive notice powers.
- However access is obtained, the Clean Energy Regulator will maintain the strict controls it has implemented on the request for, and use of, telecommunications data.

BACKGROUND

- As part of its administration of climate change laws, the Clean Energy Regulator actively pursues those who opportunistically or deliberately contravene these laws.
- The Clean Energy Regulator has a team of qualified and experienced investigators who investigate alleged breaches of the legislation we administer.
- The Clean Energy Regulator, previously as an enforcement agency under the TIA Act, could authorise the disclosure of telecommunication when reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of public revenue.
- While recognising the usefulness of telecommunications data as an enforcement tool, the Clean Energy Regulator appreciates the potential sensitivity of this information source and the legislative provisions in place to maintain integrity. In order to meet its legislative obligations, the Clean Energy Regulator limited access to telecommunications data and established robust mechanisms for requesting, accessing and using this data.
- Authorisation for the disclosure of telecommunication information was made on each occasion by Senior Executive members of the Clean Energy Regulator.
- The authorised officer must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use of telecommunications data under request is justifiable, having regard to:
  - the likely relevance and usefulness of the information or documents, and
  - the reason why the disclosure or use concerned is proposed to be authorised.
- There have been four authorisations for the disclosure of telecommunication information by the Clean Energy Regulator relating to three investigations.
- These authorisations have been limited to the disclosure of telecommunications data on the person of interest subject to an investigation, and only to verify information provided by that person to allegedly claim benefits administered by the Clean Energy Regulator to which they were not entitled.
  - In the first case, a subscriber check demonstrated that the phone number used in support of a claim made to the Clean Energy Regulator was invalid (that is, the phone number did not exist). This matter was subsequently referred to a state law enforcement agency.

  - In the second case, a subscriber check supported the allegation that an unknown person had fraudulently used the details of a known company in an attempt to create certificates. The certificates were failed.
  - The third case is ongoing and relates to an allegation of an installer providing false information (signing off on installations he had not attended). In this case the information supported the allegation that the person of interest had not attended the installation address.

- In accordance with s186 of the TIA Act, the Clean Energy Regulator reported annually to the Attorney-General's Department regarding access to telecommunications data for inclusion in its annual report to Parliament.
- The penalties contained in the climate change laws administered by the Clean Energy Regulator include significant terms of imprisonment (e.g. a breach of s 66L of the ANREU Act – 10 years).
- Additionally, for many of the matters investigated, offences under the Commonwealth and state and territory criminal codes also apply.
- Penalties applied by the courts for matters investigated by the Clean Energy Regulator include:
  - Civil penalties exceeding $200,000 applied to parties involved in a breach of the *Renewable Energy (Electricity) Act 2000* – MT Solar and others.
  - 20 months imprisonment with a nine month non-parole period to be served by way of home detention for breaches of the *Criminal Code Act 1995* arising from offences relating to the Renewable Energy Target – Mr John Testoni.
  - Two years imprisonment (served by way of intensive corrections order) for a breach of the NSW criminal code – this matter arose from an investigation into the improper creation of certificates and was referred to the NSW Police who prosecuted the matter – Ms Lucie Yeung.
  - Mr Neville Voss is currently before the Queensland courts charged with breaches of the *Criminal Code Act 1995* resulting from the improper creation of certificates. Mr Voss has entered a guilty plea and this matter has been adjourned to the Queensland District Court for sentencing on a date to be fixed in 2016.

ATTACHMENTS

Attachment A	Letter from the Attorney-General's Department
Attachment B	Response by the Chair and CEO of the Clean Energy Regulator
Attachment C	Media Article – The Guardian – 18 January 2016

Dozens of agencies want warrantless access to Australians' metadata again

More than 60 departments, councils and other agencies at all levels of government want their access to stored personal data back

Paul Farrell

Monday 18 January 2016 14.47 AEDT

More than 60 government agencies are seeking to regain warrantless access to Australians' phone and web metadata, in what appears to be a major pushback after the federal government restricted the number of agencies that could access it.

In 2015, the federal government succeeded in passing controversial news laws that vastly increased the amount of Australians' personal phone and web data required to be held by telecommunications companies.

As part of its review of the legislation, the government narrowed the definition of an "enforcement agency" that was eligible to access telecommunications data to a shortlist of law enforcement agencies, including the Australian federal police and state and territory police forces.

But it left open the potential for the list to be expanded if the attorney general, George Brandis, introduced a regulation to approve an agency's access, as part of the

changes agreed to following the parliamentary joint committee on intelligence and security inquiry into the legislation.

On Monday Zdnet published the full list of agencies that are seeking access to stored metadata, in response to a freedom of information request it sent to the Attorney General's Department.

It appears to contain agencies that have previously sought access under the scheme, which sees hundreds of thousands of requests each year by government agencies to telecommunications companies for access to personal data.

Local councils, state-based wildlife organisations and environment and consumer protection bodies are all seeking to regain their access.

In a bizarre decision, the names of four agencies seeking access have been withheld by the Attorney General's Department on the grounds that releasing them would damage commonwealth/state relations.

"During consultation, these four agencies clearly indicated that disclosure of this information would damage the relationship between the department and the relevant agencies, and could affect any future cooperation with the department," the department told Zdnet.

The process for approving acccess to telecommunications data is complex. Regulations must be introduced first by the attorney general stating the agency that is seeking access.

The matter must then be referred to the parliamentary joint committee on intelligence and security for approval, and to determine whether any conditions should be imposed on the agency's access. The privacy commissioner and commonwealth ombudsman can also be consulted.

For commonwealth agencies, it may be possible to bypass this process if amendments to their enabling legislation are introduced separately that prescribe access.

This method was taken to allow the Australian Border Force to gain access to telecommunications data without needing to gain approval from the Attorney General's Department or the intelligence committee.

The full list of agencies published by Zdnet

1 Australian Financial Security Authority
2 Australian Health Practitioner Regulation Agency
3 Australian Postal Corporation
4 Australian Taxation Office
5 Australian Transaction Reports and Analysis Centre
6 Civil Aviation Safety Authority
7 Clean Energy Regulator
8 Department of Agriculture
9 Department of Defence
10 Department of the Environment

11 Department of Foreign Affairs and Trade
12 Department of Health
13 Department of Human Services
14 Department of Social Services
15 Fair Work Building and Construction
16 National Measurement Institute
17 ACT Revenue Office
18 Access Canberra (Department of Treasury and Economic Development)
19 Bankstown City Council
20 Consumer Affairs - Victoria
21 Consumer, Building and Occupational Services - Tasmania
22 Consumer and Business Services - SA
23 [redacted]
24 [redacted]
25 Department of Agriculture, Fisheries and Forestry - Queensland
26 Department of Commerce - WA
27 Department of Corrective Services - WA
28 Department of Environment and Heritage Protection - Queensland
29 Department of Economic Development, Jobs, Transport and Resources - Victoria
30 Department of Environment, Land, Water and Planning - Victoria
31 Department of Environment Regulation - WA
32 Department of Fisheries - WA
33 Department of Justice and Regulation (Consumer Affairs) - Victoria
34 Department of Justice and Regulation (Sheriff of Victoria)
35 Department of Mines and Petroleum - WA
36 [redacted]
37 Department of Primary Industries (Fisheries) - NSW
38 Environment Protection Authority - SA
39 Greyhound Racing Victoria
40 Harness Racing New South Wales
41 Health Care Complaints Commission - NSW
42 Legal Services Board - Victoria
43 NSW Environment Protection Authority
44 NSW Fair Trading
45 Office of Environment and Heritage - NSW
46 Office of Fair Trading - Queensland
47 Office of State Revenue - NSW
48 Office of State Revenue - Queensland
49 Office of the Racing Integrity Commissioner - Vic
50 Primary Industries and Regions South Australia
51 Queensland Building and Construction Commission
52 Racing and Wagering Western Australia
53 Racing NSW
54 Racing Queensland
55 Roads and Maritime Service NSW
56 Royal Society for the Prevention of Cruelty to Animals (RSPCA) - Victoria
57 State Revenue Office - Victoria
58 Taxi Services Commission - Victoria

59 [redacted]
60 Revenue SA
61 Victorian WorkSafe Authority

Topics

Privacy

Data protection / Mobile phones / Internet / Telecoms / Australian politics / news