Questions on Notice for each of the ACIC, AFP, NSW Police and QLD Police

1. Since 13 April 2015, have you ever requested, or conducted, an audit of how the powers under sections 178, 178A, 179 and 180 are being exercised by your agency?

The ACIC has undertaken internal audits through its Compliance, Audit and Business Advisory team in June 2015 and a follow up review in 2020 by its Covert Operations Assurance (COA) team.

As part of its business as usual activities, the COA team regularly conducts internal quality assurance audits.

If not, why not? If so:

a. Who conducted the audit(s)?

The ACIC CEO and the agency's internal Organisational Health Committee requested the 2015 audit, which was conducted by the Compliance, Audit and Business Advisory team.

b. What was the outcome of the audit(s)?

The 2015 internal audit made a number of observations and recommendations, including to apply the existing Excellence in Compliance (EIC) Strategy to telecommunication data authorisations, and create additional positions to function as Subject Matter Experts and National Coordination.

c. Did the audit(s) find any problems with how the powers were being exercised?

The internal audit identified issues in relation to the workflow process that resulted in inconsistencies in how the powers were being exercised, due to the decentralised approach of the ACIC's use of authorisations. The audit also identified the ACIC required greater internal governance and oversight to ensure the agency's use of the powers were done so in accordance with legislation and ACIC internal policy and procedures.

d. Did the audit(s) make any recommendations? What were they? Were they implemented?

A number of recommendations were made, specifically that there be more internal governance and oversight around the use of the authorisations. Three positions were created, including an EIC Coordinator, a Telecommunications Data Coordinator and a National Operational Support Officer Coordinator. The EIC Strategy and training programme was also applied to telecommunication data authorisations.

Web browsing information

2. How many times has a carrier provided a person's web browsing history to your agency in response to an authorisation you made in respect of historic telecommunications data?
- **a. What have you done when this has happened? Have you deleted that data on each occasion?**
- **b. Have you ever used that data as part of an investigation? If so, please provide details.**
- **c. Have you ever used that data as evidence in a prosecution? If so, please provide details.**
- **d. Have you ever used that data or referred to it at all? If so, please provide details.**

The ACIC has no record of a carrier providing a person's web browsing history to the ACIC in response to an authorisation made in respect of historic telecommunications data.

3. How many times has a carrier provided a person's web browsing history to your agency in response to an authorisation you made in respect of prospective telecommunications data?
- **a. What have you done when this has happened? Have you deleted that data on each occasion?**
- **b. Have you ever used that data as part of an investigation? If so, please provide details.**
- **c. Have you ever used that data as evidence in a prosecution? If so, please provide details.**
- **d. Have you ever used that data or referred to it at all? If so, please provide details.**

The ACIC has no record of a carrier providing a person's web browsing history to the ACIC in response to an authorisation made in respect of prospective telecommunications data.

Number of authorised officers

4. As at 1 March 2020, how many police officers were employed by your agency?
- **a. Please provide a breakdown of those officers by ranking (e.g. of the [x] total police officers in the agency, [#] are Senior Constables, [#] are Constables etc).**

The ACIC does not designate certain roles within the agency as 'police officers', and employs staff in a range of operational and intelligence roles.

5. In total, and as at 1 March 2020, how many of your officers are "authorised officers" (i.e. have the powers to authorise the release of telecommunications data)?

a. Please provide a breakdown of those officers by ranking (e.g. of the [x] authorised officers in the agency, [#] are Senior Constables, [#] are Constables etc).

The ACIC CEO has delegated the power and functions of an authorised officer to 37 positions within the agency:

- Executive Director Intelligence Operations
- Executive Director Capability
- National Manager Operational Strategy
- National Manager Strategic Intelligence Capability
- National Manager Technical Intelligence Capability
- National Manager Human Intelligence Capability
- State Managers for New South Wales, Victoria, Queensland, Western Australia, South Australia, Tasmania and Northern Territory
- Heads of Investigations and Intelligence Operations
- Regional Intelligence Managers
- Investigations Managers for Sydney, Melbourne, Brisbane, Perth and Adelaide
- Manager Transnational Serious and Organised Crime Unit
- Manager Monitoring and Assessment Unit
- Manager Special Operations for New South Wales and Queensland
- National Registrar Covert Operations
- Manager Cybercrime Intelligence
- Manager Australian Priority Organisation Target (APOT) Disruption Unit
- Manager Australian Gangs Intelligence Coordination Centre
- Manager Financial Crime Fusion Centre
- Manager Covert Technical Capability
- Manager Covert Technical Operations
- Team Leader Joint Analyst Group - Victoria
- Team Leader Joint Analyst Group - New South Wales
- Team Leader Joint Analyst Group - Queensland
- Team Leader Joint Analyst Group - South Australia
- Team Leader APOT Disruption Unit

Training of authorised officers

6. Prior to 1 March 2020, was specific training provided to officers prior to them becoming authorised officers? If not, why not?

All of the ACIC's authorised officers are provided with an in-depth delegate briefing which explains the legal, compliance and technical considerations required to fulfil their role and authorise

instruments. In addition to the delegate briefing, relevant ACIC staff, including authorised officers, must complete EIC training and pass an assessment prior to any use or access of the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*.

7. If such training was provided:

a. Was it compulsory?

Yes.

b. What is the name of that training program?

EIC training program.

c. How long is the training program?

The EIC training program forms part of a whole-of-agency strategy, which includes an eLearning module that is required to be completed every 12 months. The eLearning module takes approximately 60 minutes to complete and includes an assessment. In addition to this module, the ACIC aims to conduct 12 monthly face-to-face review sessions with each region.

d. What is the content of that training program?

The EIC training program incorporates the legal, policy, procedure and compliance requirements of the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*.

e. Who provides that training?

The ACIC's COA team, overseen by the Learning and Development area.

f. Who conducts that training?

As above.

g. Do officers have to complete a test or some other form of examination in order to become an authorised officer?

Yes. The EIC training program includes two assessments – one general and one for warrant and authorised officers.

h. If so, do officers have to pass that test or other form of examination in order to become an authorised officer?

Yes. Authorised officers within the ACIC also undergo a delegate briefing which explains the legal, compliance and technical considerations required to fulfil their role and authorise instruments.

i. Is completion of that program a pre-requisite to becoming an authorised officer?

Yes.

j. Please provide the Committee with a copy of the training manual(s).

A copy of the relevant eLearning modules is attached to these responses.

8. Prior to 1 March 2020, were regular training programs delivered to authorised officers to ensure that decisions were being made appropriately and consistently? If not, why not?

The ACIC has adopted a 'no training, no access' policy since 2008, including in relation to decisions pertaining to information under the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*. This policy was more broadly applied to telecommunications data in 2015.

9. If such training was provided:

a. Was each of those programs compulsory?
b. How many training programs?
c. What is the name of each of those training programs?
d. How often were those training programs delivered?
e. What is the content of each training program?
f. Who provided each of those training programs?
g. Who conducted each of those training programs?
h. Was completion of regular training programs a pre-requisite to retain one's status as an authorised officer?
i. Please provide the Committee with a copy of the training manual(s).

Please refer to response to question 7 above.

10. Has an authorised officer ever been disciplined for inappropriately making an authorisation for access to historic telecommunications data? If so:

a. When?
b. How many times?
c. In each case, what was the rank of the officer(s)?
d. In each case, what action was taken by the agency?
e. In each case, why was the conduct of the officer considered inappropriate?
f. In each case, did the officer retain his or her status as an "authorised officer"?

No incidents have occurred that warranted disciplinary action with regards to inappropriate authorisations for access to historic telecommunications data.

11. Has an authorised officer ever been disciplined for inappropriately making an authorisation for access to prospective telecommunications data? If so:

- **a. When?**
- **b. How many times?**
- **c. In each case, what was the rank of the officer(s)?**
- **d. In each case, what action was taken by the agency?**
- **e. In each case, why was the conduct of the officer considered inappropriate?**
- **f. In each case, did the officer retain his or her status as an "authorised officer"?**

No incidents have occurred that warranted disciplinary action with regards to inappropriate authorisations for access to prospective telecommunications data.

12. As at 1 March 2020, other than where an officer has left the agency, has an authorised officer ever had his or her status as an authorised officer removed? If so:

- **a. How many times has this happened?**
- **b. In respect of each example, why did the officer have his or her status removed?**

No.

Use of powers – authorisations for historic telecommunications data

13. How many authorisations for historic telecommunications data did your agency make in 2018/19?

The ACIC made 6,536 (existing information) authorisations in 2018-19, of which 1,026 were for information older than 3 months (considered 'historic' by the ACIC).

14. As at 1 March 2020, how many authorisations for historic telecommunications data has your agency made in 2019/20? If precise numbers cannot be provided, please provide an estimate with an explanation of how you arrived at the estimate.

As at 1 March 2020, the ACIC had made 3,679 (existing information) authorisations in 2019-20, of which 244 were for information older than 3 months (considered 'historic' by the ACIC).

15. How many individuals did the authorisations for historic telecommunications data made by your agency in 2018/19 relate to? If precise numbers cannot be provided, please provide an estimate with an explanation of how you arrived at the estimate.

The ACIC systems used in relation to telecommunications data authorisations do not capture this information in a way that can be readily extracted, without undertaking a manual review of the details relating to each authorisation.

16. As at 1 March 2020, how many individuals have the authorisations for historic telecommunications data in 2019/20 related to? If precise numbers cannot be provided, please provide an estimate with an explanation of how you arrived at the estimate.

The ACIC systems used in relation to telecommunications data authorisations do not capture this information in a way that can be readily extracted, without undertaking a manual review of the details relating to each authorisation.

17. Please provide a breakdown of the offence provisions that authorisations for historic telecommunication data related to (for each of 2017/18, 2018/19 and 2019/20 (to 1 March)). For example, [#] authorisations related to offences in Division [x] of [x] Act.

a. If you cannot provide this information, please provide a detailed explanation as to why it is not possible.

A breakdown of the relevant special investigation or special operation determination related to ACIC authorisations for historic telecommunications data is below. This data should be considered as an approximate guide only, as the system used to extract this information produces some duplicates and anomalies, which would require a time-intensive manual process to rectify.

Determinations	2017-18	2018-19	2019-20
Targeting Criminal Wealth No. 2 Special Investigation (SI)	2,187	654	13
Targeting Criminal Wealth No. 3 SI	1,299	2,125	1,158
National Security Impacts from Serious Organised Crime No. 3 Special Operation (SO)	350	157	174
Cyber-Related Offending No. 2 SO	10	18	15
Firearm Trafficking No. 2 SO	56	93	177
Emerging Organised Crime Threats No. 3 SO	160	612	367
No determination recorded in the system	1,591	407	0
High Risk and Emerging Drugs No. 4 SO	888	0	651
Criminal Exploitation of Australia's Migration System No. 2 SO	3	3	10
Highest Risk Criminal Targets No. 2 SI	169	471	154
Emerging and Organised Crime Targets No. 2 SO	244	87	13
Highest Risk Criminal Targets No. 3 SI	1	555	581
High Risk and Emerging Drugs No. 3 SO	566	809	115
High Risk and Emerging Drugs No. 3 and High Risk and Emerging Drugs No. 4 SO	3	461	28
Highest Risk Criminal Targets No.1 SI	0	69	143
Outlaw Motor Cycle Gangs No. 2 SO	0	42	80
Firearms Trafficking No. 1 SO	0	7	0
TOTAL	**7498**	**6536**	**3679**

18. How many authorisations for historic telecommunication data under section 178 did not relate to the investigation of a serious offence (as defined in the TIA Act) or an offence against the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years (for each of 2017/18, 2018/19 and 2019/20 (to 1 March))?

a. If you cannot provide this information, please provide an approximation.

b. If you cannot provide an approximation, please provide a detailed explanation as to why it is not possible to provide any information.

None. The ACIC can only investigate serious offences in relation to ACIC Board approved determinations for special investigations and special operations. All ACIC authorisations for historic telecommunications data are issued in relation to a serious offence and under an ACIC Board approved determination and project. The ACIC has provided a breakdown of the special investigation or special operation determination related to ACIC authorisations for the relevant period at question 17.

19. How many authorisations for historic telecommunication data under section 179 did not relate to the investigation of a serious offence (as defined in the TIA Act) or an offence against the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years (for each of 2017/18, 2018/19 and 2019/20 (to 1 March))?

a. If you cannot provide this information, please provide an approximation.

b. If you cannot provide an approximation, please provide a detailed explanation as to why it is not possible to provide any information.

The ACIC has not issued any authorisations under section 179 over the specified time periods.

20. In 2017/18, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 50 occasions?

The ACIC systems used in relation to telecommunications data authorisations do not capture this information in a way that can be readily extracted.

21. In 2018/19, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 50 occasions?

Please refer to response to question 20 above.

22. In 2017/18, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 100 occasions?

Please refer to response to question 20 above.

23. In 2018/19, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 100 occasions?

Please refer to response to question 20 above.

24. In 2017/18, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 200 occasions?

Please refer to response to question 20 above.

25. In 2018/19, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 200 occasions?

Please refer to response to question 20 above.

26. In 2017/18, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 500 occasions?

Please refer to response to question 20 above.

27. In 2018/19, how many individual officers exercised their power to authorise the release of historic telecommunications data on more than 500 occasions?

Please refer to response to question 20 above.

28. In 2017/18, how many authorised officers did not exercise their power to authorise the release of historic telecommunications data at all?

The ACIC systems used in relation to telecommunications data authorisations do not maintain records in relation to officers that have not exercised their powers, and a manual review would be required to identify these officers.

29. In 2018/19, how many authorised officers did not exercise their power to authorise the release of historic telecommunications data at all?

Please refer to response to question 28 above.

30. As at 1 March 2020, how many authorised officers have not exercised their power to authorise the release of historic telecommunications data in 2019/20?

As at 1 March 2020, the following authorised officers have not exercised their power to authorise the release of historic telecommunications data in 2019-20:

- Executive Director Intelligence Operations
- Executive Director Capability
- National Manager Operational Strategy
- National Manager Strategic Intelligence Capability
- National Manager Technical Intelligence Capability
- National Manager Human Intelligence Capability

- Manager Monitoring and Assessment Unit
- Manager Australian Gangs Intelligence Coordination Centre
- Manager Financial Crime Fusion Centre
- Manager Covert Technical Capability
- Manager Covert Technical Operations
- Team Leader Joint Analyst Group - Victoria
- Team Leader Joint Analyst Group - New South Wales
- Team Leader Joint Analyst Group - Queensland
- Team Leader Joint Analyst Group - South Australia

31. Typically, how much knowledge or involvement would an officer who authorises the release of historic telecommunications data have in the particular investigation to which an authorisation relates?

The vast majority of historic telecommunications data are requested through the Intelligence Operations teams and Joint Analyst Groups in each state and territory. Each team is led by an Investigations Manager or Regional Intelligence Manager who oversees and manages all operations in their area of control.

The Investigations Manager or Regional Intelligence Manager, who are also, in most cases, the relevant authorised officer, have intimate knowledge of all operations and intelligence projects being undertaken by their teams. In instances where the Investigations Manager or Regional Intelligence Manager is unavailable to authorise a particular request, the team requesting the data must provide sufficient background information to an authorised officer so that an informed decision can be made as to whether an authorisation should be provided or not.

32. Please provide a detailed explanation of what the internal approval process for the release of historic telecommunications data looks like within your agency.

An outline of the ACIC's internal approval process for the release of historic telecommunications data is below:

- A task requesting historic telecommunications data is generated by the team (usually an Intelligence Analyst or Investigator).
- The requesting officer **must** provide information in the request to establish the **necessity** of the authorisation (linking nexus between the device, suspect and investigation), **proportionality** (taking into account the possible privacy intrusion), and the relevant **offence(s)** (including potential penalties).
- The task is processed by Operational Support Officers, which initiate the task and forward the request to the relevant authorised officer.
- The authorised officer reviews the request. If sufficient information is provided which justifies the release of historic telecommunications data, given consideration to **necessity, proportionality and offence**, the authorised officer provides his or her approval and

forwards the task to the Operational Support Officers, which notify the carrier(s) and provide the necessary authorisation.

33. In 2017/18, what was the average amount of time that authorised officers spent considering a request for the making of an authorisation for the release of historic telecommunications data?

The ACIC systems used in relation to telecommunications data authorisations do not maintain records in relation to the average amount of time that authorised officers spent considering a request for the making of an authorisation.

34. In 2018/19, what was the average amount of time that authorised officers spent considering a request for the making of an authorisation for telecommunications data?

Please refer to response to question 33 above.

35. What was the shortest amount of time an authorised officer spent considering a request for the making of an authorisation for the release of historic telecommunications data in 2017/18?

The ACIC systems used in relation to telecommunications data authorisations do not maintain records in relation to the shortest amount of time that authorised officers spent considering a request for the making of an authorisation.

36. What was the shortest amount of time an authorised officer spent considering a request for the making of an authorisation for the release of historic telecommunications data in 2018/19?

Please refer to response to question 35 above.

37. How resource intensive is the process of working through the thresholds for the use of the powers in sections 178, 178A and 179 to authorise the release of historic telecommunications data?

The resource impact of working through the thresholds for the use of these powers to authorise the release of historic telecommunications data varies from request to request, depending on the relevant special investigation or special operation determination and the information supplied for the authorised officer to consider.

As outlined above, all ACIC authorised officers undertake mandatory training every 12 months and appropriately consider each request, taking into account information relating to the **necessity** of the authorisation (linking nexus between the device, suspect and investigation), **proportionality** (taking into account the possible privacy intrusion), and the relevant **offence(s)** (including potential penalties).

38. Are the decision-making criteria for the use of the powers in sections 178, 178A and 179 applied consistently by the various authorised officers in your agency? If so, how do you know? Please provide evidence.

Yes, the decision making criteria for the use of these powers is consistently applied by all ACIC authorised officers. As outlined above, all ACIC authorised officers undertake mandatory training every 12 months and appropriately consider each request, taking into account information relating to the **necessity** of the authorisation (linking nexus between the device, suspect and investigation), **proportionality** (taking into account the possible privacy intrusion), and the relevant **offence(s)** (including potential penalties).

Further, all ACIC authorised officers are provided with an in-depth delegate briefing which includes legal, compliance and technical considerations required to fulfil their role and authorise instruments. In addition to the delegate briefing, all ACIC staff, including authorised officers, must complete EIC training and pass an assessment prior to any use or access of the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*.

Use of powers – authorisations for prospective telecommunications data

39. How many authorisations for prospective telecommunications data did your agency make in 2018/19?

The ACIC made 1,279 authorisations for prospective telecommunications data in 2018-19.

40. As at 1 March 2020, how many authorisations for prospective telecommunications data has your agency made in 2019/20? If precise numbers cannot be provided, please provide an estimate with an explanation of how you arrived at the estimate.

As at 1 March 2020, the ACIC had made 852 authorisations for prospective telecommunications data in 2019-20.

41. How many individuals did the authorisations for prospective telecommunications data made by your agency in 2018/19 relate to? If precise numbers cannot be provided, please provide an estimate with an explanation of how you arrived at the estimate.

ACIC systems maintain records for each authorisation for prospective telecommunications data and the name of the targeted person if known. Due to the nature of ACIC investigations, there are instances where the name of the person of interest is unknown at the time of issuing the authority. As a result, the ACIC is only able to provide an estimate of how many individuals the authorisations for prospective telecommunications data made by the agency in 2018-19 related to.

The ACIC estimates that authorisations for prospective telecommunications data in 2018-19 related to 578 individuals (395 recorded names and 183 unknown persons). In addition, the ACIC's Operational Support Officers identified a further 310 unique service numbers relating to prospective telecommunications data authorisations in 2018-19. The individuals linked to these unique service

numbers are unable to be readily extracted from ACIC systems, and would require significant manual analysis.

42. As at 1 March 2020, how many individuals have the authorisations for prospective telecommunications data in 2019/20 related to? If precise numbers cannot be provided, please provide an estimate with an explanation of how you arrived at the estimate.

ACIC systems maintain records for each authorisation for prospective telecommunications data and the name of the targeted person if known. Due to the nature of ACIC investigations, there are instances where the name of the person of interest is unknown at the time of issuing the authority. As a result, the ACIC is only able to provide an estimate of how many individuals the authorisations for prospective telecommunications data made by the agency in 2019-20 (as at 1 March 2020) related to.

The ACIC estimates that, as at 1 March 2020, authorisations for prospective telecommunications data in 2019-20 related to 411 individuals (298 recorded names and 113 unknown persons). In addition, the ACIC's Operational Support Officers identified a further 104 unique service numbers relating to prospective telecommunications data authorisations in 2019-20 (as at 1 March 2020). The individuals linked to these unique service numbers are unable to be readily extracted from ACIC systems, and would require significant manual analysis.

43. Could you provide a breakdown of the offence provisions that authorisations for prospective telecommunication data related to (for each of 2017/18, 2018/19 and 2019/20 (to 1 March))? For example, [#] authorisations related to offences in Division [x] of [x] Act.

a. If you cannot provide this information, please provide a detailed explanation as to why it is not possible.

A breakdown of the relevant special investigation or special operation determination related to ACIC authorisations for prospective telecommunications data is below. This data should be considered as an approximate guide only, as the system used to extract this information produces some duplicates and anomalies, which would require a time-intensive manual process to rectify.

Determinations	2017/18	2018/19	2019/20
Emerging Organised Crime Threats No. 1 SO	3	0	0
Emerging Organised Crime Threats No. 2 SO	76	47	7
Emerging Organised Crime Threats No. 3 SO	0	3	113
Firearms Trafficking No. 1 SO	4	0	0
Firearms Trafficking No. 2 SO	0	24	12
Highest Risk Criminal Targets No. 1 SI	3	0	0
Highest Risk Criminal Targets No. 2 SI	117	113	41
Highest Risk Criminal Targets No. 3 SI	0	35	132
High Risk and Emerging Drugs No. 2 SO	1	0	0
High Risk and Emerging Drugs No. 3 SO	291	194	45
High Risk and Emerging Drugs No. SO 4	0	6	85
Targeting Criminal Wealth No. 2 SO	378	233	21
Targeting Criminal Wealth No. 3 SO	0	138	170
National Security Impacts from Serious Organised Crime No 3 SO	58	76	68
Outlaw Motor Cycle Gangs No. 2 SO	13	15	10
Cyber-Related Offending No. 2 SO	0	0	2
No determination recorded in the system	438	381	152
TOTAL	**1382**	**1279**	**852**

44. In 2017/18, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 25 occasions?

Approximately 11 ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 25 occasions in 2017-18.

45. In 2018/19, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 25 occasions?

Approximately 10 ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 25 occasions in 2018-19.

46. In 2017/18, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 50 occasions?

Approximately 10 ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 50 occasions in 2017-18.

47. In 2018/19, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 50 occasions?

Approximately 6 ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 50 occasions in 2018-19.

48. In 2017/18, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 100 occasions?

Approximately 7 ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 100 occasions in 2017-18.

49. In 2018/19, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 100 occasions?

Approximately 4 ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 100 occasions in 2018-19.

50. In 2017/18, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 250 occasions?

No ACIC officers exercised their power to authorise the release of prospective telecommunications data on more than 250 occasions in 2017-18.

51. In 2018/19, how many individual officers exercised their power to authorise the release of prospective telecommunications data on more than 250 occasions?

Approximately 1 ACIC officer exercised his or her power to authorise the release of prospective telecommunications data on more than 250 occasions in 2018-19.

52. In 2017/18, how many authorised officers did not exercise their power to authorise the release of prospective telecommunications data at all?

The ACIC is unable to provide an accurate estimate of how many authorised officers did not exercise their power to authorise the release of prospective telecommunications data at all. The ACIC systems used in relation to telecommunications data authorisations do not maintain records in relation to officers that have not exercised their powers, and a manual review would be required to identify these officers.

53. In 2018/19, how many authorised officers did not exercise their power to authorise the release of prospective telecommunications data at all?

Please refer to response to question 52 above.

54. As at 1 March 2020, how many authorised officers have not exercised their power to authorise the release of prospective telecommunications data in 2019/20?

Please refer to response to question 52 above.

55. Typically, how much knowledge or involvement would an officer who authorises the release of prospective telecommunications data have in the particular investigation to which an authorisation relates?

The vast majority of prospective telecommunications data are requested through the Intelligence Operations teams and Joint Analyst Groups in each state and territory. Each team is led by an Investigations Manager or Regional Intelligence Manager who oversees and manages all operations in their area of control.

The Investigations Manager or Regional Intelligence Manager, who are also, in most cases, the relevant authorised officer, have intimate knowledge of all operations and intelligence projects being undertaken by their teams. In instances where the Investigations Manager or Regional Intelligence Manager is unavailable to authorise a particular request, the team requesting the data must provide sufficient background information to an authorised officer so that an informed decision can be made as to whether an authorisation should be provided or not.

56. Please provide a detailed explanation of what the internal approval process for the release of prospective telecommunications data looks like within your agency.

An outline of the ACIC's internal approval process for the release of prospective telecommunications data is below:

- A task requesting prospective telecommunications data is generated by the team (usually an Intelligence Analyst or Investigator). The requesting officer submits this request using the ACIC's self-service compliance management system.
- The requesting officer **must** provide information in the request to establish the **necessity** of the authorisation (linking nexus between the device, suspect and investigation), **proportionality** (taking into account the possible privacy intrusion), and the relevant **offence(s)** (including potential penalties).
- The ACIC's compliance management system generates the relevant instrument for approval by the authorised officer.
- The authorised officer reviews the request. If sufficient information is provided which justifies the release of historic telecommunications data, given consideration to **necessity, proportionality and offence**, the authorised officer provides his or her approval and processes the authorisation in the compliance management system.
- Once approved, an Assurance Officer will notify the carrier(s) and provide the necessary authorisation.

57. In 2017/18, what was the average amount of time that authorised officers spent considering a request for the making of an authorisation for the release of prospective telecommunications data?

The ACIC systems used in relation to telecommunications data authorisations do not maintain records in relation to the average amount of time that authorised officers spent considering a request for the making of an authorisation.

58. In 2018/19, what was the average amount of time that authorised officers spent considering a request for the making of an authorisation for telecommunications data?

Please refer to response to question 57 above.

59. What was the shortest amount of time an authorised officer spent considering a request for the making of an authorisation for the release of prospective telecommunications data in 2017/18?

The ACIC systems used in relation to telecommunications data authorisations do not maintain records in relation to the shortest amount of time that authorised officers spent considering a request for the making of an authorisation.

60. What was the shortest amount of time an authorised officer spent considering a request for the making of an authorisation for the release of prospective telecommunications data in 2018/19?

Please refer to response to question 59 above.

61. How resource intensive is the process of working through the thresholds for the use of the powers in section 180 to authorise the release of prospective telecommunications data?

The resource impact of working through the thresholds for the use of these powers to authorise the release of prospective telecommunications data varies from request to request, depending on the relevant special investigation or special operation determination and the information supplied for the authorised officer to consider.

As outlined above, all ACIC authorised officers undertake mandatory training every 12 months and appropriately consider each request, taking into account information relating to the **necessity** of the authorisation (linking nexus between the device, suspect and investigation), **proportionality** (taking into account the possible privacy intrusion), and the relevant **offence(s)** (including potential penalties).

62. Are the decision-making criteria for the use of the powers in section 180 applied consistently by the various authorised officers in your agency? If so, how do you know? Please provide evidence.

Yes, the decision making criteria for the use of the powers in section 180 is consistently applied by all ACIC authorised officers. As outlined above, all ACIC authorised officers undertake mandatory training every 12 months and appropriately consider each request, taking into account information relating to the **necessity** of the authorisation (linking nexus between the device, suspect and investigation), **proportionality** (taking into account the possible privacy intrusion), and the relevant **offence(s)** (including potential penalties).

Further, all ACIC authorised officers are provided with an in-depth delegate briefing which includes legal, compliance and technical considerations required to fulfil their role and authorise instruments. In addition to the delegate briefing, all ACIC staff, including authorised officers, must complete EIC training and pass an assessment prior to any use or access of the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*.

Use of section 280 of the Telecommunications Act

63. Since 13 April 2015, has your agency ever accessed a person's telecommunications data in reliance on section 280 of the *Telecommunications Act* in conjunction with another law? If so:

- **a. On how many occasions?**
- **b. On what dates?**
- **c. In each case, what law did you rely on to authorise the disclosure of telecommunications information (in conjunction with section 280)?**
- **d. In each case, why did you rely on that other law rather than using your powers under the TIA Act?**
- **e. In each case, did you use that information as part of an investigation? If so, please provide details.**
- **f. In each case, did you use that information as evidence in a prosecution? If so, please provide details.**

The ACIC has not accessed a person's telecommunications data in reliance on section 280 of the *Telecommunications Act* in conjunction with another law over the specified time period.

64. Since 13 April 2015, has your agency ever requested a person's web browsing history in reliance on (i) section 280 of the *Telecommunications Act* and (ii) some other law? If so:

- **a. On how many occasions?**
- **b. When?**
- **c. In each case, what law did you rely on to authorise the disclosure of telecommunications information (in conjunction with section 280)?**
- **d. In each case, did you use that information as part of an investigation? If so, please provide details.**
- **e. In each case, did you use that information as evidence in a prosecution? If so, please provide details.**

The ACIC has not requested a person's web browsing history in reliance on section 280 of the *Telecommunications Act* and some other law over the specified time period.

Innocent parties – historic telecommunications data

65. In 2017/18, how many of the authorisations for historic telecommunications data that were made by your agency related to innocent parties?

ACIC systems do not capture individual instances where authorisations for historic telecommunications data that were made by the agency related to innocent parties, and this information is not readily extractable. While there have certainly been instances where access to historic telecommunications data has ruled out a telecommunications number or person from an active investigation, it is difficult to quantify the number of cases where this has occurred without manually inspecting all records and interrogating relevant ACIC systems.

For background, the ACIC's *Telecommunications (Interception and Access) Act 1979* Policy and Procedure provides safeguards and controls in relation to the access, use and communication of authorisation and warrant information. This includes instruction in the instance of an administrative, legal or technical anomaly that is, or may be, a breach of the Act, which requires relevant information to be restricted and quarantined.

66. In 2017/18, how many individuals were ruled out from suspicion as a result of your agency's use of historic telecommunications data?

Please refer to response to question 65 above.

67. In 2018/19, how many of the authorisations for historic telecommunications data that were made by your agency related to innocent parties?

Please refer to response to question 65 above.

68. In 2018/19, how many individuals were ruled out from suspicion as a result of your agency's use of historic telecommunications data?

Please refer to response to question 65 above.

69. As at 1 March 2020, how many of the authorisations for historic telecommunications data that were made by your agency in 2019/20 related to innocent parties?

Please refer to response to question 65 above.

70. As at 1 March 2020, how many individuals have been ruled out from suspicion as a result of your agency's use of authorisations for historic telecommunications data in 2019/20?

Please refer to response to question 65 above.

Innocent parties – prospective telecommunications data

71. In 2017/18, how many of the authorisations for prospective telecommunications data that were made by your agency related to innocent parties?

The ACIC has identified no authorisations for prospective telecommunications data that were made by the agency which related to innocent parties in 2017-18.

For background, the ACIC's *Telecommunications (Interception and Access) Act 1979* Policy and Procedure provides safeguards and controls in relation to the access, use and communication of authorisation and warrant information. This includes instruction in the instance of an administrative, legal or technical anomaly that is, or may be, a breach of the Act, which requires relevant information to be restricted and quarantined.

72. In 2017/18, how many individuals were ruled out from suspicion as a result of your agency's use of prospective telecommunications data?

ACIC systems do not capture individual instances where authorisations for prospective telecommunications data that were made by the agency ruled out persons as suspects.

73. In 2018/19, how many of the authorisations for prospective telecommunications data that were made by your agency related to innocent parties?

In 2018-19, the ACIC made one authorisation for prospective telecommunications data which related to an innocent party.

For background, the ACIC's *Telecommunications (Interception and Access) Act 1979* Policy and Procedure provides safeguards and controls in relation to the access, use and communication of authorisation and warrant information. This includes instruction in the instance of an administrative,

legal or technical anomaly that is, or may be, a breach of the Act, which requires relevant information to be restricted and quarantined.

74. In 2018/19, how many individuals were ruled out from suspicion as a result of your agency's use of prospective telecommunications data?

Please refer to response to question 72 above.

75. As at 1 March 2020, how many of the authorisations for prospective telecommunications data that were made by your agency in 2019/20 related to innocent parties?

As at 1 March 2020, the ACIC had made approximately 5 authorisations for prospective telecommunications data which related to innocent parties in 2019-20. The ACIC is continuing to undertake quality assurance to validate this figure.

For background, the ACIC's *Telecommunications (Interception and Access) Act 1979* Policy and Procedure provides safeguards and controls in relation to the access, use and communication of authorisation and warrant information. This includes instruction in the instance of an administrative, legal or technical anomaly that is, or may be, a breach of the Act, which requires relevant information to be restricted and quarantined.

76. As at 1 March 2020, how many individuals have been ruled out from suspicion as a result of your agency's use of authorisations for prospective telecommunications data in 2019/20?

Please refer to response to question 72 above.

Innocent parties – retention of telecommunications data

77. As at 1 March 2020, when a person is ruled out from suspicion as a result of your agency's use of authorisations for telecommunications data (whether historic or prospective), does your agency delete the individual's telecommunications data from your system? If so:

- **a. Whose responsibility is it to delete the individual's telecommunications data from your system?**
- **b. What systems are in place to ensure that this happens?**
- **c. Is there a policy that governs these matters? If so, please provide the Committee with a copy.**

The ACIC's *Telecommunications (Interception and Access) Act 1979* Policy and Procedure provides safeguards and controls in relation to the access, use and communication of authorisation and warrant information. This includes instruction in the instance of an administrative, legal or technical anomaly that is, or may be, a breach of the Act, which requires relevant information to be restricted and quarantined. The ACIC is currently reviewing all telecommunications data processes, including destructions for permitted purposes.

78. As at 1 March 2020, did your agency hold any telecommunications data that related to an individual who had been ruled out from suspicion?

a. If so, why?

b. If not, how did you satisfy yourself that your agency does not hold any of this information? How can you be certain?

ACIC systems do not capture individual instances where the agency held any telecommunications data that ruled out persons as suspects.