AUSTRALIAN FEDERAL POLICE

PARLIAMENTARY INQUIRY QUESTION TAKEN ON NOTICE:

Intelligence and Security .

28 February 2020

Subject: PJCIS – Review of the mandatory data retention regime

Asked

Question Submitted by: Senator Fawcett and Julian Leeser

Question:

Senator Fawcett: Commissioner, welcome. Can I take you to table 5 in your submission, which looks at authorisations granted under sections 178, 178A and 179. It usefully splits into different time brackets. The data between financial years 2016-17 and 2017-18 is somewhat variable. In the 24-months-plus category there is a very clear trend of increasing authorisations. Can you talk to the committee about the importance of data that's available beyond 24 months? In the light of very clear requests by both New South Wales and Queensland police for an extension of the mandated data retention, would you support those calls? Are there investigations where you have been frustrated by the fact that some Telco's don't hold data beyond that mandated period?
Mr Kershaw: Yes. The example that I gave, without me being emotive, was tragic in the sense that that probably would have led us to either an individual or a group of individuals who were exploiting children. My argument would be that that's just one case. We had many, and that's why I'm also very grateful to those carriers and so on that do keep that data longer than two years. Our officers will still request, because they often just hope that that data is there, but for us to substantiate—in that particular case, it was identifying the actual offender. We already had the evidence pretty much in from the other agency, the referrals that come in to say we've got this IP address et cetera. It would probably mean that criminals are getting away with it and probably continually offending in Australia and beyond. We would encourage that change and we'd welcome that. It's a serious thing. Historical matters are always going to come up, especially when we take down some of these servers and other things. Not just child protection but drug trafficking now is all done on the dark web. A lot of it is anyway, as far as international goes. It goes back a long way now. We're facing encryption and other techniques that criminal networks and criminals are using to avoid law enforcement detection. So this is a primary tool for us.
Mr LEESER: Can I interrupt Senator Fawcett on this point? How many years would you want the extension to go to and why?
Mr Kershaw: We'd probably have to talk to our Home Affairs portfolio. That would be a matter for us to discuss at a portfolio level. And we would have to talk to our partner agencies as well.
Mr LEESER: The state police suggested seven years.

Answer:

Criminal investigations are complex and access to information is crucial. The AFP provided the Committee with statistics that show data over two (2) years old has been sought, and provided, to assist investigations into very serious offending including terrorism and drug importations.

While the bulk of authorisations by AFP relate to data under two (2) years old, complex and more serious investigations may necessitate authorisations be made more than two years after the fact. The AFP is grateful to providers who store data longer than the current mandatory retention period.

The AFP is aware a number of law enforcement and national security agencies have advocated for a longer retention period. While a final policy should be agreed across law enforcement and national security agencies, the AFP supports a strengthening of the data retention period.

While, as a minimum, the AFP would support maintaining the current two (2) year limit for retention as set by Parliament, the AFP would have significant concerns if there was reduction to current two (2) year period. The AFP places on record our belief this would increase the risk of harm to our communities, including the safety of children or other vulnerable groups, through an eroded ability to access crucial data.

Asked
Question Submitted by: Senator Fawcett

Question:

Senator FAWCETT: Table 4 in your submission is a very helpful breakdown of the range of offences. I note that the peaks of inquiry deal with things like illicit drugs and terrorism and the sort of offences where we give our full support to the AFP to have access to the data. But I am somewhat surprised to see, compared to the 1,764 terrorism authorisations that were requested, 16 traffic and vehicle regulatory offences. You've heard the concern of the committee about some other agencies at a state level accessing metadata for things that are not what we would call serious crime. As we look at that, and we look at 31 requests for property damage and environment pollution, I'm interested to get your perspective on why they are there and what the impact on you and like bodies in state jurisdictions would be if we sought to limit this to purely the majority of your table, which is serious and violent crime?
Mr Kershaw: To get the detail of those particular 16, that was in 2015-16. Could I take that on notice? I myself would be interested in having a look at what those particular matters entailed. Would that assist?
Senator FAWCETT: It would help if you could take that on notice. As well, there's 'miscellaneous offences'. I would be interested to know what's included in that. There's also 'offences relating to the enforcement of law imposing a pecuniary penalty'. I would be interested to know about that.
Mr Kershaw: I could take all them on notice.
Senator FAWCETT: And 'property damage and environment pollution'. That would be just good to know. They seem at odds with the rest of your table, which is large and extensive and deals with all the issues that we consider that you need to have the access for.
Mr Kershaw: I am only speculating, but I would suspect it has to do with ACT policing and our other functions, even with some of our establishments and other operations. But I'll come back to you.

Answer:

The statistics referenced in Table 4 of the AFP submission includes both AFP National and ACT Policing data. The AFP adheres to the Attorney-General's Department guidance which adopts and expands on the Australian and New Zealand Standard Offence Classification (ANZSOC) which is the standardised statistical framework for organising key behavioural characteristics of criminal offences and to overcome differences in legal offence definitions across states and territories.

Miscellaneous Offences

According to the ANZSOC, miscellaneous offences are defined as an offence which involves a breach of statutory rules or regulations governing activities that are prima facie legal, where such offences are not explicitly dealt with under any other division.

Some offences identified by the AFP in this category include offences relating to certain migration offences, and the making of nuisance calls or hoax threats (relevant to public health and safety) and trade mark offences.

Traffic and vehicle regulatory offences

The AFP notes this category includes higher end traffic offences, such as driving while suspended, aggravated furious, reckless or dangerous driving, negligent driving causing death and culpable driving causing death or grievous bodily harm. An offender may also be charged with vehicle regulatory offences at the same time as the more serious charge. ACT Policing has observed that recidivist property offenders may engage in dangerous driving behaviours in combination with committing serious offences including aggravated robbery, which pose significant risks to the ACT community.

Property damage and environment pollution

According to the ANZSOC, property damage and environment pollution offences is defined as the wilful and unlawful destruction, damage or defacement of public or private property, or the pollution of property or a definable entity held in common by the community.

Offences involving property damage could potentially be included in this category.

Offences relating to the enforcement of law imposing a pecuniary penalty

This could include offences under the Customs Act such as smuggling tobacco.

Asked

Question Submitted by: *Mark Dreyfus*

Question:

Mr DREYFUS: The other matter I want to raise with you really arises from the fact that this committee recently completed a review of a proposal for a national facial recognition system. We're told that the government is going to introduce legislation again on that subject in this current session of parliament, so it will come back. There are media reports today that agencies across Australia are using the facial recognition technology of a company called Clearview AI. Does the AFP use this technology?
Mr Kershaw: I have asked that question today myself, off the back of media reporting. To give you a fulsome answer, I'd like to take that on notice until I've clarified the information.
Mr DREYFUS: The media report says the AFP has rejected several freedom of information requests in relation to Clearview AI. Do you know why those requests have been rejected?
Mr Kershaw: I have had advice from my legal team, who have advised me that they need to do some further digging, given the media reporting and the matters raised in those articles.
Mr DREYFUS: You will appreciate the concern in in this committee that, in the absence of existing legal framework in Australia, the thought that such facial recognition technology was being used by the Australian Federal Police would be a concern. We would like you to take that on notice.
Mr Kershaw: I'd like to take that on notice.
Mr BYRNE: This is not a criticism, but to add to that, we're also advised that that particular service has been hacked. When we've been looking at the biofacial data regime, one of the key points of concern is that it's almost like a fingerprint. If someone can steal your fingerprint, the ramifications of that are gravely concerning. So I am gently flagging our concerns. If this is something that's being used by law enforcement and it has been hacked, then you have a system that is potentially vulnerable. We're keen to understand where it's at.
Mr Kershaw: I'll come back to you.

Answer:

1. *Does the AFP use this technology?*

The AFP has not adopted the facial recognition platform Clearview.AI as an enterprise product and has not entered into any formal procurement arrangements with Clearview.AI.

However, between 2 November 2019 and 22 January 2020, members of the AFP-led Australian Centre to Counter Child Exploitation (ACCCE) registered for a free trial of the Clearview AI facial recognition tool and conducted a limited pilot of the system in order to ascertain its suitability. The trial was to assess the capability of the Clearview.AI system in the context of countering child exploitation.

This trial involved nine (9) invitations sent from Clearview.AI to AFP officers to register for a free trial. Of these, seven (7) AFP officers then activated the trial and conducted searches. These searches included images of known individuals, and unknown individuals related to current or past investigations relating to child exploitation.

Outside of the ACCCE Operational Command there was no visibility that this trial had commenced. The potential value of the Clearview.AI product in identifying victims or perpetrators of child abuse had been communicated to the AFP via the national and international network of agencies who work collaboratively on this crime. This motivated the commencement of a limited trial.

The AFP is continuing to review this matter internally. It is our understanding that, accepting the limited pilot outlined above, that no other areas or individuals have utilised the Clearview.AI product or engaged with the company.

The Office of the Australian Information Commissioner (OAIC) has issued a notice to produce under s/44 of the Privacy Act in relation to Clearview.AI. The AFP is fully cooperating with the OAIC and is continuing to review and evaluate our governance and policy setting in this space.

The AFP seeks to balance the privacy, ethical and legal challenges of new technology with its potential to solve crime and even save victims. We are actively looking to improve our processes and governance without necessarily constraining innovative investigative approaches.

2. *The media report says the AFP has rejected several freedom of information requests in relation to Clearview AI. Do you know why those requests have been rejected?*

The AFP received three requests under the Freedom of Information Act 1982 (FOI Act) on 22 January 2020, 24 January 2020, and 4 February 2020, seeking documents held by the AFP relating to Clearview AI. The requests were processed in accordance with the FOI Act, in that reasonable searches were undertaken by the AFP portfolio with responsibility for facial identification capabilities. No information relating to Clearview AI was identified.

On 14 February 2020, the AFP wrote to each FOI applicant stating reasonable steps had been taken to find the documents, however no documents had been located. As such, the FOI requests were refused in accordance with section 24A(b)(ii) of the FOI Act, which provides an agency may refuse a request for access to a document if all reasonable steps have been taken to find the document and the agency is satisfied the document does not exist.

It was subsequently discovered, in our response to Question 1 (above), the AFP-hosted Australian Centre to Counter Child Exploitation (ACCCE) held information relevant to Clearview AI, which was not identified in response to the earlier freedom of information requests.

Asked
Question Submitted by: *Mark Dreyfus*

Question:

Mr DREYFUS: Just a small thing on the stats—thanks very much for the breakdown you've provided in your submission—it only goes up to the 2017-18 year. We've got, in the Home Affairs annual report of the last year, your high level stats for 2018-19. I wonder if I could ask you to extend the table that you've already provided to encompass the 2018-19 figures but broken down in the way that you have in the table?
Mr Kershaw: Yes, we can do that.
Mr DREYFUS: Thanks very much. On the question of individuals, which I've asked the other agencies about, in 2018-19 the AFP made about 17,000 authorisations for historic telecommunications data under sections 178 and 179. I'm sure you haven't got it to hand, but are you able to estimate or tell us something about how many individuals that is likely to relate to?
Mr Kent: Our current systems don't actually capture the number of people that that would relate to. Attribution then back to persons would be quite challenging for us to obtain, so the short answer is I don't believe we could do that quickly or easily using our current systems. They simply don't carry that attribution. I think it goes to the efficiency of the system. Unlike other aspects of the act, we're not required to record efficiency as it pertains to this particular provision.
Mr DREYFUS: Can you offer an anecdotal view of this, Deputy Commissioner? I'm assuming that the 17,000 authorisations definitely didn't relate to 17,000 individuals.
Mr Kent: Without doubt there would be multiple devices for individuals. It would be more than likely that the number of individuals impacted would be much lower.
Mr DREYFUS: I appreciate you not keeping this stat. I invite you to take on notice that question of giving the committee some idea of what number of individuals this might relate to, even if it's a range, or even if it's just to state formally to us, 'It's less than the last year. It's less than 17,000 individual people.'
Mr Kent: Yes, certainly, we can take that on notice.
Mr DREYFUS: See how you go. I asked the other agencies who were here earlier about the department's proposition that the regime already contains a number of rigorous conditions that must be satisfied before agencies seek access to telecommunications data for investigations and operations. When these thresholds are applied in succession it ensures that agencies exercise their power to access telecommunications data appropriately and only when necessary. It's paragraph at 94 of the department's submission. How many officers in the AFP have got power to make these authorisations?
Mr Kershaw: We did hear that question. To give you the exact number I will have to come back to you, but its commissioned officers, which we're estimating around 250 in the AFP.

Answer:

Updated Table 4 ***(Attachment A).***

The AFP's data retention request management system does not capture details of how many individuals an authorisation relates to. It is the AFP experience that often persons of interest to investigations use multiple handset or multiple SIMS to obfuscate their identity. Therefore the number of individuals would be less than the number of authorisations.

As at 1 March 2020 the AFP consisted of 132 Sworn Superintendents and 41 Sworn Senior Executive employees; and one (1) Officer in Charge (Sergeant) in ACT Policing who is also authorized by instrument of Authorisation. The total number of officers able to make authorisations was 174.

Asked

Question Submitted by: *Mark Dreyfus*

Question:

Mr DREYFUS: I've got a couple more questions. One is in relation to the specific category of authorising historic telecommunications data to enforce what are described as public order offences. This, again, is out of the annual report. For the AFP, it's a very small number. There are 14 authorisations, but it still struck me as a somewhat unusual category for the AFP. Can you say what those offences would have been?
Mr Kershaw: It's highly likely it's limited to perhaps our ACT policing, but also it could be our establishments that we protect as well, including Parliament House, for example, but we will take that on notice and come back to you.
Mr DREYFUS: When you do that, could you perhaps also elaborate on how many of those authorisations resulted in arrests, how many resulted in charges and how many resulted in prosecutions? It's only a small number.
Mr Kershaw: Yes.

Answer:

Three authorisations *were requested by AFP National, these were in relation to the offences of smuggling tobacco products, and for vilify or incite hatred on racial, cultural, religious or ethnic grounds. Whilst reported in annual reporting with the public order category, the smuggling tobacco offence was incorrectly classified as a property damage matter. This authorisation should have been categorised elsewhere. The three authorisations made were in relation to AFP ongoing investigations and, to date, have not resulted in an arrest, charge or prosecution.*

Eleven authorisations *were requested by ACT Policing, these related to offences including disorderly conduct, prostitution, and riot and affray offences. Whilst the results of the outcomes of the authorisations themselves are not directly attributable to charges and prosecutions, the results of the investigations for which these authorisations were sought were:*

Offence Type	***Number of Charges***	***Prosecution***
Common Assault	*2*	*1 x Convicted with recognizance*
		1 x Withdrawn before prosecution commenced
Act of Indecency	*1*	*1x Withdrawn*
Operate a brothel other than in a prescribed location	*6*	*3x Withdrawn*
		2 x Fine
		1 x Convicted with recognizance
Affray	*3*	*2x Convicted with recognizance*
		1x Withdrawn before prosecution
Breach of Good Behaviour Obligations	*1*	*1x Arrest without warrant on bail*
Total	***13***	

UNCLASSIFIED

ATTACHMENT A

Update Table 4: Offences where authorisations were made for historical data s186(1)(e), s178-180, 2015-16 - 2017-18

Offences where authorisations were made for historical data s186(1)(e)	FY15-16 s178	FY15-16 s179	FY15-16 s180	FY16-17 s178	FY16-17 s179	FY16-17 s180	FY17-18 s178	FY17-18 s179	FY17-18 s180	FY18-19 s178	FY18-19 s179	FY18-19 s180
Abduction, harassment and other offences against the person	254	0	17	559	0	32	456	0	100	516	3	64
ACC investigation	1	0	0	0	0	0	201	0	0	0	0	0
Acts intended to cause injury	150	0	7	97	0	13	16	0	6	144	0	17
Bribery or corruption	322	1	17	340	0	21	110	0	19	161	0	28
Cartel offences	10	0	0	38	0	13	10	0	24	0	0	0
Conspire/aid/abet serious offence	31	0	1	55	0	3	37	1	4	76	44	27
Cybercrime and telecommunications offences	1472	0	38	1924	0	76	179	0	132	912	0	154
Dangerous or negligent acts and endangering a person	124	0	3	192	0	7	133	0	67	93	0	2
Fraud, deception and related offences	1277	8	174	1268	12	158	947	2	138	1032	5	191
Homicide and related offences	559	0	11	281	0	23	649	0	64	414	0	46
Illicit drug offences	9504	2	1286	12362	4	1823	8200	11	2219	7636	7	2343
Loss of life	72	0	1	21	0	2	6	0	5	25	0	5
Miscellaneous offences	306	0	41	254	1	37	334	0	37	212	2	20
Offences against justice procedures, government security and government operations	105	1	2	154	4	9	327	0	123	317	1	104
Organised offences and/or criminal organisations	327	0	57	350	0	105	476	1	386	620	4	1228
Other offences relating to the enforcement of a law imposing a pecuniary penalty	70	11	0	51	5	3	43	1	1	26	4	0

UNCLASSIFIED

UNCLASSIFIED

Other offences relating to the enforcement of a law protecting the public revenue	68	12	0	30	9	5	7	0	2	6	2	0
People smuggling and related	147	0	7	171	0	2	110	0	26	260	0	35
Prohibited and regulated weapons and explosive offences	133	2	40	401	0	90	227	0	60	206	0	74
Property damage and environment pollution	31	0	0	60	0	4	56	0	10	91	0	20
Public order offences	84	0	0	7	0	5	9	0	0	14	0	1
Robbery, extortion and related offences	215	0	0	345	0	14	474	0	62	347	0	50
Serious damage to property	31	0	0	142	0		25	0	1	16	0	2
Sexual Assault and related offences	377	0	14	574	0	26	415	9	30	1658	0	75
Terrorism offences	1764	0	150	1561	0	189	1627	0	109	1367	1	72
Theft and related offences	738	0	63	768	3	55	294	1	35	466	0	97
Traffic and vehicle regulatory offences	16	0	0	27	0	4	57	0	6	44	0	2
Unlawful entry with intent/burglary, break and enter	27	0	1	95	0	8	107	0	31	159	0	47

AUSTRALIAN FEDERAL POLICE

PARLIAMENTARY INQUIRY (ADDITIONAL WRITTEN) QUESTION TAKEN ON NOTICE:

Intelligence and Security

28 February 2020

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? If not, why not? If so:**
   a. **Who conducted the audit?**
   b. **What was the outcome of the audit?**
   c. **Did the audit find any problems with how the powers were being exercised?**
   d. **Did the audit make any recommendations? What were they? Were they implemented?**
   e. **When was the audit conducted?**

PwC Australia has recently been commissioned to conduct an independent audit into requests to telecommunications carriers made by the AFP under Section 180(2) of the TIA Act. The public announcement relating to this audit can be found here: https://policenews.act.gov.au/news/media-releases/afp-scrutinise-telecommunications-requests

The AFP commissioned this audit after identifying compliance issues, some dating back to 2007. The identified issues relate to record-keeping, authorisations and reporting of requests under Section 180(2). On 24 January 2020, the AFP self-reported the identified issue to the Commonwealth Ombudsman.

The AFP has worked with the Commonwealth Ombudsman's Office to establish this agreed method of assurance through audit and inspection by PwC Australia.

This audit formally commenced on 13 March 2020, with the contractual engagement of PwC on that date. The independent audit is expected to be completed by June 2020.

On 11 March 2020, the Commonwealth Ombudsman wrote to the AFP Commissioner to inform him, under section 8 of the Ombudsman Act 1976 that the Ombudsman has determined to commence an own motion investigation into the administration of, and compliance with the telecommunications data access provisions under the Telecommunications (Interception and Access) Act 1979.

The Commonwealth Ombudsman has also informed the Minister for Home Affairs of this own motion investigation.

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 AFP's data retention management system contains limited searchable fields. To answer this question comprehensively would require significant effort to manually review each individual authorisation. Nevertheless, in checking with numerous records on hand, and with numerous investigative contact points, the AFP has not located any instances of this having occurred.

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.**

As above.

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).**

Band	Rank	Police
Bands 1-5	Constable	2310
Bands 6-8	Sergeant	697
EL	Superintendent	132
SES 1	Commander	28

SES 2	Assistant Commissioner	8
SES 3	Deputy Commissioner	4
CMR	Commissioner	1
Grand Total		**3180**

** Please note these figures are based on officer's substantive band, and exclude any rank for higher duties at the time.*

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).**

As at 1 March 2020, the AFP consisted of 132 Sworn Superintendents and 41 Sworn Senior Executive employees; as well as one (1) Officer in Charge (Sergeant) in ACT Policing who is also authorised by instrument of authorisation. The total number of officers able to make authorisations was 174.

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?**

Yes. The online Authorising Officer training package was released 17 November 2017, and officers are able to access it via the AFP's training portal.

7. **If such training was provided:**
    a. **Was it compulsory?**

Yes. In February 2018 AFP executive communicated an internal policy that all Authorising Officers must complete internal mandatory training prior to exercising their delegations.

In addition, Authorising Officers are required to complete the training package annually for certification.

    b. **What is the name of that training program?**

Authorised Officer Training.

    c. **How long is the training program?**

The course is an online program and self-paced. This allows officers the ability to pause due to operational priorities and resume when time becomes available.

The minimum estimated time to complete the course is 1 hour.

d. **What is the content of that training program?**

This training program provides AFP Authorising Officers (AO) with key points and considerations necessary to perform the duties of an Authorised Officer under the Crimes Act 1914, the Telecommunications (Interception and Access) Act 1979, and the Surveillance Devices Act 2004.

The training program will enable Authorising Officers to:

- *Understand the powers available under the legislative regimes.*
- *Understand the statutory obligations and threshold requirements to authorise certain things under the legislative regimes.*
- *Understand the reporting requirements and oversight by the Commonwealth Ombudsman.*
- *Have an understanding of the significance of compliance requirements in relation to the Acts and the potential adverse consequences of authorising an investigative power incorrectly (i.e. legislative, evidentiary, privacy and media repercussions).*
- *Know where to find assistance and resources to meet obligations.*

<u>Regimes Covered</u>

The applicable legislative regimes provide powers to covertly capture evidence and information, ensuring justification, oversight and accountability to safeguard the privacy of the Australian community.

Under the Crimes Act 1914:

- *Controlled Operations*
- *Major Controlled Operations*
- *Delayed Notification Search Warrants*

Under the Telecommunications (Interception and Access) Act 1979:

- *Telecommunications Interception Warrants*
- *Stored Communications Warrants*
- *Data Authorisations*
- *Journalist Information Warrants*
- *Control Order Interception Warrants*

Under the Surveillance Devices Act 2004:

- *Surveillance Device Warrants*
- *Tracking Device Authorisations*

e. **Who provides that training?**

The Covert Analysis & Assurance (CAA), Statutory Compliance Team business area developed the package in consultation with subject matter experts. AFP Learning & Development own the portal (iAspire) for online training packages.

iAspire is the AFP's online learning management system customised to meet personal and professional development needs as well as deliver measurable information to management.

f. **Who conducts that training?**

AFP's online Learning & Development learning management system (iAspire) delivers the training.

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

Yes. AFP internal policy requires that all Authorising Officers must successfully complete internal mandatory training prior to exercising their delegations.

At the completion of the course the officer is asked 16 questions to test their understanding and knowledge and must answer at least 80% correctly to pass.

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

Yes, as above.

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

Yes. AFP internal policy requires that all Authorising Officers successfully complete the iAspire training package prior to exercising their delegation.

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

The AFP has provided a copy of this document to the Committee on an in-confidence basis.

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?**

Yes, the Authorising Officer online training package was released on 17 November 2017 and is available to all Authorising Officers and mandatory to complete prior to utilising their delegation. Additionally the Handbook for Authorising officers is available to all Authorising Officers on the AFP intranet as a reference tool. The AFP has provided a copy of this document to the Committee on an in-confidence basis.

9. **If such training was provided:**
   a. **Was each of those programs compulsory?**

Yes. Online re-validation through successful completion of the course is also required annually.

b. **How many training programs?**

One online training package developed that extensively covers the Authorising Officer's obligations, key points and considerations necessary to perform the duties of an Authorising Officer.

One Handbook for Authorising Officers as a reference tool and further supporting material is available to members on the AFP intranet.

c. **What is the name of each of those training programs?**

The training program is the iAspire Authorising Officer online training.

d. **How often were those training programs delivered?**

Annually, and available through iAspire online training delivery system at any time.

e. **What is the content of each training program?**

Please refer to our response to question 7(d).

f. **Who provided each of those training programs?**

The online package is delivered through the AFP's Learning & Development management system (iAspire).

g. **Who conducted each of those training programs?**

As above.

h. **Was completion of regular training programs a pre-requisite to retain one's status as an authorised officer?**

Yes. In February 2018, the AFP Executive, communicated an internal policy that all Authorising Officers must complete internal mandatory training prior to exercising their delegations.

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

The AFP has provided a copy of this document to the Committee on an in-confidence basis.

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"?**

The AFP does not have systems to capture this data. However, the Professional Standards Unit advises they are not aware of any occurrences, outside of the 2017 breach the AFP self-disclosed to the Commonwealth Ombudsman. The investigation undertaken by the Ombudsman made a recommendation in relation to enhancing training for Authorised Officers which has occurred. The Ombudsman stated they 'found no evidence to counter the AFP's assessment that the breach was a mistake with no ill will, malice or bad intent involved' (Paragraph 1.34, Page 8 of the Investigation Report). The conclusions and recommendations provide a summary of the action taken by the AFP in relation to this single breach.

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"?**

The AFP does not have systems to capture this data. However, the Professional Standards Unit advises they are not aware of any occurrences.

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?**

The AFP does not have systems to capture this data. However, the Professional Standards Unit advises they are not aware of any occurrences.

Use of powers – authorisations for historic telecommunications data

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

There have been 17146 authorisations for historic telecommunications data for AFP made in 2018/19.

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, 10101 authorisations for historic telecommunications data for AFP (not including ACT Policing) were made in 2019/20.

As at 14 March 2020, 2679 authorisations for historic telecommunications data for ACT Policing were made in 2019/20.

The final count for 19/20 (for AFP including ACT Policing) will be published in 2019/20 annual reporting.

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 AFP's data retention request management system does not capture details of how many individuals an authorisation relates to. It is the AFP experience that often persons of interest to investigations use multiple handsets or multiple SIMs to obfuscate their identity. Therefore the number of individuals would be much less than the number of authorisations.

We are aware of the following examples where multiple authorisations were sought in a single investigation in 2019:

- *An investigation into the importation of illicit drugs resulted in 102 historic telecommunication authorisations made between March 2019 and August 2019.*
- *A money laundering investigation resulted in 93 historic telecommunication authorisations made between April and November 2019.*
- *An investigation into illicit drugs resulted in 159 historic telecommunications authorisations made between January and December 2019.*

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.**

As above.

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.**

The AFP's data retention management system contains limited searchable fields. To answer this question comprehensively would require significant effort to manually review each individual

authorisation. The recording database used by the AFP, records request for authorisation by major offence category. The AFP is unable to provide the specific divisions of Acts, relevant to the offence type. Please refer to ***Attachment A*** *which sets out a sample list of offence provisions under each offence category.*

The offences have been categorised and are captured below. The AFP cannot provide accurate statistics for 19/20 at this time, as these would require significant effort to manually extract. The final count for 19/20 will be published in 2019/20 annual reporting.

Offences where authorisations were made for historical data s186(1)(e)	***FY17- 18 s178***	***FY17- 18 s179***	***FY18-19 s178***	***FY18-19 s179***
Abduction, harassment and other offences against the person	*456*	*0*	*516*	*3*
ACC investigation	*201*	*0*	*0*	*0*
Acts intended to cause injury	*16*	*0*	*144*	*0*
Bribery or corruption	*110*	*0*	*161*	*0*
Cartel offences	*10*	*0*	*0*	*0*
Conspire/aid/abet serious offence	*37*	*1*	*76*	*44*
Cybercrime and telecommunications offences	*179*	*0*	*912*	*0*
Dangerous or negligent acts and endangering a person	*133*	*0*	*93*	*0*
Fraud, deception and related offences	*947*	*2*	*1032*	*5*
Homicide and related offences	*649*	*0*	*414*	*0*
Illicit drug offences	*8200*	*11*	*7636*	*7*
Loss of life	*6*	*0*	*25*	*0*
Miscellaneous offences	*334*	*0*	*212*	*2*
Offences against justice procedures, government security and government operations	*327*	*0*	*317*	*1*
Organised offences and/or criminal organisations	*476*	*1*	*620*	*4*
Other offences relating to the enforcement of a law imposing a pecuniary penalty	*43*	*1*	*26*	*4*
Other offences relating to the enforcement of a law protecting the public revenue	*7*	*0*	*6*	*2*
People smuggling and related	*110*	*0*	*260*	*0*
Prohibited and regulated weapons and explosive offences	*227*	*0*	*206*	*0*
Property damage and environment pollution	*56*	*0*	*91*	*0*
Public order offences	*9*	*0*	*14*	*0*
Robbery, extortion and related offences	*474*	*0*	*347*	*0*
Serious damage to property	*25*	*0*	*16*	*0*
Sexual Assault and related offences	*415*	*9*	*1658*	*0*
Terrorism offences	*1627*	*0*	*1367*	*1*
Theft and related offences	*294*	*1*	*466*	*0*
Traffic and vehicle regulatory offences	*57*	*0*	*44*	*0*
Unlawful entry with intent/burglary, break and enter	*107*	*0*	*159*	*0*

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.**

The AFP notes that in relation to historical data there is no requirement for the threshold offence to be a serious offence, which is distinct from the requirement for prospective data.

As above, the AFP's data retention request management system retains a record of the offence provisions, however, this is not a searchable field and would require significant resources to manually review each individual authorisation. This would be a significant diversion of AFP resources and is not possible in the timeframe.

As the statistics above demonstrate, there are some instances in which the AFP has sought historical data for offences that either do not meet the definition of a serious offence under the TIA Act, or an offence punishable by over 3 years imprisonment. This has included, for example, traffic and public order offences under state and territory laws (which are enforced by ACT Policing, and AFP officers policing external territories including Christmas Island). However, the statistics above also demonstrate that a large majority (over 85%) of the authorisations sought are in relation to offences widely regarded as serious within our community (for example, in 2018-19, 14,638 of the authorisations were in relation to homicide, loss of life, fraud, illicit drugs, sexual assault, terrorism, weapons and explosives, people smuggling, organised crime, robbery, bribery and corruption).

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))?**

In 2017/18, three authorisations for historic telecommunication data under section 179 (out of 26 in total) did not relate to the investigation of a serious offence.

In 2018/19, 13 authorisations for historic telecommunication data under section 179 (out of 73 in total) did not relate to the investigation of a serious offence.

In 2019/20 to date, seven authorisations for historic telecommunication data under section 179 did not relate to the investigation of a serious offence.

    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.**

Not applicable.

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 AFP's data retention request management system could not run a report on the number of authorisations made by individual authorising officers prior to October 2018. This was a technical deficiency of the system. A system upgrade was undertaken in October 2018, allowing data searches to occur by authorising officer name.

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

The AFP has identified that within the period October 2018 to 30 June 2019, 19 individual officers authorised release of historic telecommunications data on more than 50 occasions.

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

The AFP's data retention request management system could not run a report on the number of authorisations made by individual authorising officers prior to October 2018.

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

The AFP has identified that within the period October 2018 to 30 June 2019, 17 individual officers authorised release of historic telecommunications data on more than 100 occasions.

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

The AFP's data retention request management system could not run a report on the number of authorisations made by individual authorising officers prior to October 2018.

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

The AFP has identified that within the period October 2018 to 30 June 2019, 12 individual officers authorised release of historic telecommunications data on more than 200 occasions.

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

The AFP's data retention request management system could not run a report on the number of authorisations made by individual authorising officers prior to October 2018.

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

The AFP has identified that within the period October 2018 to 30 June 2019, one (1) officer authorised release of historic telecommunications data on more than 500 occasions.

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

Unknown, the AFP only records authorisations that are made.

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

Unknown, the AFP only records authorisations that are made.

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?**

Unknown, the AFP only records authorisations that are made.

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 level of initial knowledge or involvement an authorising officer has in relation to a request to access telecommunications data varies. For example, an authorising officer can be involved in real-time aspects of an investigation and have extensive knowledge of the case, be aware of the target entities and the usefulness and purpose of requesting telecommunications data. At the other end of the spectrum, if the authorising officer has limited or no prior knowledge of the case they may request additional background information, for example, a briefing, to satisfy the thresholds of making an authorisation.

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

The requesting officer identifies the need to access telecommunications data and completes an electronic request form. The request form is designed to capture the request types specific to each carrier, as well as meet the authorising officer considerations, reason for request and reporting requirements.

The request is emailed to the authorising officer for approval or rejection. The authorising officer may seek additional information from the requesting officer, if required.

If approved, the request is emailed by the authorising officer to the team of 'notifying officers', responsible for sending the request to the carrier as well as maintaining a record of the authorisation, request and result.

The AFP has previously provided the Committee with a detailed summary of internal AFP considerations made prior to formalising a request to obtain Historical Telecommunications Data.

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 AFP's data retention request management system does not capture the length of time an authorising officer spends considering the request. The time spent would vary to accord with the level of initial knowledge or involvement an authorising officer has in relation to a request to access telecommunications data.

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?**

As 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?**

As above.

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?**

As 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 length of time and number of persons involved in submitting, approving and notifying the carrier varies depending on the complexity of the request and prior knowledge the authorising officer has in relation to the case. The authorising officer may request additional information in order to satisfy the thresholds around usefulness, relevance and privacy.

Typically, a standard request would involve a requesting officer attached to an investigation completing the request form, including the purpose of the telecommunications data sought; the authorising officer's own considerations; and the notifying officer's role in sending the request to the carrier.

The notifying officer also facilitates compliance, record-keeping and reporting obligations.

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.**

The prompts and wording in the request form serves as a consistent approach for all requesting and authorising officers when considering and making an authorisation.

Use of powers – authorisations for prospective telecommunications data

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

In 2018/19, 4633 authorisations for prospective telecommunications data were made by the AFP.

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.**

In 2019/20, 3227 authorisations for prospective telecommunications data were made by the AFP.

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.**

An estimated 1628 authorisations for prospective telecommunications data in 2018/19 related to specified individuals. This estimation was reached by exporting data for the 2018/19 period and removing duplicate individual names. This figure does not take into account instances where the user of the telecommunication service was unidentified.

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.**

An estimated 1294 authorisations for prospective telecommunications data in 2019/20 related to specified individuals. This estimation was reached by exporting data for the 2019/20 period and removing duplicate individual names. This figure does not take into account instances where the user of the telecommunication service was unidentified.

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.**

The recording database used by the AFP records requests for authorisations by major offence category. Unfortunately, the AFP is unable to provide the specific divisions of Acts, relevant to the offence type. The figures for 2019/20 have been manually counted against the categories. The final count will be published in the Home Affairs TIA Act Annual Report 2019.20.

Offence	2017/18	2018/2019	2019/2020
Abduction, offences against the person	100	64	17
Acts intended to cause injury	6	17	14
Bribery or Corruption	19	28	2
Cartel offences	24	0	0
Conspire/ Aid & Abet serious offence	4	27	12
Cybercrime & Telecommunications offences	132	154	93
Dangerous/ negligent Acts Endangering Person	66	2	1
Dealing in Firearms/Armaments	1		
Family Violence	2		
Fraud, Deception & Related Offences	138	191	119
Homicide & Related Offences	64	46	48
Illicit Drug Offences	2218	2343	2008
Loss of Life	5	5	7
Miscellaneous Offences	37	20	22
Offences/Justice/Govt Security & Procedures	123	104	26
Pecuniary Penalty offences	1	0	3
Organised Offences/ Criminal Orgs	386	1228	662
People Smuggling	26	35	22
Property Damage & Environment Pollution	10	20	1
Protecting Public Revenue	2		
Regulated Weapons & Explosive Offences	61	74	46
Robbery. Extortion & Related Offences	62	50	67
Serious Damage to Property	1	2	1
Sexual Assault Against the Person	31	75	69
Terrorism Offences	109	72	82
Theft & Related Offences	35	97	58
Traffic & regulatory Offences	6	2	2
Unlawful Entry with Intent/ Burglary	30	47	21
Murder or equivalent	0	1	0
Public Order Offences	0	1	0

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

Not applicable.

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

In 2017/18, 23 individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 25 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 25 occasions in this period.

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

In 2018/19, 16 individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 25 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 25 occasions in this period.

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

In 2017/18, 14 individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 50 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 50 occasions in this period.

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

In 2018/19, nine individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 50 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 50 occasions in this period.

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

In 2017/18, eight individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 100 occasions. Due to

reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 100 occasions in this period.

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

In 2018/19, five individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 100 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 100 occasions in this period.

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

In 2017/18, two individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 250 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 250 occasions in this period.

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

In 2018/19, three individual officers (substantive authorised officers) exercised their power to authorise the release of prospective telecommunications data on more than 250 occasions. Due to reporting limitations with AFP systems, the AFP is unable to determine if any authorised officers (performing higher duties at the rank of Superintendent) authorised the release of prospective data on more than 250 occasions in this period.

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

Unknown, the AFP only records authorisations that are made.

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

Unknown, the AFP only records authorisations that are made.

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?**

Unknown, the AFP only records authorisations that are made.

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 level of initial knowledge or involvement of an authorising officer varies. For example, an authorising officer can be involved in real-time aspects of an investigation and have extensive knowledge of the case and be aware of the target entities and the usefulness and purpose of requesting prospective telecommunications data.

At the other end of the spectrum, if the authorising officer has limited or no prior knowledge of the case they may request additional background information, for example, a briefing, to satisfy the thresholds of making an authorisation.

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

The requesting officer identifies the need to access prospective telecommunications data and completes an electronic request form. The request form is designed to capture the request types specific to each carrier, as well as meet the authorising officer considerations, reason for request and reporting requirements.

The request is emailed to the authorising officer for approval or rejection. The authorising officer may seek additional information from the requesting officer, if required.

If approved, the request is emailed by the authorising officer to the Digital Surveillance Support Team, responsible for sending the request to the carrier as well as maintaining a record of the authorisation, request and result.

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 AFP's data retention request management system does not capture the length of time an authorising officer spends considering the request. The time spent would vary to accord with the level of initial knowledge or involvement an authorising officer has in relation to a request to access telecommunications data.

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?**

As 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?**

As above.

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?**

As 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?**

As above.

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.**

The prompts and wording in the request form serves as a consistent approach for all requesting and authorising officers when considering and making an authorisation. The authorising officer must be satisfied that the disclosure is reasonably necessary for the investigation of a serious offence that is punishable by imprisonment for at least three years, with a section for the authorising officer to make supporting comments and privacy considerations for granting the request.

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.**

No.

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.**

No.

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?**

Unknown.

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

Unknown.

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

Unknown.

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

Unknown.

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?**

Unknown.

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?**

Unknown.

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?**

Unknown.

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

Unknown.

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

Unknown. (Note, the AFP has amended the question above in good faith based on our understanding of the intent of questions 65 – 78 inclusive.)

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

Unknown.

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?**

Unknown.

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?**

Unknown.

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.**

No, all historic and prospective telecommunications data received by the AFP is routinely retained, except where there is a legislative requirement to delete the data. If data is received that is outside the scope of the authorisation, steps are taken to quarantine the data.

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?**

All telecommunications data received by the AFP is routinely retained, except where there is a legislative requirement to destroy the data. . If data is received that is outside the scope of the authorisation, steps are taken to quarantine the data.

Attachment A

Offence Type	Example	Description	Penalty
Abduction, harassment and other offences against the person	Section 474.17 Criminal Code Act 1995	Using a carriage service to menace, harass or cause offence	Imprisonment for 3 years.
Acts intended to cause injury	Section 115.4 of the Criminal Code Act 1995	Recklessly causing serious harm to an Australian citizen or a resident of Australia	Imprisonment for 15 years.
Bribery or corruption	Section 141.1(3) of the Criminal Code Act 1995	Bribery of a Commonwealth public official	Imprisonment for not more than 10 years, a fine not more than 10,000 penalty units, or both.
Cartel offences	Sections 44ZZRF, 44ZZRG, 79 of the Competition and Consumer Act 2010	Making a contract etc. containing a cartel provision	Fine not exceeding $10,000,000.
Conspire/aid/abet serious offence	Section 135.4 by virtue section 11.5 of the Criminal Code Act 1995	Conspiracy to defraud	Imprisonment for 10 years.
Cybercrime and telecommunications offences	Section 477.2 of the Criminal Code Act 1995	Unauthorised modification of data to cause impairment	Imprisonment for 10 years.
Dangerous or negligent acts endangering persons	Section 80.2A of the Criminal Code Act 1995	Urging violence against groups	Imprisonment for 7 years.
Fraud, deception and related offences	Section 134.2 of the Criminal Code Act 1995	Obtaining a financial advantage by deception	Imprisonment for 10 years.
Homicide and related offences	Section 268.70 of the Criminal Code Act 1995	War crime—murder	Imprisonment for life.
Illicit drug offences	Section 307.1 of the Criminal Code Act 1995	Importing and exporting commercial quantities of border controlled drugs or border controlled plants	Imprisonment for life or 7,500 penalty units, or both.
Loss of life	Section 474.15 of the Criminal Code Act 1995	Using a carriage service to make a threat (threat to kill)	Imprisonment for 10 years.
Miscellaneous offences	Section 10(a) of the Crimes (Currency) Act 1981	Import and export of counterfeit money or counterfeit securities	Imprisonment for 12 years.
Offences against justice procedures, government security and government operations	Section 42 of the Crimes Act 1914	Conspiracy to defeat justice	Imprisonment for 10 years.
Organised offences and/or criminal organisations	Section 400.3 of the Criminal Code Act 1995	Dealing in proceeds of crime etc.—money or property worth $1,000,000 or more	Imprisonment for 25 years, or 1500 penalty units, or both.
Other offences relating to the enforcement of a law imposing a pecuniary penalty	Sections 18 and 19 of the Proceeds of Crime Act 2002	People suspected of committing serious offences	Restraining orders
Other offences relating to the enforcement of a law protecting the public revenue	Section 400.9 of the Criminal Code Act 1995	Dealing with property reasonably suspected of being proceeds of crime etc.	Imprisonment for 3 years, or 180 penalty units, or both.
People smuggling, and related	Section 73.3 of the Criminal Code Act 1995	Aggravated offence of people smuggling (at least 5 people)	Imprisonment for 20 years or 2,000 penalty units, or both.
Prohibited and regulated weapons and explosives offences	Section 361.2 of the Criminal Code Act 1995	Trafficking prohibited firearms or firearm parts into Australia	Imprisonment for 10 years or a fine of 2,500 penalty units, or both.
Property damage and environment pollution	Section 186.1 of the Biosecurity Act 2015	Contravening conditions applying to conditionally non-prohibited goods brought or imported into Australian territory	Imprisonment for 5 years or 300 penalty units, or both.
Public order offences	Section 67 of the Criminal Code Compilation Act 1913 (WA)	Rioters causing damage	Imprisonment for 10 years.
Robbery, extortion and related offences	Section 249K(2) of the Crimes Act 1900 (NSW)	Blackmail offence	Imprisonment for 14 years.
Serious damage to property	Section 117 of the Crimes Act 1900 (NSW)	Punishment for larceny	Imprisonment for 5 years.
Sexual assault and related offences	Section 474.22 of the Criminal Code Act 1995	Using a carriage service for child abuse material	Imprisonment for 15 years.
Terrorism offences	Section 102.3 of the Criminal Code Act 1995	Membership of a terrorist organisation	Imprisonment for 10 years.
Theft and related offences	Section 400.4 of the Criminal Code Act 1995	Dealing in proceeds of crime etc.—money or property worth $100,000 or more	Imprisonment for 20 years, or 1200 penalty units, or both.
Traffic and vehicle regulatory offences	Section 63(1)(a) of the Road Traffic Act 1974 (WA)	Driving under the influence of alcohol etc.	Fine of not less than 18 or more than 50 penalty units.
Unlawful entry with intent/burglary, break and enter	Section 312 of the Criminal Code 2002 (ACT)	Aggravated burglary	Imprisonment for 20 years or 2,000 penalty units, or both.