Australian Government
Department of Human Services

Malisa Golightly
Deputy Secretary

Katherine Jones
Deputy Secretary
National Security and Criminal Justice Group
Attorney-General's Department
BARTON ACT 2600

Dear Ms Jones

s 22(1)

Enforcement agency access to telecommunications data

Thank you for your letter of 22 May 2015 to Ms Kathryn Campbell, Secretary of the Department of Human Services, in relation to changes to the *Telecommunications (Interception and Access) Act 1979* affecting access to historical telecommunication data by this department. The Secretary has asked me to respond on her behalf.

The Department of Human Services (the Department) is seeking endorsement from the Attorney-General for the Department of Human Services to be recognised as an 'enforcement agency' under Section 176A of the Data Retention Act.

Our understanding is that if the department is not recognised as a law enforcement agency, the department will lose access to certain telecommunication data from 13 October 2015. The department requires access to this data to protect Government outlays. This is a key priority for the Government which has been recognised through the 2015 Budget measure to strengthen the integrity of the welfare system which will produce approximately $1.7 billion in revenue over the next four years. The proposed removal of access will put the effective implementation of this measure at some risk.

Please find at Attachment A, a submission detailing our case for continued access to telecommunication data and our requirements for inclusion as an 'enforcement agency'.

If you have any questions or would like to discuss this matter further, Mark Withnell, General Manager, Business Integrity Division, can be contacted on s 47E(d)

Yours sincerely

s 47F(1)

Malisa Golightly

17 June 2015

PO Box 7788, Canberra Business Centre ACT 2610 • Telephone (02) 6223 4411 • Facsimile (02) 6223 4489
Internet www.humanservices.gov.au

ATTACHMENT A

Australian Government
Department of Human Services

THE DEPARTMENT OF HUMAN SERVICES' REQUIREMENT FOR CONTINUED ACCESS TO TELECOMMUNICATIONS DATA

Recommendation

That the Attorney-General declare the Department of Human Services (the department) an '*enforcement agency*' for the purposes of Section 110A of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

Overview of submission

1. The department wishes to thank the Attorney-General's Department for inviting us to provide advice about the department's requirement for direct access to telecommunications data.
2. The department understands that if the Attorney-General does not prescribe the department as an 'enforcement agency' that it will lose its ability to access relevant telecommunications data from 13 October 2015.
3. The department has a clear need for continued access to certain telecommunications data. This is required in the context of the department's enforcement functions which act to protect the integrity of the social, health and welfare systems against the risk of fraud and other forms of criminal exploitation.
4. The department's criminal law enforcement function employs approximately 295 investigators and approximately 89 intelligence analysts. Typically, the department conducts approximately 3,000 criminal investigations each year. This leads to the referral of approximately 1,300 briefs of evidence to the Commonwealth Director of Public Prosecutions (CDPP) each year. The vast majority of these matters are prosecuted with offences under the *Criminal Code Act 1995* or the *Crimes Act 1914.*
5. In 2013-14 the department made 334 requests for telecommunications data for 106 unique customer records which resulted in 20 referrals to the Commonwealth Director of Public Prosecutions (CDPP), 8 cases that resulted in warrants and 8 cases which are still being investigated.
6. The department has a strong framework in place to protect the confidentiality of customers. The department complies with all Australian Privacy Principles, with controls embedded within the department's systems. There are strong penalties for those who breach privacy and understanding responsibilities with regard to privacy of customer information is a key component of training given to all departmental staff. The relevant enforcement teams within the department have additional controls related to sensitive information obtained during investigations.

Enforcement of Criminal Law

7. In accordance with Section 176A subsection (a) of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* the Attorney-General may declare a body or authority to be an enforcement agency if satisfied on reasonable grounds that its functions include enforcement of the criminal law.
8. The department has a long history of enforcing criminal law. Criminal investigations and prosecution activities have been a key activity for this department and its former agencies since at least the 1980's and continues to this day...
9. Between 2011-12 and 2013-14, the department investigated 8,905 criminal matters and referred 3,471 matters to the Commonwealth Director of Public Prosecutions (CDPP). The department consistently refers more cases to the CDPP than any other Commonwealth Agency on an annual basis.
10. The department's criminal law enforcement function currently employs approximately 295 investigators and approximately 89 intelligence analysts. These individuals maintain appropriate security clearances to undertake this work. Investigators are trained to comply with Australian

Government Investigation Standards and decision making is subject to a high degree of senior managerial oversight.

11. The department's fraud intelligence and investigation functions currently benefit from having direct access to telecommunications data provided under the *Telecommunications (Interception and Access) Act 1979*. The department has had direct access to this data since at least 2009.
    - In 2013-14, the department made 334 requests for telecommunication data for 106 unique customer records for the purposes of detecting or investigating fraud.
    - In 2013-14 these requests assisted the department in making 20 separate referrals to the CDPP for prosecution. The vast majority of these matters were charged with either summary or indictable offences under the *Criminal Code Act 1995* or *Crimes Act 1914*.
    - Under provisions of Section 186 of the *Telecommunications (Interception and Access) Act 1979*, the head of the department has reported annual usage of accessed telecommunication data to the Attorney-General since 2009.
12. The types of telecommunications data required by the department consists of search requests through Telstra's Integrated Public Number Database (IPND) including the ability to obtain:
    - subscriber details linked to a specific phone number and the history of subscribers
    - the phone number of a known subscriber
    - the address relating to a specific phone number.
13. The department's requests to the IPND allow for the identification of phone subscribers who would otherwise remain unknown.
14. This data is used to detect and investigate fraud matters across Welfare , Health and Child Support programs including:
    - identity frauds
    - people who receive payments as a single person while in a marriage like relationship
    - fraudulent claims for disaster recovery payments.
15. The department's requirements do not include the content of telecommunications or the power to obtain or execute warrants to intercept telecommunications.
16. The department has close links to the law enforcement community. We are a member of the Heads of Commonwealth Government Operational Law Enforcement Agencies (HOCOLEA) and makes regular contributions to discussion papers and official requests related to government efforts to combat organised crime. The department is a member of the Australian Crime Commission's Fusion Centre on Organised Crime, the AFP's Fraud & Anti-Corruption Centre and is also represented on the National Disruption Group focusing on counter terrorism activities. Defining the department as an 'enforcement agency' for the purposes of accessing telecommunications data would be consistent with this activity.

Protecting Public Revenue

17. In accordance with Section 176A subsection (c) of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* the Attorney-General may declare a body or authority to be an enforcement agency if satisfied on reasonable grounds that its functions include administering a law relating to the protection of the public revenue.
18. The department has a significant role in protecting public revenue.
    - In 2013-14 we distributed $159.2 billion to customers and providers.
    - In 2013-14, the department identified approximately $2.2 billion in overpayments and recovered revenue of approximately $1.2 billion through debt recovery processes.

- Approximately $76 million in overpayments was as a result of criminal activity identified through fraud investigations including $80,000 associated with fraudulently claimed disaster recovery payments.

Privacy considerations

19. The department complies with all Australian Privacy Principles. The department considers the privacy and confidentially of personal data to be a fundamental part of the department's obligations.

20. Access and use of telecommunications data supplied to the department would be restricted to the purposes for which it is obtained. It is currently a criminal offence under social security and family assistance law for a person to breach secrecy provisions.

21. Access to the department's IT systems is strictly controlled and any access requires appropriate authorisation. This includes logon identification codes, passwords and security groupings to ensure that access to information in on a needs-only basis. All access to personal information is monitored and recorded. Information control plans are put in place to manage the security of data outside of the main systems.

Public interest elements

22. There is a clear public interest in ensuring agencies have the capability to cooperate to prevent, detect and disrupt criminal activities as well as ensuring that public revenue is used for the purpose for which is intended

23. The 2015-16 Budget Measure – *Strengthening the integrity of welfare payments* will target high risk geographic clusters of fraud risk through data analytics and geospatial capability. This will be a highly visible initiative implemented in cooperation with the AFP that will include investigative as well as general compliance activities. If the department was not able to access telecommunications data from 13 October 2015, this may jeopardise the successful implementation of this measure.

s 22(1)

From: s 22(1)
Sent: Wednesday, 17 June 2015 5:00 pm
To: Jones, Katherine
Cc: Withnell, Mark; Golightly, Malisa
Subject: FW: Enforcement agency access to telecommunications data [SEC=UNCLASSIFIED]
Attachments: Replacement cover letter - Katherine Jones - Enforcement agency access to telecommunications data.pdf

Good afternoon,
Please find attached replacement cover letter for correspondence sent at 9.08am this morning. Please note the content is exactly the same, it is only the letterhead which has been changed.
Regards

s 22(1)
Executive Officer to the Deputy Secretary, Participation, Aged Care, Service Strategy and Integrity
Department of Human Services
P s 22(1)

humanservices.gov.au | Medicare | Centrelink | Child Support | CRS Australia

---

From: s 22(1)
Sent: Wednesday, 17 June 2015 9:08 AM
To: 'Katherine.Jones@ag.gov.au'
Cc: Withnell, Mark; Golightly, Malisa
Subject: Enforcement agency access to telecommunications data [SEC=UNCLASSIFIED]

Good morning
Please find attached correspondence in relation to the above matter.

Many thanks

s 22(1)
Executive Assistant to Malisa Golightly
Deputy Secretary - Participation, Aged Care, Service Strategy and Integrity Group
Department of Human Services
Address: Level 5 South – Executive – Caroline Chisholm Building
PO Box 7788, Canberra BC, ACT, 2610
Phone: s 22(1)
Mobile: s 22(1)
s 22(1)

Australian Government
Department of Human Services

Katherine Jones
Deputy Secretary
National Security and Criminal Justice Group
Attorney-General's Department
BARTON ACT 2600

Dear Ms Jones

Enforcement agency access to telecommunications data

Thank you for your letter of 22 May 2015 to Ms Kathryn Campbell, Secretary of the Department of Human Services, in relation to changes to the *Telecommunications (Interception and Access) Act 1979* affecting access to historical telecommunication data by this department. The Secretary has asked me to respond on her behalf.

The Department of Human Services (the Department) is seeking endorsement from the Attorney-General for the Department of Human Services to be recognised as an 'enforcement agency' under Section 176A of the Data Retention Act.

Our understanding is that if the department is not recognised as a law enforcement agency, the department will lose access to certain telecommunication data from 13 October 2015. The department requires access to this data to protect Government outlays. This is a key priority for the Government which has been recognised through the 2015 Budget measure to strengthen the integrity of the welfare system which will produce approximately $1.7 billion in revenue over the next four years. The proposed removal of access will put the effective implementation of this measure at some risk.

Please find at Attachment A, a submission detailing our case for continued access to telecommunication data and our requirements for inclusion as an 'enforcement agency'.

If you have any questions or would like to discuss this matter further, Mark Withnell, General Manager, Business Integrity Division, can be contacted on s 47E(d).

Yours sincerely

s 47F(1)

Malisa Golightly PSM
Deputy Secretary

17 June 2015

PO Box 7788 Canberra Business Centre ACT 2610 Ph (02) 6143 7299
Internet: www.humanservices.gov.au

humanservices.gov.au

E-MAILED
17/6/15

Australian Government
Department of Human Services

RECEIVED
22 JUN 2015
Deputy Secretary
NSCJ

14-JL 23/6

Katherine Jones
Deputy Secretary
National Security and Criminal Justice Group
Attorney-General's Department
BARTON ACT 2600

Dear Ms Jones

Enforcement agency access to telecommunications data

→ Anna Harmer
→ s 22(1)

Thank you for your letter of 22 May 2015 to Ms Kathryn Campbell, Secretary of the Department of Human Services, in relation to changes to the *Telecommunications (Interception and Access) Act 1979* affecting access to historical telecommunication data by this department. The Secretary has asked me to respond on her behalf.

The Department of Human Services (the Department) is seeking endorsement from the Attorney-General for the Department of Human Services to be recognised as an 'enforcement agency' under Section 176A of the Data Retention Act.

Our understanding is that if the department is not recognised as a law enforcement agency, the department will lose access to certain telecommunication data from 13 October 2015. The department requires access to this data to protect Government outlays. This is a key priority for the Government which has been recognised through the 2015 Budget measure to strengthen the integrity of the welfare system which will produce approximately $1.7 billion in revenue over the next four years. The proposed removal of access will put the effective implementation of this measure at some risk.

Please find at Attachment A, a submission detailing our case for continued access to telecommunication data and our requirements for inclusion as an 'enforcement agency'.

If you have any questions or would like to discuss this matter further, Mark Withnell, General Manager, Business Integrity Division, can be contacted on (02) 6133 0966.

Yours sincerely

s 47F(1)

Malisa Golightly PSM
Deputy Secretary

17 June 2015

Australian Government
Department of Human Services

ATTACHMENT A

THE DEPARTMENT OF HUMAN SERVICES' REQUIREMENT FOR CONTINUED ACCESS TO TELECOMMUNICATIONS DATA

Recommendation

That the Attorney-General declare the Department of Human Services (the department) an '*enforcement agency*' for the purposes of Section 110A of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*.

Overview of submission

1. The department wishes to thank the Attorney-General's Department for inviting us to provide advice about the department's requirement for direct access to telecommunications data.
2. The department understands that if the Attorney-General does not prescribe the department as an 'enforcement agency' that it will lose its ability to access relevant telecommunications data from 13 October 2015.
3. The department has a clear need for continued access to certain telecommunications data. This is required in the context of the department's enforcement functions which act to protect the integrity of the social, health and welfare systems against the risk of fraud and other forms of criminal exploitation.
4. The department's criminal law enforcement function employs approximately 295 investigators and approximately 89 intelligence analysts. Typically, the department conducts approximately 3,000 criminal investigations each year. This leads to the referral of approximately 1,300 briefs of evidence to the Commonwealth Director of Public Prosecutions (CDPP) each year. The vast majority of these matters are prosecuted with offences under the *Criminal Code Act 1995* or the *Crimes Act 1914*.
5. In 2013-14 the department made 334 requests for telecommunications data for 106 unique customer records which resulted in 20 referrals to the Commonwealth Director of Public Prosecutions (CDPP), 8 cases that resulted in warrants and 8 cases which are still being investigated.
6. The department has a strong framework in place to protect the confidentiality of customers. The department complies with all Australian Privacy Principles, with controls embedded within the department's systems. There are strong penalties for those who breach privacy and understanding responsibilities with regard to privacy of customer information is a key component of training given to all departmental staff. The relevant enforcement teams within the department have additional controls related to sensitive information obtained during investigations.

Enforcement of Criminal Law

7. In accordance with Section 176A subsection (a) of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* the Attorney-General may declare a body or authority to be an enforcement agency if satisfied on reasonable grounds that its functions include enforcement of the criminal law.
8. The department has a long history of enforcing criminal law. Criminal investigations and prosecution activities have been a key activity for this department and its former agencies since at least the 1980's and continues to this day...
9. Between 2011-12 and 2013-14, the department investigated 8,905 criminal matters and referred 3,471 matters to the Commonwealth Director of Public Prosecutions (CDPP). The department consistently refers more cases to the CDPP than any other Commonwealth Agency on an annual basis.
10. The department's criminal law enforcement function currently employs approximately 295 investigators and approximately 89 intelligence analysts. These individuals maintain appropriate security clearances to undertake this work. Investigators are trained to comply with Australian

Government Investigation Standards and decision making is subject to a high degree of senior managerial oversight.

11. The department's fraud intelligence and investigation functions currently benefit from having direct access to telecommunications data provided under the *Telecommunications (Interception and Access) Act 1979*. The department has had direct access to this data since at least 2009.

    - In 2013-14, the department made 334 requests for telecommunication data for 106 unique customer records for the purposes of detecting or investigating fraud.
    - In 2013-14 these requests assisted the department in making 20 separate referrals to the CDPP for prosecution. The vast majority of these matters were charged with either summary or indictable offences under the *Criminal Code Act 1995* or *Crimes Act 1914*.
    - Under provisions of Section 186 of the *Telecommunications (Interception and Access) Act 1979*, the head of the department has reported annual usage of accessed telecommunication data to the Attorney-General since 2009.

12. The types of telecommunications data required by the department consists of search requests through Telstra's Integrated Public Number Database (IPND) including the ability to obtain:

    - subscriber details linked to a specific phone number and the history of subscribers
    - the phone number of a known subscriber
    - the address relating to a specific phone number.

13. The department's requests to the IPND allow for the identification of phone subscribers who would otherwise remain unknown.

14. This data is used to detect and investigate fraud matters across Welfare , Health and Child Support programs including:

    - identity frauds
    - people who receive payments as a single person while in a marriage like relationship
    - fraudulent claims for disaster recovery payments.

15. The department's requirements do not include the content of telecommunications or the power to obtain or execute warrants to intercept telecommunications.

16. The department has close links to the law enforcement community. We are a member of the Heads of Commonwealth Government Operational Law Enforcement Agencies (HOCOLEA) and makes regular contributions to discussion papers and official requests related to government efforts to combat organised crime. The department is a member of the Australian Crime Commission's Fusion Centre on Organised Crime, the AFP's Fraud & Anti-Corruption Centre and is also represented on the National Disruption Group focusing on counter terrorism activities. Defining the department as an 'enforcement agency' for the purposes of accessing telecommunications data would be consistent with this activity.

Protecting Public Revenue

17. In accordance with Section 176A subsection (c) of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* the Attorney-General may declare a body or authority to be an enforcement agency if satisfied on reasonable grounds that its functions include administering a law relating to the protection of the public revenue.

18. The department has a significant role in protecting public revenue.

    - In 2013-14 we distributed $159.2 billion to customers and providers.
    - In 2013-14, the department identified approximately $2.2 billion in overpayments and recovered revenue of approximately $1.2 billion through debt recovery processes.

- Approximately $76 million in overpayments was as a result of criminal activity identified through fraud investigations including $80,000 associated with fraudulently claimed disaster recovery payments.

Privacy considerations

19. The department complies with all Australian Privacy Principles. The department considers the privacy and confidentially of personal data to be a fundamental part of the department's obligations.

20. Access and use of telecommunications data supplied to the department would be restricted to the purposes for which it is obtained. It is currently a criminal offence under social security and family assistance law for a person to breach secrecy provisions.

21. Access to the department's IT systems is strictly controlled and any access requires appropriate authorisation. This includes logon identification codes, passwords and security groupings to ensure that access to information in on a needs-only basis. All access to personal information is monitored and recorded. Information control plans are put in place to manage the security of data outside of the main systems.

Public interest elements

22. There is a clear public interest in ensuring agencies have the capability to cooperate to prevent, detect and disrupt criminal activities as well as ensuring that public revenue is used for the purpose for which is intended

23. The 2015-16 Budget Measure – *Strengthening the integrity of welfare payments* will target high risk geographic clusters of fraud risk through data analytics and geospatial capability. This will be a highly visible initiative implemented in cooperation with the AFP that will include investigative as well as general compliance activities. If the department was not able to access telecommunications data from 13 October 2015, this may jeopardise the successful implementation of this measure.

From: s 22(1) on behalf of s 47E(d)
To: ESPB
Cc: s 22(1)
Subject: FW: Applications for ongoing access to telecommunications data - Department of Human Services [DLM=For-Official-Use-Only]
Date: Thursday, 3 September 2015 2:47:39 PM
Attachments: image001.jpg

Good afternoon s 22(1)

I have been requested by Karl Marjoribanks (a/g National Manager, Serious Non-compliance Branch, Business Integrity Division, DHS) to seek an update regarding our application for ongoing access to telecommunications data.

To-date we have not received advice as to whether our application was successful. We would appreciate any information that you are able to provide regarding our application.

Kind regards
s 22(1)

Coordination – Business Support | Serious Non-compliance Branch
Business Integrity Division | Department of Human Services
E: s 47E(d)
Louisa Lawson Building | 25 Cowlishaw St Greenway ACT 2900

s 22(1)

From: ESPB [mailto:ESPB@ag.gov.au]
Sent: Wednesday, 1 July 2015 3:01 PM
To: Withnell, Mark
Subject: Applications for ongoing access to telecommunications data - Department of Human Services [DLM=For-Official-Use-Only]

For Official Use Only

Dear Mark

Following up a call with s 22(1), I am sending an email regarding AGDs assessment of the Department of Human Services' (DHS) application to obtain ongoing access to telecommunications data.

I would be grateful if you would provide responses to the questions below so AGD can progress the application.

I understand that DHS administers the offences under the Criminal Code Act 1995 and the Crimes Act 1914. Grateful if you would provide further details in relation to:

- Specific penalties imposed by the legislation
- The role of telecommunications data in enforcing the legislation (if possible, include case studies)
- Whether DHS has alternative methods to progress the investigation instead of accessing telecommunications data

If DHS obtains ongoing access to telecommunications data, it will be subject to additional record-keeping and oversight requirements. Further information about these requirements can be found here. Please provide an undertaking that the DHS is aware of these requirements and intends to comply with them. We ask that such an undertaking be made by an individual who has the authority to bind the Department of Health.

Thank you for your assistance in this matter, I would appreciate if you would provide your response by **COB Thursday 2 July 2015.** Do not hesitate to contact me if you wish to discuss your application further.

Kind regards

s 22(1) **| Legal Officer**
Electronic Surveillance Policy Branch
Attorney-General's Department |3-5 National Circuit |Barton ACT 2600
✉ s 22(1) | ☎ s 22(1)

From: ESPB
To: s 22(1)
Cc: ESPB
Subject: Enforcement agency access to telecommunications data - DHS [DLM=For-Official-Use-Only]
Date: Wednesday, 14 October 2015 3:04:28 PM
Attachments: image001.jpg

For Official Use Only

Dear s 22(1)

Thank you for your call this afternoon in relation to the Department of Human Service's interest in being temporarily declared as an enforcement agency following the enactment of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

As discussed, the Attorney-General has not yet determined to make any temporary declarations at this time, including in relation to your agency. Consequently, from 13 October 2015, only those criminal law-enforcement agencies specifically listed in section 110A of the Act will be able to directly access historical telecommunications data. We continue to work with the Attorney on the range of issues raised by affected agencies, and will update you on any developments.

You may wish to consider alternative means of accessing historical telecommunications data. This could include joint investigation arrangements with a criminal law-enforcement agency. You may wish to contact an appropriate criminal law-enforcement agency to determine whether that is feasible. You may also wish to obtain legal advice about whether your agency could access telecommunications data under section 280 of the *Telecommunications Act 1997.*

Please do not hesitate to contact s 22(1) on s 22(1) or myself if you have any further questions about this matter.

Kind regards,

s 22(1)

s 22(1) **| Legal Officer**
Electronic Surveillance Policy Branch
Attorney-General's Department |3-5 National Circuit |Barton ACT 2600
✉ s 22(1) | ☎ s 22(1)

From: s 22(1)
Bcc: s 22(1) ;s 22(1) ; s 47E(d) ;s 22(1) ; s 22(1)
Subject: FW: Enforcement agency access to telecommunications data [SEC=UNCLASSIFIED]
Date: Thursday, 24 March 2016 4:38:07 PM
Importance: High
Sensitivity: Confidential

UNCLASSIFIED

From: ESPB
Sent: Thursday, 24 March 2016 4:36 PM
Subject: Enforcement agency access to telecommunications data [SEC=UNCLASSIFIED]
Importance: High
Sensitivity: Confidential

UNCLASSIFIED

Dear Colleagues

I am writing to update you on the status of your agency's submissions indicating an interest in obtaining direct access to metadata under the *Telecommunications (Interception and Access) Act 1979.* A letter in similar terms to this email (from Katherine Jones, the Deputy Secretary of the National Security and Emergency Management Group of the Attorney-General's Department) to the chief executive of your organisation is in the post.

The Attorney-General acknowledges agency concerns generally and will continue to consider applications to be included in the Act as an enforcement agency on a case by case basis. However, it is unlikely that any agencies will be added to the legislated list of specified enforcement agencies in the immediate term.

You may wish to consider how your agency might otherwise obtain the information it needs to undertake its functions. You could consider joint investigation arrangements with a criminal law-enforcement agency. Alternatively, the *Telecommunications Act 1997* may enable some agencies to obtain information where they have separate notice to produce powers.

If you require further assistance or would like to discuss this matter in more detail, please contact s 22(1) Director of the Electronic Surveillance Policy Section on s 22(1) or email s 22(1) .

Thank you again for writing in relation to this matter.

Kind regards

s 22(1) **| Legal Officer**
Communications Security Branch | Attorney-General's Department
s 22(1) | s 22(1)

From: ESPB
Sent: Tuesday, 26 May 2015 4:22 pm
To:
Subject: Enforcement agency access to telecommunications data [SEC=UNCLASSIFIED]

UNCLASSIFIED

Dear Colleagues,

I am writing to advise you about changes to the *Telecommunications (Interception and Access) Act 1979* that will affect your agency's ability to access to historical telecommunications data. A letter in similar terms to this email (from Katherine Jones, the Deputy Secretary of the National Security and Criminal Justice Group of the Attorney-General's Department) to the chief executive of your organisation is in the post.

Background

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* will come into effect on 13 October 2015. The data retention legislation will ensure that law enforcement and national security agencies will continue to have the information they need to keep the community safe. To better protect individual privacy, Parliament reduced the number of agencies that may access telecommunications data from around eighty to twenty-one.

Our records indicate that your agency has accessed telecommunications data under the *Telecommunications (Interception and Access) Act 1979* in the past. However, your agency is not included within the more limited access scheme commencing in October this year.

Next Steps

The legislative scheme reflects Parliament's intent that access to telecommunications data be limited to a small number of core agencies.

However, in the event you consider that your agency requires ongoing direct access to telecommunications data, please write to the Attorney-General's Department via

ESPB@ag.gov.au by **12 June 2015**. Your letter will need to make a compelling case for access and clearly demonstrate an ability to uphold the privacy safeguards embedded in the data retention scheme. In particular, section 176A of the Data Retention Act outlines a range of matters relevant to the possible inclusion of additional agencies on a temporary basis which should be addressed. I enclose a guidance document that may assist in considering whether your agency may be suitable for inclusion within the scheme in future. Your advice on these matters will assist the Department to advise the Attorney-General on appropriate access arrangements.

For further assistance please contact Anna Harmer, Assistant Secretary of the Electronic Surveillance Policy Branch on s 47E(d) or s 22(1), Director of the Electronic Surveillance Policy and Advice Section on s 22(1).

Kind regards

s 22(1) **Legal Officer**
Electronic Surveillance Policy and Advice
Attorney-General's Department |3-5 National Circuit |Barton ACT 2600
✉ s 22(1) | ☎ s 22(1)

From: s 22(1)
To: s 22(1)
Cc: s 22(1) s 22(1) s 22(1)
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]
Date: Monday, 28 February 2022 2:23:52 PM
Attachments: image001.jpg
image002.jpg

OFFICIAL

Hi s 22(1)

Much appreciated – looking forward to our discussion tomorrow.

Many thanks,
s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

From: s 22(1) <s 22(1)>
Sent: Friday, 25 February 2022 3:07 PM
To: s 22(1) s 22(1)
Cc: s 22(1) ; s 22(1) ; s 22(1)
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

Hi s 22(1)

The approvals to release the above draft submission have not been provided in full. However, I have permission to share the draft report for the purpose of facilitating a conversation next week.

A final report is forthcoming, however the key points are unlikely to change. Please note that the draft still requires SES approval and is not for publication, however provides a understanding of our operating environment.

Thanks

s 22(1) Assistant Director

Phone s 22(1)
Operational Policy Team
Operational Planning and Coordination / Intelligence and Investigation Branch
FRAUD CONTROL AND INVESTIGATIONS DIVISION
cid:image004.jpg@01D76682.23F0E350
s 22(1)

From: s 22(1)
Sent: Thursday, 17 February 2022 12:25 PM
To: s 22(1) >
Cc: s 22(1) ; s 22(1) >; s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

Hi s 22(1)

Thank you for the response.

We would definitely welcome the opportunity to discuss the request for telecommunication powers with your team.

For the Working Group please include s 22(1) , Director, Operational Planning and Coordination.
Email: s 22(1)
Phone: s 22(1)

Anthony Seebach (General Manager) and Craig Palmer (National Manager) Fraud Control and Investigations would both love to discuss telecommunications reform and a request for access to powers with Ashleigh McDonald.

The easiest way to arrange a time is through their exec assistant s 22(1) at s 22(1)

s 22(1) Assistant Director
Phone s 22(1)
Operational Policy Team
Operational Planning and Coordination / Intelligence and Investigation Branch
FRAUD CONTROL AND INVESTIGATIONS DIVISION
cid:image004.jpg@01D76682.23F0E350
s 22(1)

From: s 22(1) >
Sent: Thursday, 17 February 2022 11:46 AM
To: s 22(1) >
Cc: s 22(1) >; s 22(1) >; s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

OFFICIAL

Hi s 22(1)

Thank you for sending this through, much appreciated.

Our team would love to start a discussion with yourself and colleagues to discuss your thoughts on the submission and request for access to powers in more detail. We can then also run through the project and our current thoughts and deadlines. Let me know a time that would work for you, and we can send through a Webex meeting.

Given the ongoing working level discussions we are having with other Commonwealth agencies regarding policy decisions for the new electronic surveillance framework, we would also like to include Services Australia in the Working Group. If you could nominate the most appropriate points of contact from your agency that would like to be part of these discussions, that would be greatly appreciated. Other members attending the working group are typically around an EL2.

Additionally, if you are able to forward your SES1 contact's details, I will forward this to our SES1 (Ashleigh McDonald) so they can reach out.

As always, feel free to call if there are any further questions.

Many thanks!

s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

From: s 22(1) >
Sent: Monday, 14 February 2022 3:44 PM
To: s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

Hi s 22(1)

Thank you for the opportunity to provide a submission to the discussion paper on reforming Australia's electronic surveillance framework.
Services Australia delivers one of the largest criminal investigation capabilities in the Commonwealth, protecting over $230 billion in outlays and significant sensitive data holdings. We operate in a complex environment, impacted by a range of factors such as major emergency events including delivery of the Government's COVID-19 pandemic responses.

Opportunists exploit our social supports in a variety of ways with identity crime among the most prevalent crime impacting our agency. Services Australia has modernised service delivery and moved access to our services to online and telephony channels using personal identifying information. Identity fraud, in particular identity takeover, has wide reaching impacts on the victims in the wider community can be severe and long lasting.

s 37(2)(b)

s 37(2)(b)

Thank you

s 22(1) , Assistant Director
Phone s 22(1)
Operational Policy Team
Operational Planning and Coordination / Intelligence and Investigation Branch
FRAUD CONTROL AND INVESTIGATIONS DIVISION
cid:image004.jpg@01D76682.23F0E350
s 22(1)

From: s 22(1) >
Sent: Tuesday, 8 February 2022 9:56 AM
To: s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

OFFICIAL

Hi s 22(1)

Just following up on this email I sent last week.

Do not hesitate to call if you need! I can't seem to reach your phone in our signature block (unsure whether its due to the WFH situation?).

Many thanks,

s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

From: s 22(1)
Sent: Thursday, 3 February 2022 4:10 PM
To: s 22(1) >
Cc: s 22(1) >; s 22(1) >; s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

OFFICIAL

Hi s 22(1)

I just tried giving you a call but couldn't get through.

Thank you for your call earlier, and appreciate the notice that Services Australia's submission will arrive in our hands a week or two after the submission date due pandemic response priorities and the clearance process.

Noting that your submission will come in after the deadline, we would be keen to get a read out about the kinds of issues that Services Australia are likely to canvas so we can start considering them in our policy development.

If you could provide some insight into the key issues that will be the submission, that would be greatly appreciated – and please feel free to reach out if any questions arise!

Many thanks,

s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

From: s 22(1) >
Sent: Thursday, 3 February 2022 1:08 PM
To: s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

Hi s 22(1)

Are you available to have a quick discussion this week.

At this stage our branch is interested in seeking enforcement agency status, and will be seeking support from the Secretary to put a submission through to you.

In the interim I am preparing a response to the discussion paper.

If you are available I can give you a call.

s 22(1) , Assistant Director
Phone s 22(1))
Operational Policy Team
Operational Planning and Coordination / Intelligence and Investigation Branch
FRAUD CONTROL AND INVESTIGATIONS DIVISION
cid:image004.jpg@01D76682.23F0E350
s 22(1)

From: s 22(1) >
Sent: Wednesday, 15 December 2021 9:05 AM
To: s 22(1) >
Cc: s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

OFFICIAL

HI s 22(1)

No worries. Thank you for the update.

Kind regards,
s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division

Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

From: s 22(1)
Sent: Tuesday, 14 December 2021 1:07 PM
To: s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

Hi s 22(1)

Thanks for the email and apologies for the late reply.

We have a new executive in the fraud space in Services Australia, and presently they are taking a brief period to assess whether an approach to be considered an enforcement agency is appropriate for us.

Hopefully I will be back to you this week, otherwise it will be the first week in the new year.

If you would like to discuss I am free this week.

s 22(1) , Assistant Director
Phone s 22(1)
Operational Policy Team
Operational Planning and Coordination / Intelligence and Investigation Branch
FRAUD CONTROL AND INVESTIGATIONS DIVISION

cid:image004.jpg@01D76682.23F0E350

s 22(1)

From: s 22(1) >
Sent: Tuesday, 7 December 2021 11:20 AM
To: s 22(1) >; s 22(1) >
Cc: s 22(1) >; s 22(1) >; s 22(1) >
Subject: RE: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

OFFICIAL

Good afternoon both,

I am just following up on this email, and whether Services Australia is still considering enforcement agency status under the Electronic Surveillance Reform.

Happy to discuss.

Thanks,
s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

From: s 22(1)
Sent: Wednesday, 15 September 2021 3:14 PM
To: s 22(1) >;
s 22(1) >
Cc: Chris GOWER <CHRIS.GOWERs 47E(d) >; s 22(1)
>; s 22(1)
>
Subject: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]

OFFICIAL

Good Afternoon s 22(1) ,

As part of the electronic surveillance reform, we are open to considering the need for agencies to have access to electronic surveillance powers beyond those recommended by the Comprehensive Review. In considering the need for powers it would be useful to get some further details and operational case studies to support Services Australia's position.

The key questions we are taking into account when considering whether an agency should have access to a particular power are as follows:

1. Does the agency need access to the particular electronic surveillance power to effectively perform its functions?
2. Are there other effective mechanisms the agency could use to obtain the information it needs?
3. Does the agency have appropriate privacy safeguards in place to deal with information received through electronic surveillance?
4. Does the agency have appropriate processes in place to allow it to comply with the law (e.g., secure systems to ensure information is only used for permitted purposes, mechanisms to identify when information is no longer required and should be destroyed, processes to meet record-keeping and reporting requirements etc.)?
5. Is it in the public interest for the agency to have these powers?
6. Are there any other matters weighing in favour of or against giving the agency these powers?

Additionally, providing particular examples/case studies for the above questions would greatly assist in our understanding and consideration.
Please do not hesitate to reach out to one of us if you have any questions.
Kind regards,

s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country - signature block graphic 2020

OFFICIAL

parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****
****

IMPORTANT: This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****
****

IMPORTANT: This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****
****

IMPORTANT: This e-mail is for the use of the intended recipient only and may contain information that is confidential, commercially valuable and/or subject to legal or parliamentary privilege. If you are not the intended recipient you are notified that any review, re-transmission, disclosure, dissemination or other use of, or taking of any action in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****

From: s 22(1)
To: s 22(1)
Cc: s 22(1) ; s 22(1) ; s 22(1)
Subject: Electronic surveillance reform - Questions to consider [SEC=OFFICIAL]
Attachments: image001.jpg
image002.jpg

OFFICIAL

Hi s 22(1)

As discussed on the phone, setting up a meeting to further discuss your agency's thoughts on the electronic surveillance reform and request for powers under the framework in more detail.

Let me know if the proposed time works for you and your colleagues.

Looking forward to the discussion.

Thanks,

s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

s 22(1)

From: s 22(1)
To: s 22(1)
Cc: s 22(1)
Subject: Offences in Services Australia"s criminal investigations [SEC=OFFICIAL]
Date: Tuesday, 1 March 2022 12:48:04 PM
Attachments: image001.jpg

Hi s 22(1)

The Agency conducts criminal investigations across all the programs we administer and offences are considered under a range of legislation including the Acts we administer and the *Criminal Code Act 1995*.

Our criminal investigations primarily consider offences relating to Part 7.3 *Criminal Code Act* , in particular Division 135 and 136 offences which include fraudulent conduct and false and misleading statements. Offences in these divisions have penalties ranging from 12 months to 10 years imprisonment. Generally speaking, it is irregular for the CDPP to charge under provisions of the legislation that we administer for identity related crimes.

For matters involving identity fraud, identity takeover and hijacking of payments, where telecommunications data is critical evidence, the offences considered are *Criminal Code* offences each carrying a penalty of 10 years imprisonment.

- Section 134.2(1) – Obtaining a financial advantage by deception
- Section 135.1 (1) – Obtaining a gain
- Section 135.1 (3) – Causing a loss
- Section 135.1 (5) – Causing a loss
- Section 145.1 (1) – Using a forged document
- Section 145.1 (3) – Using a forged document

Where we are investigating the actions of an individual in relation to fraud as a customer, other offences in Part 7.3 of *Criminal Code Act* are possibly more relevant and they carry lower penalties. For example, when investigating a customer misrepresenting their circumstances we may considered section 135.2 (2) Criminal Code which carries a 12 month penalty.

Happy to discuss of you want more information.

s 22(1) , Assistant Director
Phone s 22(1)
Operational Policy Team
Operational Planning and Coordination / Intelligence and Investigation Branch
FRAUD CONTROL AND INVESTIGATIONS DIVISION
cid:image004.jpg@01D76682.23F0E350
s 22(1)

in reliance upon, this information is prohibited and may result in severe penalties. If you have received this e-mail in error please notify the sender immediately and delete all electronic and hard copies of this transmission together with any attachments. Please consider the environment before printing this e-mail
****

From: s 22(1)
To: s 22(1) ; s 22(1)
Subject: FW: Services Australia Submission to ESR [SEC=OFFICIAL:Sensitive]
Date: Thursday, 21 April 2022 1:57:15 PM
Attachments: DRAFT - Services Australia response to Department of Home Affairs (002).pdf
image001.jpg

~~OFFICIAL: Sensitive~~

For your awareness.

s 22(1)
Policy Officer | Electronic Surveillance Reform Policy Section
Electronic Surveillance Reform Project Team | Electronic Surveillance and Law Enforcement Policy Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

Acknowledgement of Country Signature Block Graphic 2022

~~OFFICIAL: Sensitive~~

From: s 22(1) >
Sent: Thursday, 21 April 2022 1:56 PM
To: s 22(1) ; s 22(1)
Cc: s 22(1) >; s 22(1) >
Subject: Services Australia Submission to ESR [SEC=OFFICIAL:Sensitive]

~~OFFICIAL: Sensitive~~

Good afternoon s 22(1)

I am emailing to possibly get an update on Services Australia's submission to the Electronic Surveillance Reform Discussion Paper.

The Electronic Surveillance Reform Branch received a draft copy of Services Australia's submission in late February, but were informed that it was not SES-approved (see attached). We have still yet to receive a formal submission from Services Australia.

We are now moving into the drafting phase of the reforms and would value Services Australia's input as we move forward.

Can we take the draft that was provided to ESRB as your formal submission?

Happy to discuss

Kind regards,

s 22(1)

s 22(1)
Policy Officer | ESR Governance & Engagement Section
Electronic Surveillance Reform Branch
Electronic Surveillance and Law Enforcement Policy Division
Department of Home Affairs
P: s 22(1)
E: s 22(1)

~~OFFICIAL: Sensitive~~