



Anthony Smith

By email: [REDACTED]

2 December 2025

Our Ref: REV-2025-0947041
Your Ref: N/A

Dear Mr Smith

**Government Information (Public Access) Act 2009 (NSW)
Internal Review Notice of Decision**

1. Original access application

I refer to your access application made under the *Government Information (Public Access) Act 2009 (NSW)*, (**GIPA Act**) received on 2 October 2025 requesting:

Following the withdrawal of my previous broad application (GIPAA-2025-0897481), I am submitting this refined application for specific records held by the NSW Police Force. This request is focused on documents related to the investigation, prosecution, and handling of charge H81615839, particularly concerning disputed evidence and alleged procedural misconduct by officers at the Kings Cross Police Area Command.

Please search under Tony as well as Anthony Smith

I formally request access to the following documents:

I. RECORDS REGARDING DISPUTED EVIDENCE IN BRIEF H81615839

This section pertains to specific items of evidence included in the Brief of Evidence that were directly contradicted by records also in the possession of the investigating officer.

Phone Call Fabrication Evidence:

- 1. All internal police reports, running sheets, or file notes detailing the decision-making process to include the sworn allegation of a phone call from [mobile phone number provided] on September 4, 2023, as a "fact" in the Police Facts Sheet for H81615839.*
- 2. A copy of the telecommunication records obtained by police for the number [mobile phone number provided] covering the period September 1–7, 2023, which showed a "Total*

InfoLink

Office of the General Counsel

Locked Bag 5102 Parramatta NSW 2124

T: 02 8835 6888 **W:** www.police.nsw.gov.au **E:** GIPA@police.nsw.gov.au

TTY: 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

TRIPLE ZERO (000)

Emergency only

POLICE ASSISTANCE LINE (131 444)

For non emergencies

CRIME STOPPERS (1800 333 000)

Report crime anonymously

Result Count: 0".

Meta Data Omissions and Entrapment Evidence:

3. *A complete, unredacted copy of all Meta data obtained by Kings Cross PAC in relation to this investigation, specifically for the Instagram accounts [usernames provided]*
4. *Any internal report or email detailing Constable Dellenty's review of the full conversation history I provided, which proved the [username provided] account had engaged in conversation prior to the dates alleged in the complaint.*
5. *Any file note or record explaining the decision to omit from the Brief of Evidence the Meta data showing (person named) (account name) followed the [username provided] account in July 2023, months before the November 2023 date he claimed in his sworn statement.*

II. RECORDS REGARDING ALLEGED MISCONDUCT AND PROCEDURAL OBSTRUCTION

This section pertains to the conduct of police officers in restricting communication, dismissing evidence, and the handling of official records.

Denial of Right to Make Representations:

6. *Any records, file notes, or emails documenting the receipt and assessment of the psychological report I provided, which detailed my diagnosed PTSD and inability to attend Kings Cross Police Station for a formal interview.*
7. *Any internal correspondence discussing the decision to nonetheless require an in-person interview as the only means for me to make representations against the charge.*

Communication Ban and "Harassment" Label:

8. *All internal records, recommendations, and correspondence between Constable Dellenty, Inspector Martha Winch, and Commander David El-Badawi that led to the formal communication ban issued on February 21, 2025.*
9. *Any internal email or report where my attempts to provide evidence were officially characterized as "harassment."*

False Claim of Brief of Evidence Service:

10. *All internal emails and records from Inspector Martha Winch relating to her assertion that the Brief of Evidence (BoE) for H81615839 had been served on me prior to February 16, 2025.*
11. *Copies of the CMFMS system alerts or "Brief Overdue" warnings sent to Constable Dellenty between May 3, 2025, and June 5, 2025, which confirm the BoE was not served on the defence.*

Alleged Destruction of Records:

12. *All records relating to the internal review finding where Constable Dellenty advised that "some information she had received that was not saved on ViewIMS had been deleted" after the court matter was finalized. This includes any notes or reports detailing what information was deleted and the reason for its deletion.*

III. RECORDS REGARDING DISMISSAL OF COMPLAINANT'S ALLEGED CRIMINALITY

This section pertains to the police assessment of evidence I provided concerning alleged criminal acts by the complainant, (person named).

Assessment of Impersonation and Drug Sales:

- 13. All documents, running sheets, and reports detailing Senior Constable Joseph De Angeli's assessment of the video evidence I provided on November 29, 2024, showing (person named) allegedly using the "Tony Smith" alias to sell drugs on Telegram.*
- 14. The formal report or file note where Senior Constable De Angeli made the determination that this conduct did "not constitute a crime" under identity crime legislation.*

I have added numbering next to each item for easy reference to the item within this Notice.

2. Original Decision

On 20 November 2025, the NSW Police Force (**NSWPF**) made a decision in response to your access application.

It was determined, under section 58(1)(d) of the GIPA Act, to refuse to provide access to some of the information you seek because there is an overriding public interest against disclosure of the information.

It was determined, under sections 58(1)(a) and 58(1)(d) of the GIPA Act, to provide access to some of the information you seek, except where there is an overriding public interest against disclosure.

It was determined, under section 58(1)(b) of the GIPA Act, that the balance of the information is not held by this agency.

3. Application for Internal Review

On 23 November 2025, InfoLink received your valid application for an internal review of the original decision.

Part 5 of your application for internal review states:

5. REQUESTED OUTCOME

I request that the Internal Review Officer:

- 1. Set aside the original decision.*
- 2. Release unredacted (or appropriately redacted) versions of:*
 - (a) Meta business records relating to the identified accounts,*
 - (b) the phone search results showing the "Total Result Count: 0,"*
 - (c) any internal communications regarding these contradictions.*
- 3. Apply s.74 redaction only where strictly necessary (e.g., unrelated personal addresses or third-party identifiers).*

The requested information is essential to understanding how a prosecution proceeded on sworn allegations that were contradicted by data police already possessed.

I acknowledge your submissions accompanying your internal review application. I note that I have considered the internal review to be limited to the above scope provided by you.

I have added letters to the above scope for ease of reference. I note that I interpreted point 2(c) of your request as whether records for item 4 and 5 of your original scope are held. For an abundance

of clarity, I have taken point 2(c) to be as follows:

4. *Any internal report or email detailing Constable Dellenty's review of the full conversation history I provided, which proved the [username provided] account had engaged in conversation prior to the dates alleged in the complaint.*
5. *Any file note or record explaining the decision to omit from the Brief of Evidence the Meta data showing (person named) (account name) followed the [username provided] account in July 2023, months before the November 2023 date he claimed in his sworn statement.*

An internal review is to be done by making a new decision, as if the primary decision being reviewed has not been made, with the new decision being made as if it were being made when the access application to which the review relates was originally received.

An internal review is not to be done by the person who made the original decision and is not to be done by a person who is less senior than the person who made the original decision.

4. Searches for Information

Under the GIPA Act, NSWPF must conduct reasonable searches to locate the government information you seek.

During the original decision, InfoLink conducted searches with Kings Cross Police Area Command. Kings Cross PAC advised that searches were conducted on COPS, the Record Management System (RMS), its P-drive and email archives.

I confirm I have reviewed the searches conducted by Kings Cross PAC during the original decision for the purposes of the limited internal review scope. I note that Kings Cross PAC advised InfoLink during the original decision that no documents exist for items 4 and 5 of your original scope. The PAC also advised that the only Meta data information and telecommunications records obtained by police are found in the brief of evidence for charge H81615839, which I note was already served on you in June 2025. I note that Kings Cross PAC has already conducted searches for similar material related to charge H81615839 across several of your access and internal review applications made under the GIPA Act.

I note that the NSW Civil and Administrative Tribunal in the matter of *Wojciechowska v Commissioner of Police (NSW)* [2020] NSWCATAP 173 at [38] observed the following:

"Being familiar with the type of information it holds, its information management and retrieval systems, generally the agency will be best placed to make an assessment about the likelihood that the requested information exists and is held by it."

I am also guided by the Tribunal in the case *Fisher v Upper Lachlan Shire Council* [2022] NSWACATAD 65 at [78], in that having a reasonable expectation of that certain records is held does not automatically mean that an Agency has failed to conduct reasonable searches:

"...while there might be an expectation or obligation that a public sector agency holds the specified information for which access is sought, and the public sector agency fails to locate that information in dealing with the access request, this does not automatically mean that the public sector agency has failed to comply with the requirements of s 53(2). On the contrary, it can also mean that the public sector agency does not hold the information, which is a decision that is open to the public sector agency to make under s 58(1)(b) of the GIPA Act regardless of whether there is an expectation or obligation on that agency to have and hold such information."

I am satisfied no other information within the scope of your internal review application is held by the agency other than the documents listed in the schedule.

5. Decision

I am authorised by the New South Wales Commissioner of Police to determine applications made under Section 9(3) of the GIPA Act.

With regard to the Meta business records, Subscriber/CCR (phone search results) and emails sent from PCSC De Angeli to yourself, I have decided, under sections 58(1)(a) and 58(1)(d) of the GIPA Act, to provide access to the information you seek, except where there is an overriding public interest against disclosure.

I also note that the Meta business records and Subscriber/CCR responsive to this request were already served on you in June 2025 in a brief of evidence for charge H81615839. From your submissions, it appears that you are of the belief that this agency holds meta data details for the Instagram accounts identified in your application for item 3 of your original scope. I have decided, under section 58(1)(b) of the GIPA Act, that the meta data records for those identified accounts are not held by this agency.

With regard to “*any internal communications regarding these contradictions*” (which I’ve taken to be points 4 and 5 of your original scope), I have decided, under section 58(1)(b) of the GIPA Act, that the information is not held by this agency.

I have also considered section 74 of the GIPA Act, which allows an agency to redact information from a record if the deleted information is irrelevant to the application, or is not within the scope, or an agency has decided to refuse access to the information.

I note that there is a discrepancy in the internal review page numbers compared to the original decision page numbers because a duplicate record was removed. This is because the last seven pages (from pages 33-39 of the original decision) is a duplicate record of the phone search. I have removed the duplicate phone search record i.e. pages 33-39 from the internal review records.

In making my decision, I took into account that this agency cannot control how information released under the GIPA Act is used or disseminated.

These grounds for my decision are set out in my reasons for decision below where I have addressed the public considerations both in favour of, and against, disclosure of the information you have requested.

In the schedule of documents, I have identified whether each document relevant to your application has been released in full, partially or withheld entirely. Against each document I have identified the relevant public interest considerations against disclosure that have justified the decision not to disclose the information.

6. Reason for decision

Under section 9(1) of the GIPA Act, you have a legally enforceable right to access the information you seek, unless there is an overriding public interest against its disclosure.

In order to determine whether or not there is an overriding public interest against disclosure of the information I must apply the public interest test.

Section 13 of the GIPA Act sets out the public interest test as follows:

There is an overriding public interest against disclosure of government information for the purposes of this Act if (and only if) there are public interest considerations against disclosure and, on balance, those considerations outweigh the public interest considerations in favour of disclosure.

The public interest test requires that I undertake the following steps:

Step I: identify the public interest considerations in favour of disclosure;

Step II: identify the public interest considerations against disclosure; and

Step III: decide the weight of the public interest considerations in favour of and against disclosure and where the balance between those interests lies.

Public Interest considerations in favour of disclosure

In accordance with section 12 of the GIPA Act, I have taken into account the following public interest considerations in favour of disclosure of the information:

- The statutory presumption in favour of the disclosure of government information.
- The general right of the public to have access to government information held by the agencies.
- The release of the information requested could reasonably be expected to promote accountability and transparency of this agency.
- Disclosure of the information could reasonably be expected to inform the public about the operations of agencies and, in particular, their policies and practices for dealing with members of the public.
- Disclosure of the information could reasonably be expected to promote open discussion of public affairs and the effectiveness of policies and legislations, enhance Government accountability or contribute to positive and informed debate on issues of public importance.
- The information under review includes your personal information and it is in the public interest for you to have access to government information held about you by the agencies.
- The disclosure of information will assist you to understand the investigator's findings and it is expected to promote accountability of police investigations and actions.

Public Interest considerations against disclosure

When applying the public interest test, the only public interest considerations against disclosure that I can take into account are those set out in the table to Section 14, and Schedule 1 of the GIPA Act.

Section 14, Clause 1(f)

Clause 1(f) provides that there is a public interest consideration against the disclosure of information if disclosure of the information could reasonably be expected to prejudice the effective exercise of an agency's functions.

Some information refused under clause 1(f) relates to contact details of government employees. Should these internal contact details be made publicly available, the functions of the agency would be prejudiced as police would be required to spend time managing unsolicited communication and redirecting members of the public to the appropriate channel for their concern. I note that this would not contribute to the core objectives of NSW Police to enhance community safety by preventing, detecting and disrupting crime. I have therefore given strong weight to clause 1(f).

Section 14, Clause 3(a)

Clause 3(a) of the section 14 table provides that there is a public interest consideration against the disclosure of information that would *reveal an individual's personal information*.

The information withheld under this clause contains information, of and about other individuals whose identity is apparent or can be reasonably ascertained from it. It is therefore personal information as defined in clause 4 of schedule 4 to the GIPA Act.

"Reveal" is defined in clause 1 of schedule 4 to mean *"to disclose information that has not otherwise*

been publicly disclosed". In *Commissioner of Police (NSW) v Field* [2016] NSWCATAP 59, the NCAT Appeal Panel held that personal information is only revealed when it is publicly disclosed.

In *DQN v University of Sydney* [2019] NSWCATAD 159 (DQN), the Tribunal held that even if an applicant is aware of the name of a third party, this information would not be considered to have been "revealed" where there is no evidence that the information has been publicly disclosed.

There is nothing in your application or this agency's records to indicate that the information withheld about this third party, such as personal contact information of third parties, is in the public domain – i.e. revealed. Disclosure would therefore reveal the information and breach the rights of the individuals concerned to have their information protected.

I am satisfied there is a public interest consideration against disclosure of information under clause 3(a) of the section 14 table.

Section 14, Clause 3(b)

Clause 3(b) provides that there is a public interest consideration against the disclosure of information that would contravene an information protection principle (IPP) under the *Privacy and Personal Information Protection Act 1998 (PPIPA)*.

The IPP relevant to this application is that contained in section 18 of the PPIPA, which only allows for disclosure of personal information in certain prescribed circumstances.

Section 18 provides as follows:

18 Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

- (a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or*
- (b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or*
- (c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.*

The personal information withheld was recorded by police for law enforcement purposes in the course of their duties.

Disclosure of the personal information in response to an access application under the GIPA Act would not be a disclosure directly related to the purpose for which the information was collected.

There is no basis for the agency to have a reasonable belief that the persons concerned would not object to disclosure.

There is no basis for a reasonable belief that the persons would be aware that their personal information, including images could be disclosed in response to an application under the GIPA Act and disclosure is not necessary to prevent or lessen a serious and imminent threat to the life or health of an individual concerned or another person.

Disclosure of personal information in response to your access application would not therefore fall within the scope of any of the disclosures permitted under the terms of section 18.

Therefore, I am satisfied there is a public interest consideration against disclosure of information under clause 3(b).

Balancing the public interest considerations

On balance, I decided that the section 14 table factors outweigh the section 12 factors and there is an overriding public interest against disclosure of the redacted information.

I have given significant weight to the considerations in favour of disclosure, particularly that some of the information relates to you and disclosure of the information would assist you to understand the investigator's findings and it is expected to promote accountability of police actions. I have also taken into account your motives for making the application as outlined in your submissions for the internal review.

I have, however, decided to afford greater weight to considerations against disclosure as disclosure under the GIPA Act is effectively disclosure in the public domain and there is the risk that the information, if disclosed, could be made available in the broader community. I have decided that there is a significant public interest to protect the personal privacy of individuals and to not disclose contact information of government employees into the world at large to ensure the effective exercise of this agency's functions.

I also note that individuals expect government agencies to not reveal personal information about them unless they have provided consent to the release. Should members of the public become aware that their information was being released under a GIPA Act application such as their IP addresses and other details, they could become reluctant to assist NSW Police in future investigations thereby jeopardising the criminal investigative functions of this agency.

In summary, I have satisfied that the section 14 public interest considerations against disclosure outweighs the section 12 public interest considerations in favour of disclosure.

7. Review rights

If you are not satisfied with any of the decisions in this notice that are reviewable, you may exercise your review rights under Part 5 of the GIPA Act by requesting:

- an external review of the decision by the Information Commissioner or the NSW Civil and Administrative Tribunal (**NCAT**) which must be lodged within 40 working days from the date of this notice.

For further information on your review rights, please visit: <https://www.ipc.nsw.gov.au>

If you have any enquiries in relation to this decision, please contact me on (02) 8835 6888. In any return correspondence, please quote Our Reference Number stated at the top of this notice.

Yours sincerely



Janita K
Senior Advisory Officer
InfoLink

SCHEDULE OF DOCUMENTS

InfoLink Page No.	Document Description	Format of Record	Location of record in agency	Released or Refused	Relevant Public Interest consideration(s) against disclosure: T = Section 14 Table
1-3	Email dated 29 Nov 2024	PDF	Kings Cross PAC	Released in part	T1(f) T3(a) T3(b)
4-21	Meta Platforms Business Record x 2	PDF	Kings Cross PAC / Brief of Evidence	Released in part	T3(a) T3(b)
22-32	Subscriber/CCR (Phone Search Results)	PDF	Kings Cross PAC / Brief of Evidence	Released in part	T3(a) T3(b)

On 29 Nov 2024, at 18:08, Joseph De Angeli T1(f) @police.nsw.gov.au> wrote:

Hi Tony,

Thank you for the additional information. I've reviewed the relevant sections of the *Crimes Act* and would like to provide further clarification.

Under the *Crimes Act*:

- **Section 192K** relates to the possession of identification information with the intention of committing or facilitating the commission of an indictable offence.
- **Section 192J** concerns dealing with identification information with the same intention.
- **Section 192I** defines "identification information" as data capable of identifying a person, including names, addresses, identification numbers, biometric data, and other personal information.

For an act to constitute an offence under these provisions, it must be proven beyond a reasonable doubt that the person:

1. Possessed or dealt with **your specific identification information**, and

2. Used this information with the **intention of committing or facilitating an indictable offence**.
In this case, while T3 appears to have used your name as an alias online, this does not meet the threshold for an offence under these sections. Using an alias, even if it matches your name, does not establish that he had possession of your personal identification documents or information, nor does it demonstrate intent to use your identity to commit an indictable offence. Without clear evidence of these elements, the conduct does not constitute an offence under sections 192K or 192J.
Essentially investigators would need to prove that your identification documents were used to open these accounts and facilitate the supply of prohibited drugs. An example of this would be if a person possessed your driver's licence passport and took out a personal loan in your name. They have utilised your identification documents to fraudulently obtain a financial benefit.
In this case, a person using a name matching yours, would not suffice in these circumstances.
I acknowledge the seriousness of your allegations regarding drug supply and have noted the information you provided. I will pass this on to the relevant officers for further consideration.

Regards,
<image001.jpg>

Joseph De Angeli
Plain Clothes Senior Constable
Kings Cross Criminal Investigations Kings Cross Police Area Command
1-15 Elizabeth Bay Road, Elizabeth Bay, NSW, 2011
E T1(f@police.nsw.gov.au P T1(f) E T1(f M T1(f)

s74 Not in Scope

On 29 Nov 2024, at 17:18, Joseph De Angeli T1(f) @police.nsw.gov.au wrote:

Tony,
Thank you for your email. I've reviewed the lengthy email chain you've provided and the associated attachments. I would like to clarify the situation and address your concerns regarding T3(a) alleged use of your personal information online.
From what I understand, you believe T3 is using your personal details to create accounts across various platforms, including Telegram and Microsoft Teams, and operating under your name as an alias. Based on the information and evidence you've provided; I can confirm that T3 appears to be using your first and last name as an alias.
However, after reviewing the relevant offences under identification and fraud laws, the two sections potentially applicable are:

- **Section 192K – Possess identification information to commit/facilitate an indictable offence.**
 - This offence applies to a person who possesses identification information with the intention of committing, or facilitating the commission of, an indictable offence.
- **Section 192J – Dealing with identification information to commit/facilitate an indictable offence.**
 - This offence applies to a person who deals in identification information with the intention of committing, or facilitating the commission of, an indictable offence.

Section 192I – Definition of "Identification Information":

The term "identification information" is defined broadly and includes:

- A name or address.
- Date/place of birth, marital status, relative's identity, or similar information.
- Driver licence or licence number.
- Passport or passport number.
- Biometric data or a voice print.
- Credit/debit card, account numbers, usernames, or passwords.

Digital signatures.

- Any information or identifiers intended for personal identification (e.g., ABN).

The law also defines "deal" with identification information to include **making, supplying, or using such information**.

To meet the legal threshold for the offences outlined above, it must be proven beyond a reasonable doubt that T3(possesses or deals with your identification information with the intent of committing, or facilitating, an indictable offence. Based on the evidence you have provided, the use of an alias online does not currently meet these requirements, as there is no proof that T3(is using your identification information in a manner that meets the legal standard of these offences.

Regarding your concerns about the handling of arrests or investigations, I am unable to provide detailed information about these matters. If you require further details, you may:

1. Submit a **GIPPA request** online to formally request access to records.
2. If you are a victim of specific offences involving T3(provide me with those details. I can then share the names and contact information of the relevant officers handling those cases. Any additional information must be obtained through a formal GIPPA request.

I hope this clarifies the situation. If you have further evidence or specific concerns, please don't hesitate to provide those details, and I'll assist where

Regards,

<image001.jpg>

Joseph De Angeli

Plain Clothes Senior Constable

Kings Cross Criminal Investigations Kings Cross Police Area Command

1-15 Elizabeth Bay Road, Elizabeth Bay, NSW, 2011

E T1(f@police.nsw.gov.au P T1(f) E T1(f M T1(f)

s74 Not in Scope

Service Instagram
Internal Ticket Number 8393011
Target T3(a) T3(b)
Account Identifier
Account Type InstagramUser
Generated 2024-02-05 06:41:06 UTC
Date Range 2022-09-01 00:00:00 UTC to 2023-12-01 23:59:59 UTC

Ncmec Reports NCMEC Cybertips: NCMEC cybertip reports associated to the account of the sender.
Definition CyberTip ID: Unique identifier associated with the cybertip.
Time: Date and time the NCMEC cybertip was sent.
Responsible Id: Identification number of the sender's Facebook account associated with the NCMEC cybertip report.

NCMEC CyberTip Numbers No responsive records located

Name Name: Provided by the account holder.
Definition First: First name provided by the account holder.

Name **First** T3(a) T3(b)

Emails Emails: Captures the listed email address associated with the account.
Definition

Registered Email Addresses T3(a) T3(b) Verified)

Vanity Vanity: Username associated with the account.
Definition

Vanity Name T3(a) T3(b)

Registration Date Registration Date: Date and time of account creation.
Definition

Registration Date T3(a) T3(b)

Registration Ip Registration Ip: IP address associated with account creation.
Definition

Registration Ip T3(a) T3(b)

Account End

Date Definition Account End Date: Displays the status of the account at the time the records were generated.
Account Still Active: Indicates true or false.
Time: Date and time the account was closed.

Account Closure Date	Account Still Active Time	false T3(a) T3(b)
-----------------------------	----------------------------------	----------------------

Phone Numbers Definition Phone numbers: Phone number(s) provided by the account holder. "Verified" indicates the account holder responded to a text sent to the listed phone number.

Phone Numbers No responsive records located

Ip Addresses Definition IP Addresses: IP addresses associated with the account.
Time: Date and time associated with the IP address.

Ip Addresses	IP Address Time	T3(a) T3(b)
---------------------	------------------------	-------------

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address Time

IP Address T3(a) T3(b)

Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address

Time
T3(a) T3(b)

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
T3(a) T3(b)
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address

Time T3(a) T3(b)

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address T3(a) T3(b)

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time

IP Address

Time T3(a) T3(b)

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address T3(a) T3(b)

Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

Service Instagram
Internal Ticket Number 8393011
Target Account Identifier T3(a) T3(b)
Account Type InstagramUser
Generated 2024-02-05 06:40:56 UTC
Date Range 2022-09-01 00:00:00 UTC to 2023-12-01 23:59:59 UTC

Ncmec Reports NCMEC Cybertips: NCMEC cybertip reports associated to the account of the sender.
Definition CyberTip ID: Unique identifier associated with the cybertip.
Time: Date and time the NCMEC cybertip was sent.
Responsible Id: Identification number of the sender's Facebook account associated with the NCMEC cybertip report.

NCMEC CyberTip Numbers No responsive records located

Name Name: Provided by the account holder.
Definition First: First name provided by the account holder.

Name **First** T3(a) T3(b)

Emails Emails: Captures the listed email address associated with the account.
Definition

Registered Email Addresses T3(a) T3(b) (Verified)

Vanity Vanity: Username associated with the account.
Definition

Vanity Name T3(a) T3(b)

Registration Date Registration Date: Date and time of account creation.
Definition

Registration Date T3(a) T3(b)

Registration Ip Registration Ip: IP address associated with account creation.
Definition

Registration Ip T3(a) T3(b)

Account End

Date Definition Account End Date: Displays the status of the account at the time the records were generated.
Account Still Active: Indicates true or false.
Time: Date and time the account was closed.

Account Closure Date	Account Still Active Time	false T3(a) T3(b)
-----------------------------	----------------------------------	----------------------

Phone Numbers Definition Phone numbers: Phone number(s) provided by the account holder. "Verified" indicates the account holder responded to a text sent to the listed phone number.

Phone Numbers No responsive records located

Ip Addresses Definition IP Addresses: IP addresses associated with the account.
Time: Date and time associated with the IP address.

Ip Addresses	IP Address Time	T3(a) T3(b)
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	
	IP Address Time	

IP Address T3(a) T3(b)

Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address

Time

T3(a) T3(b)

IP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
TimeIP Address
Time

IP Address T3(a) T3(b)

Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address

Time T3(a) T3(b)

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address T3(a) T3(b)

Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address

Time
T3(a) T3(b)

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address T3(a) T3(b)

Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

IP Address
Time

REQUEST TYPE	IP Address Check
DATE RANGE	04.09.2023 - 00:00:00 / 04.09.2023 - 00:00:00 Australia/Queensland
RECORD COUNT	1
PUBLIC IP	T3(a) T3(b)
PUBLIC PORT	
TPGT_REFERENCE	T3(a) T3(b)
AGENCY_REFERENCE	12796713

Subscription Type	Private IP	Private Port	IPv6 Address	MSISDN
T3(a) T3(b)	T3(a) T3(b)			

23/04/2024 11:11:27

AVC ID	Event Start Date	Event Start Time	Event End Date	Event End Time
--------	------------------	------------------	----------------	----------------

T3(a) T3(b)

T3(a) T3(b)				
Name	Address	Service Type	Dob	Connection Date

Confidential

Service Provider	T3(a) T3(b)
Disconnection Date	

Request Summary: Phone Search - Communication Records

Summary

CSP Reference: 2617668
Agency Reference: Normal Users 12647763
Request Completion Duration: 25 second(s)
Date Submitted: 03-Feb-2024 17:16:21
Completed On: 03-Feb-2024 17:16:46
Submitted By: POLNSFS2 RDHI
Assigned To: *****

Status: Complete

More Details

Organisation making Request: POLNSFS - NSW Police Force - State Intelligence Command

Relevant Legislation: 178(2) Criminal
Case Agency Reference: Normal Users 12647763 20240203T171621+1100
Request Type: Phone Search - Communication Records
Repeat Interval: Non Repeatable
Priority: Routine
Execution Start Date: 03-Feb-2024 17:16:21
Date From: 01-Sep-2023 00:00:00 - Australia/Sydney (AEST)
Date To: 07-Sep-2023 23:59:59 - Australia/Sydney (AEST)
Service Number: T3(a) T3(b)
IMEI:
IMSI:
Call Direction: A Party
Types of Calls to search through: All

GST EXCL AMT: \$20.00

Results

Query Start Time : 03-Feb-2024 17:16:29
Total Result Count : 0

Results for table : Multiple Source Record Table

Result count : 0

Data Type Data Sourc UTC Times A Party Loc B Party Loc Duration (\$ A Party Ori A Party For A Party IMI

A Party IM| A Party IM| A Party Sta A Party Sta A Party Sta A Party Sta A Party Sta A Party Sta A Party Sta

A Party Enc A Party Enc A Party Enc A Party Enc A Party Enc A Party Enc A Party Enc B Party Ori B Party For

B Party IMI B Party IMI B Party IM! B Party Sta B Party Sta B Party Sta B Party Sta B Party Sta B Party Sta

B Party Sta B Party Enc B Party Enc B Party Enc B Party Enc B Party Enc B Party Enc B Party Enc R Party For

R Party Original Number

From	To	Carrier	Csp
#####		Telstra	Telstra Limited