From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No. 15/25 - S.40(2) - CRU Circulation (08/01/2025) - Wrongful protest arrests & Police powers and arrests - Including Advice
Date: 10 January 2025 14:14:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU today. Advice is at the end of the message.

Log Number: 15/25
Case worker: S.40(2) [redacted]
Logged with: National
Sent from: S.40(2) [redacted]

Applicants Request:

1. Between 1 January 2022 and 1 January 2025, how many times has your force made a wrongful arrest, when "protest" was recorded as part of the arrest, or the arrest was recorded as taking place at a "protest." Please provide data by calendar year.

2. For each wrongful arrest when "protest" was recorded as part of the arrest, or the arrest was recorded as taking place at a "protest", please can you provide the offence under which the arrest was made, e.g. the offence of locking on; assaulting an emergency worker.

3. Between 1 January 2022 and 1 January 2025, how much compensation has your force paid out to victims of wrongful arrest, when "protest" was recorded as part of the arrest, or the arrest was recorded as taking place at a "protest." Please provide data by calendar year.

4. In the time period 28/06/2022 up to 01/01/2025, on how many occasions has your force used the powers allowed for in Section 75 of the Police, Crime, Sentencing and Courts Act 2022: Offences under sections 12 and 14 of the Public Order Act 1986?

Sections 12 and 14 of the 1986 Act (as amended by the Police, Crime, Sentencing and Courts Act 2022) allow the police to impose any type of condition on a public procession or public assembly necessary to prevent: significant impact on persons or serious disruption to the activities of an organisation by noise; serious disorder; serious damage to property; serious disruption to the life

of the community; or if the purpose of the persons organising the protest is the intimidation of others with a view to compelling them not to do an act they have a right to do, or to do an act they have a right not to do.

5. In the time period 28/06/2022 up to 01/01/2025, how many arrests has your force made under Section 78 of the Police, Crime, Sentencing and Courts Act 2022: the offence of intentionally or recklessly causing public nuisance

6. In the time period 28/06/2022 up to 01/01/2025, on how many occasions has your force used the powers allowed for in Section 79 of the Police, Crime, Sentencing and Courts Act 2022: imposing conditions on one-person protests?

7. In the time period 12/05/2022 up to 01/01/2025, how many arrests has your force made under Section 80 of the Police, Crime, Sentencing and Courts Act 2022: wilful obstruction of a highway?

Please provide data by calendar year.

CRU Advice:

We are aware that not all forces have received every question set out above in their request, some have referred only 1-3, some only 4-7. However for ease of reference for everyone, the below advice applies to all of the above questions. If you have received these questions over 2 or 3 different requests from the same applicant, then please be advised they can be aggregated for cost purposes.

Assuming s12 is not applicable, then we cannot see any immediate harm in providing the requested data, including where no information is held. However disclosure of figures, if held, will be subject to your local assessment that no individuals can be identified nor personal data released, and no ongoing investigations undermined.

A query has been raised by one force whether disclosure would risk undermining policing at protests in the future. On balance, as this is largely statistical data only we cannot see enough evidence to warrant exemption for that reason. Even where numbers are low or no information is held, providing data on arrests at past protest events would not be indicative of actions taken at future events.

Kind regards

S.40(2)
[redacted]
National Freedom of Information Referral Officer
National Police FOI & DP Central Referral Unit (NPFDU)
National Police Chiefs' Council

NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)
[redacted]

From: NPCC CRU Mailbox
Bcc: S.31(1) [redacted]
Subject: Log No.39/25 - Goldsmith Chambers - CRU Circulation (19/02/2025) - Including Advice
Date: 19 February 2025 13:02:00
Attachments: image001.png

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Please find the below advice regarding:

Log Number:39/25
Case worker:S.40(2) [redacted]

Applicants Request:

I am sending this as a request for information to establish relative to the document attached (Goldsmiths Chambers - private criminal prosecution), if your constabulary either individually or in groups of two or more, or officers individually, have supported and or gained from support for private criminal cases - be that on the prosecution or defence teams.

In that respect, please consider as examples (not limited):
1. 2002-08 aligned to work conducted by Keir Starmer with PSNI, CPS and DUP
2. 2013-14
3. Aligned to Brexit - therefore from 2016 onwards
4. Electoral issues
5. Profiling issues
6. Political parties or interests of other Countries (e.g. Joe Biden/Democrats/Irish Govt but not limited), private businesses such as Warner, CWU, Royal Mail (not limited), Services, individuals and celebrities such as Gallagher Gwyther, Govt Depts and non Govt bodies, Family Courts, Churches and schools
7. Councils

There is good reason to believe Police at most senior level have background interfered into my work, family court, healthcare, finances, credit score, benefits and profiling in abuse of private law - and mucked it up. This allowed case precedent to wide spread economic abuse, human trafficking, undue surveillance, normalisation of fraud on profiles to feed courts, cover up of violence, targeted discrimination and cover up of child grooming and predation.

That being so, please outline any gains - direct or indirect- and relative value. NHS has already disclosed their activity in this arena and scorched by the Priory (who confirmed never knowing me and also subject to NHS fraud).

CRU Advice:

There are multiple thoughts/statements from the applicant in this request, however we believe the only questions they are asking is if any members of your force have supported or gained from private criminal cases and to outline any gains - direct or indirect- and relative value from this.

We would advise to clarify with the applicant on their interpretation of 'Gains' & 'Value'. We are assuming they mean monetary gains and values but equally this could also mean promotional, popularity, gratuities etc. We would also ask the applicant for a timeframe for their request.

This may fall into a s12 cost for some of you, and if so, we see no harm in this response.

If however information is held and retrievable and the applicant does mean monetary gains and values, then we would see no harm in a total cost being disclosed as long as the numbers are not low enough to identify an individual, in which case s40 personal details would need to be applied.

Should the applicant come back with more defined questions and further breakdowns, we would be happy to look at them for you.

Any questions please just ask, or drop in to one of our CRU drop in sessions.

Kind regards

S.40(2)
[redacted]
National Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit | National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]
[redacted]

Advanced notification of leave:

S.40(2) [redacted]

From: NPCC CRU Mailbox
Bcc: S.31(1) [redacted]
Subject: Log No.43/25 - Hospital Armed Officers - CRU Circulation (13/02/2025) - Including Advice
Date: 14 February 2025 07:56:00
Attachments: image001.png

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Please see the below advice regarding the following:

Log Number:43/25
Case worker:S.40(2) [redacted]
Logged with:National
Sent from:S.40(2) [redacted]

Applicants Request:

Could you please provide me with a list of the occasions when armed police units have been sent to hospitals since January 1 2020.

For each occasion could you please give the date, the name of the hospital, the number of officers deployed and, if possible, a brief description of the incident.

CRU Advice:

Advice is provided on the assumption that all the requested information can be located and retrieved within the cost threshold. Where this is not relevant, s12 is recommended to be used. When issuing your refusal notice we recommend that you advise the applicant how best to refine their request to fit within the cost threshold, if feasible to do so.

As you will probably know already, the number of firearms operations per force is published via the Home Office - Police use of firearms statistics - GOV.UK.

The applicant has asked for a few categories which we have broken below for ease:

Date + Name Of Hospital + Brief Description – We would advise to locally asses 31(1) Law enforcement and s40 personal information for these details depending on each occasion details. S21 may be relevant to details in the public domain such as Middlesex hospital stabbing: Two people knifed as patients lockdown and man arrested - Mirror Online or Armed response police called to tackle 'aggressive subject' at Leicester Royal Infirmary - Leicestershire Live

Number of armed officers deployed – We would advise against disclosing the number of AFOs in attendance for an event, particularly when the applicant is requesting numbers of AFOs for each occasion such as in this case. Disclosing this would undermine the operational policing purpose and give those with intent the know how on how many AFOs may be sent to a single event and intercept and exploit this for any future deployments and create diversional scenarios to undermine the forces tactics and response of reaching the incident. This would risk the harm of the general public as well as the AFOs themselves, and as the AFOs are a specialist asset we would advise to exempt s24(1) national security and s31(1) Law Enforcement.

[redacted] S.31(1) [redacted]

If you need any further assistance please let us know.

Kind Regards

S.40(2) [redacted]

[redacted] -

[redacted]

National Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit | National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]
[redacted]

Advanced notification of leave:

S.40(2) [redacted]

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Update on Cellebrite - FW: For Info - Information on the BlueLight Portal - Xref 57/25
Date: 14 February 2025 14:32:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear all,

For awareness, following contact with the relevant policing leads the stance on requests seeking to know which providers and their products are used for Digital Forensics should be withheld. And where the request is seeking to confirm a named provider/supplier or product then NCND is advised.

In this instance the supplier in question is Cellebrite - Accelerate justice with Cellebrite. As mentioned below, please continue to conduct relevant housekeeping when possible S.31(1) [redacted] about which there is ICO agreement that information about suppliers can be exempt disclosure. For example - the ICO has previously upheld use of substantive exemptions in revealing products/suppliers in the DF sphere - https://ico.org.uk/media/action-weve-taken/decision-notices/2020/2617697/fs50892736.pdf

For your records, the following form of words is a steer used to assist with responses citing NCND s24(2) and 31(3).

HARM

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying if a particular policing tool of this type (in this case Cellebrite products) is used by FORCE NAME as part of an investigative process could reveal operational tactics linked to policing, compromise police investigations and/or adversely affect the ability of FORCE NAME and others to safeguard national security.

It is well established that police forces utilise Digital Forensic techniques in order to counteract

criminal behaviour, detect crime, and assist in the apprehension and prosecution of offenders. Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. In this case the information relates to a service provider and by extension their products for the extraction of data from devices.

By revealing specific tactical information such as requested within this request, it would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders. When considered on a Force by Force basis, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Likewise, given the sensitive areas in which tools of this type may be used, such as counter-terror investigations, to disclose if any particular tools are used would allow criminals and other adversaries to focus on evaluating the particular capabilities of its use. With this knowledge it would allow criminals and other adversaries to take steps to counteract a specific tool – be it adjusting how they interact and present themselves to take advantage of any weaknesses or gaps in capability they identify. For example, at a simple level, if a policing tool doesn't search 'X 'social media site or was unable to identify 'Y' format of images and criminals can establish this, they will exploit this position. FORCE NAMEs more sophisticated adversaries may be able to go further and take more proactive measures to undermine the tool and/or its provider, and a specific confirmation allows efforts to be focused accordingly.

This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tools are or are not deployed. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

PUBLIC INTEREST TEST

Factors favouring confirming or denying whether any information is held in respect of both exemptions claimed

Confirming or denying whether information is held in response to the request, would provide the public with information about technologies and FORCE NAME capabilities. This would reinforce the wider commitment to openness and transparency with the general public and facilitate public debate. Furthermore, owing to the inherent link between transparency and public

confidence, confirming or denying whether information is held would be likely to improve the general public's confidence in FORCE NAME. Over time, an increase in public confidence would be likely to improve public engagement with the police. This would, in turn, lead to an improvement in our ability to both prevent and detect crime, and apprehend and prosecute offenders.

Factors against confirming or denying whether any information is held for Section 24(2) - National Security

Security measures are put in place to protect the community that we serve. To confirm whether any information relevant to this request is/is not held would be useful intelligence to terrorists and individuals intent on carrying out criminal activity. Irrespective of what information is or is not held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of those with ill-intent gathering information about force capabilities, would have greater impact when linked to other information gathered from various sources. The more information that is disclosed over time will provide a detailed account of the tactical infrastructure, not only at force level but across the country as a whole. Any incident that results from confirming that any information is held would by default affect National Security.

Factors against confirming or denying whether any information is held for Section 31(3) - Law Enforcement

To confirm or deny information is held would compromise the forces' ability to protect the public. Disclosing FORCE NAME capabilities would provide persons intent on disrupting their work, with information that would assist them to do so. In this case, for the reasons outlined in the evidenced harm, the effectiveness of current and future strategies when carrying out investigations and gathering evidence may be compromised. The safety of the public is of paramount importance to policing purposes, and any increase in crime would place the public at risk of harm. When the current or future law enforcement role of the force may be compromised by the release of information, the effectiveness of the force will be reduced.

The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, disclosing tactical information relating to the extraction of data from computers and other devices, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

Balance Test

The points above highlight the merits of confirming, or denying, whether information relevant to this request does or does not exist. Having considered the reasons why FORCE NAME should opt to neither confirm nor deny that information is held, although openness and transparency is at the forefront when considering the public interest, in this case confirmation or denial relating to Digital tools used by the police for investigative purposes would not be in the public interest.

Whilst there is a public interest in appropriately and effectively engaging with the threat from criminals, there is a very strong public interest in safeguarding National Security. As much as

there is a public interest in knowing that policing activity is appropriate and balanced in matters of National Security, this will only be overridden in exceptional circumstances.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with any information that is released. Confirming or denying whether information is or isn't held would reveal specific policing activity in the digital sphere of investigations and would assist those intent on causing harm. Any incident that results from confirmation or denial could, as a result, affect National Security.

I have found that confirming or denying whether information is held in response to questions of this nature, would make public, areas of police interest. This would directly harm the ability of FORCE NAME to investigate crime. This could also reveal police capabilities, compromise police investigations and/or otherwise, adversely affect the ability of FORCE NAME to safeguard national security. I have attached considerable weight to these interests as the primary role of the Police Service is to both prevent and detect crime and apprehend those responsible for committing criminal offences.
Therefore, at this moment in time, it is our opinion that for these issues the balance test for confirming, nor denying, that information is held is made out.

Kind regards,

S.40(2)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)
[redacted]

From: NPCC CRU Mailbox S.31(1) [redacted]
Sent: 17 January 2025 15:40
Subject: For Info - Information on the BlueLight Portal - Xref 572/5

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear all,

S31(1) [redacted]

[redacted]

The reason for my email is on the back of a request referred to the CRU concerning CELLEBRITE, which is a company that provides products for extraction of data from devices such as mobile phones. Previously, responses about CELLEBRITE have been NCND, but we will need to revisit this due to the time elapsed since such advice was provided.

However, should the likelihood be that the NCND is maintained, S31(1) [redacted]

[redacted]

Lastly, I recognise that there is a further piece of CRU work to be done here, and I will look to contact relevant leads with a view to obtaining an update on technologies, products and capability's that should not be highlighted via BlueLight portal or other expenditure. That is easier said than done, but I will keep you informed. S31(1) [redacted]

I will look to provide a further update as soon as possible.

Thank you.

S.40(2) [redacted]
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Good afternoon S.40(2)

Apologies for the delays. I was off for a few days which also crossed over with the reply received from the Policing Lead. In short, it is the Leads view that the direction of travel across the board is to respond NCND about Cellebrite. S31(1) [redacted].

The reason why there has been a delay getting to this position is that there was a need to revisit the stance since it was last advised on during late 2020. S31(1) [redacted]

You may also be interested to note that the ICO has previously upheld use of substantive exemptions in revealing products/suppliers in the DF sphere - https://ico.org.uk/media/action-weve-taken/decision-notices/2020/2617697/fs50892736.pdf

S31(1) [redacted]

In conclusion, NCND s31(3) is our advised course of action. I intend to write to all forces re-enforcing the NCND stance, and will look to include a form of words. In the meantime, if you can extrapolate rationale for the NCND from any previous NCND responses, or from manipulating the wording provided by Cheshire in the DN linked above, please continue accordingly.

Kind regards,

S.40(2)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)

From: NPCC CRU Mailbox
To: S31(1)
Subject: RE: OFFICIAL-SENSITIVE [POLICE]: {FOI/13352}
Date: 11 April 2025 11:26:00
Attachments: image008.jpg
image002.jpg
image003.png
image004.png

Good morning [redacted]
Thank you for sending the below.
I can confirm the current position remains and we reengaged with policing leads early this year.
Please let me know if you'd like me to resend our advice for this one to help form any response?
I've taken a look at the links below, the first one appears to not be found (assuming PSNI have now removed this?) and the second too appear the same. This is not an official site so I do not think this is an issue and I cannot seem to read the rest of the article without signing up. To address the applicants comment that the use of the technology is in the public domain, you can reply that it is well established that police forces utilise Digital Forensic techniques in order to counteract criminal behaviour, detect crime, and assist in the apprehension and prosecution of offenders. But by revealing specific tactical information such as requested within this request, it would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders. When considered on a Force by Force basis, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.
Happy to have sight of your IR draft and address any further concerns.
Many thanks

S.40(2) [redacted]
Head of National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]

Book time with S.40(2) [redacted]

From: NPCC CRU Mailbox
To: S31(1) [redacted]
Subject: RE: OFFICIAL [PUBLIC] [FOI/13603] Security at Homes and Offices of MLAs
Date: 20 January 2025 14:13:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear all,

Thank you for the referral, now logged as 58/25. Please forward a correspondence address for the applicant.

If the following article is to be regarded as a reputable source of information, then it confirms that PSNI does carry out security surveys of MLA residences and work places - PSNI to provide Stormont MLAs with security training amid safety concerns – The Irish News

As such, if the activity can be confirmed generally then our advice is to substantively exempt the data under s24(1), 31(1), 38(1) and 40(2). That way PSNI is not revealing how many MLAs have been provided security advice, and does not reveal any fluctuation of the data through repeated requests of this type. I say this bearing in mind MLAs are elected, and that there are 90 of them, meaning the data would likely change after each election. Through FOI it could then be determined how regularly such surveys are conducted, and whether the numbers change in line with the number of outgoing/incoming MLAs. FOI would then be an intelligence gathering tool about security education amongst the collective pot of MLAs.

If however, this was a request focused on a specific individual or location then the NCND would be advised.

I don't see an need to include a partial NCND s23(5) at this stage S31(1) [redacted]

Kind regards,

S.40(2) [redacted]
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: FW: Update to - FW: Log No.73/25 CRU Circulation (22/01/2025) - AI -GeoSpy Technology - Advice to Follow
Date: 26 February 2025 11:45:00
Attachments: image001.png
image002.png
image003.png
image004.png

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear all,

Thank you for your patience waiting for this.

Please be advised that it is the view of a relevant Policing Lead for Internet Intelligence and Investigations that forces can confirm geolocation tools are used, but not which ones exactly.

Accordingly, as this request names the tool in question, the advice is NCND at Q1, 2 and 3 and 4. Q5 is addressed separately.

Applicants Request

1. Have you engaged the services of the AI geolocation company GeoSpy, or any other AI geolocation company?

2. If so, when did you first engage their services and is the engagement ongoing?

3. If the software has been used, what purposes has it been used for?

4. If the software has been used, are identified locations always independently verified by a human to ensure they match?

5. Has anyone been charged with a crime based wholly or in part on evidence gleaned from

GeoSpy or other AI geolocation software? If so, how many people, and what crimes were they charged with?

Advice for Q5 as follows:

All forces can respond No Information Held along with the following caveat that GeoSpy AI, or similar products, are geolocation tools that can use artificial intelligence to analyse images and determine where they were taken. Any results generated by the use of such tools would be for that purpose alone, which in and of itself would be useful intelligence, but would not constitute evidence sufficient to result in a criminal charge being brought against any individual.

The following is a form of words to assist with a response of NCND s24(2) National Security, and s31(3) Law Enforcement for the remaining questions:

[START]
HARM

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying if Geospy AI is used by **[Force Name]** could reveal operational tactics linked to policing, compromise police investigations and/or adversely affect the ability of **[Force Name]** and others to safeguard national security.

It is well established that police forces utilise intelligence gathering techniques in order to counteract criminal behaviour, detect crime, and assist in the apprehension and prosecution of offenders.

Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. To do this forces rely on access to relevant tools to gather intelligence in a way that would be too resource intensive to do manually. When considered on a Force by Force basis, a malign individual could identify those tactical options most critical to the Law-and-Order sector and specifically target those proving the most assistance. Accordingly, to confirm or deny as to whether any particular software or tool is used by police to gather such intelligence would allow those with malicious intent to target cyber-attacks on those producers, causing disruption or service denial to police forces and thereby preventing intelligence acquisition and undermining law enforcement.

The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level based upon current intelligence, and that threat is currently judged as "SUBSTANTIAL", meaning that an attack on the UK is likely. It is well established that police forces use tactics and technology to gain intelligence in order to counteract criminal behaviour, and it has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.

Confirming or denying whether any information is held about the use of specific internet intelligence gathering tools/platforms would limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling offenders

to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

Public Interest Test

Factors favouring Confirming or Denying for Section 24 - The information, if held, only relates to national security and confirming or denying whether it is held would not actually harm it. The public are entitled to know what public funds are spent on and what measures are in place. By confirming or denying if business is conducted with Geospy AI, or any other likeminded third-party provider, would lead to a better informed public.

-

Factors against Confirming or Denying for Section 24 - By confirming or denying whether any information is held would render policing and security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Factors favouring Neither Confirming or Denying for Section 31 - Confirming or denying whether business is conducted with Geospy AI, or any other likeminded third-party provider, would provide an insight into the Police Service. This would enable the public to have a better understanding of the effectiveness of the police and about how the police gather intelligence. It would greatly assist in the quality and accuracy of public debate, which could otherwise be steeped in rumour and speculation. Where public funds are being spent, there is a public interest in accountability and justifying the use of public money.

Factors against Confirming or Denying for Section 31 - Confirming or denying that any information is held regarding business with Geospy AI, or any other likeminded third-party provider, would have the effect of compromising law enforcement tactics. It has been recorded that FOIA releases are monitored by criminals and terrorists and so to confirm or deny information is held concerning intelligence gathering would lead to law enforcement being undermined. The Police Service is reliant upon all manner of techniques during operations and the public release of any modus operandi employed, if held, would prejudice the ability of the Police Service to perform the functions it exists to provide.

By confirming or denying that a business interest exists would hinder the prevention or detection of crime. The Police Service would not wish to reveal what tactics may or may not have been used to gain intelligence as this would clearly undermine the law enforcement and investigative process. This would impact on police resources and more crime and terrorist incidents would be committed, placing individuals at risk. It can be argued that there are significant risks associated with providing information, if held, in relation to any aspect of investigations or of any nation's security arrangements so confirming or denying that information is held, may reveal the relative vulnerability of what we may be trying to protect.

Decision

The security of the country is of paramount importance and **[Force Name]** will not divulge whether any information is or is not held regarding business with any company, if to do so would place the safety of an individual at risk, undermine National Security or compromise law enforcement.

Whilst there is a public interest in the transparency of policing operations and providing assurance that the **[Force Name]** is appropriately and effectively engaging with the threat posed by various groups or individuals, there is a very strong public interest in safeguarding the integrity of police investigations and all areas of operations carried out by police forces throughout the UK.

As much as there is public interest in knowing that policing activity is appropriate and balanced this will only be overridden in exceptional circumstances. The use of technology can be a sensitive issue that would reveal police tactics and therefore it is our opinion that for these issues the balancing test for confirming or denying whether any information is held regarding the police, Geospy AI, or any other likeminded third-party provider, is not made out.

However, this should not be taken as necessarily indicating that any information that would meet your request exists or does not exist.
[END]

Kind regards,

S.40(2)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)
[redacted]

From: NPCC CRU Mailbox
Sent: 11 February 2025 10:55
Subject: Update to - FW: Log No.73/25 CRU Circulation (22/01/2025) - [redacted] - AI -GeoSpy Technology - Advice to Follow

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear all,

A quick update.

We have not dealt with a request concerning this company before, [redacted]. However, please do not respond to that effect whilst we wait on policing leads feedback.

If necessary, please PIT extend s31 at this time.

Kind regards,

[redacted]
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
[redacted]

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No.77/25 CRU Circulation (11/02/2025) - Facial recognition and PND - Including Advice
Date: 11 February 2025 12:18:00
Attachments: Log No. 96122 - S.40(2) CRU Circulation (06072022) - Facial Recognition - Including Advice.msg
image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU. Advice is at the end of the message.

Log Number:000077/25
Case worker: S.40(2)
Logged with: National
Sent from: S.40(2)

Applicant Request:

Regarding your force's use of Facial Recognition Technology, Retrospective Facial Recognition and the Police National Database (PND). Please provide the following information about your force's use of Facial Recognition Technology, Retrospective Facial Recognition and the Police National Database (PND) for the periods between January 2024 and today's date; if you do not hold this information for the whole length of the period stated above, please provide it for the period starting from the date you began recording the information:

1. The processes (if any) undertaken by your force when using the Police National Database's face search capability to identify children (minors under the age of 18).

2. If there is a Child Rights Impact Assessment for the use of:
The Police National Database (PND)
Facial Recognition Technology
Retrospective Facial Recognition Technology

3. The number of times Facial Recognition Technology, Retrospective Facial Recognition Technology and/or the Police National Database were used to identify children (minors under the age of 18).

4. The following information about each search:

date
reason for search
officer defined ethnicity
self-defined ethnicity
gender of the person searched
age of person searched
response (i.e., whether the search returned a record and led to an arrest)

5. Are CCTV images used during facial recognition checks which utilise the PND? If so, please share the number of times CCTV images were used for facial recognition checks

6. Are CCTV images and footage retained on the Force Video management system, including those which depict children under the age of 16 and under the age of 18?

7. Are images or data from facial recognition searches (in particular of minors under the age of 18) shared with other agencies or private organisations? If so, under what conditions?

8. If your force does not currently use Facial Recognition Technology, retrospective Facial Recognition and/or the Police National Database (PND) please state if there are there plans to.

CRU Advice:

We are aware that the PND NSG has showed interest in this request and as a result the SPOCS for each force were asked to send the request to the Staff Officer to collate. I have engaged with the representative from the PND group to make them aware of the remit of our unit and further discussed the request itself in order to provide the following advice.

The request relates to FR, RFR and PND. Although some questions are solely targeted at PND, the phase 'facial recognition' will capture the use of covert FR and therefore although the questions can be answered, but it must be stated that your response only relates to overt uses of FRa partial NCND s23(5), s24(2) and s31(3) will be required in respect of any potential covert use which may or may not be in use.

Q1 - the applicant is asking for a 'process' used by forces when PND is utilised to identify children. I can confirm there is no nationally produced guidance, but forces may hold local guidance, which will require local assessment to ensure policing is not undermined (s31) and personal data considerations with regards to any names/authors (s40).

Q2 - I have confirmed with the PND policing lead that there is no Child Rights Impact Assessment national for PND, we do not think forces would have undertaken one, and a NIH response is appropriate for all 3 specified FR technologies.

Q3 and Q4 - We understand the Home Office hold the number of searches conducted by each force and, at regular intervals, provide these back to forces, so a total number is held. However, no further breakdown is provided by the HO, i.e. the age, ethnicity or gender is not provided back to the force as a data return. We anticipate these 2 questions will trigger a s12 cost exemption for most forces as they will need to manually review each PND facial recognition search in order to respond. If s12 is not relevant for your force, then we see no harm in providing an overall total for question 3, removing any searches completed in a covert capacity. However, question 4 is then asking for a breakdown per search, which will require a thorough local assessment to ensure that at that level individuals cannot be identified, and only overt

information is considered.

Q5 - CCTV images are used as a probe image in PND which is run against custody images, so the first part of this question is an affirmative 'Yes'. However, the number of times they are used would again likely trigger the s12 cost limit due to requiring a manual search.

Q6 and Q7 - These 2 questions are asking for yes/no response to very general questions and will be force specific. However, we do not feel it is harmful to respond either way (yes or no) to question 6. In relation to question 7, images should only be shared if there is a legal basis to do so, in which case we can see no harm in responding with 'yes' to the question 7.

Q8 - The FOI Act only relates to information 'held' at the time of the request. If you hold confirmation that FR is going to be implemented at a future date, then you can respond to this request confirming plans for LFR, RFR and OIFR only. Any plans to introduce covert specific FR should be withheld under the partial NCND.

A form of words for the partial NCND is attached to help with your response..

Kind regards

S.40(2) [redacted]
Deputy Manager
National Police Freedom of Information and Data Protection Unit (NPFDU)
National Police Chiefs' Council
,NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.40(2), S.31(1) [redacted]

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No. 961/22 - S.40(2) [redacted] - CRU Circulation (06/07/2022) - Facial Recognition - Including Advice
Date: 14 July 2022 11:36:00
Attachments: image003.jpg
image004.jpg

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU today. Advice is at the end of the message.

Log Number: 961/22
Case worker: [redacted]
Logged with: National
Sent from: [redacted]

Applicants request:

Please answer the following questions:

1. Has your police force utilised facial recognition technology on a non-trial basis? If so, what was the first date of implementation?

2. Please list every time facial recognition technology has been used by date (and if possible, the reason for its deployment)

3. Please list how many people have been identified as "True positives" and please subdivide into ethnicity.

4. Please list how many people have been identified as "False positives" and please subdivide into ethnicity.

5. Please provide a percentage breakdown of the ethnicities that were identified as false positives as a total figure

CRU Advice:

To provide some context in support of the below stance: Towards the end of last year there was a change in how we approached requests related to Facial Recognition which was intended to simplify understanding of the technology and assist with responses to FOI requests. Key to the new approach was to identify exactly which type of FR was being referenced in a request (LFR,

OIFR, RFR, CRFRS or COIFRS) and respond accordingly in line with the Terminology Overview which was published. This meant that requests related to LFR, OIFR and RFR could be handled entirely within the window of overt use, thus negating the need for a partial NCND. To support this approach, if an FOI request is received which did not specify exactly what type of Facial Recognition was being referred to, then this must first be clarified with the applicant. This can be done by providing the applicant with a link to the Terminology overview and asking them to confirm which type of FR they require information for.

Responding to the request:

If your force is not using facial recognition technology at all, then you can respond NIH to this request. There is no requirement to include a partial NCND in this instance.

For the handful of forces who do currently utilise facial recognition technology on a non-trial basis then:

We note the applicant has not stated that it is specifically LFR, OIFR or RFR which is being referred to in this request so in line with the above, our advice is that you seek clarification of type of FR being referenced before proceeding, to assist the applicant the terminology overview link can be provided.

If the applicant clarifies they only refer to Live Facial Recognition (as we suspect they do), Operator Initiated Facial Recognition (OIFR) and/or Retrospective Facial Recognition (RFR) then the request can be answered entirely within the window of overt use with no requirement for a partial NCND to be added. In terms of the questions, we see no specific harm in providing information, assuming it is not already published by the force. In terms of question 5 as percentages are unlikely to be held, you could provide the numbers for each ethnicity.

If the applicant clarifies that their request relates to ALL forms of Facial Recognition, so, LFR, OIFR, RFR AND covert options CRFRS and COIFRS, then you will need to make a distinction within your response between overt and covert use. The questions can be answered, but it must be stated that your response only relates to overt uses of FR. A partial NCND s23(5), s24(2) and s31(3) will be required in respect of any potential covert use which may or may not be in use.

Please see below for example wording to assist with the partial NCND should it be required:

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying that any other information relating to the covert practise of facial recognition would show criminals what the capacity, tactical abilities and capabilities of the force are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities. Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of facial recognition would lead to an increase of harm to covert investigations and compromise law enforcement. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.

The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level, based upon current intelligence and that threat is currently categorised as 'substantial', see below link:

https://www.mi5.gov.uk/threat-levels

The UK continues to face a sustained threat from violent extremists and terrorists.

It is well established that police forces use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.

Confirming or denying whether any information is held relating to the covert use of facial recognition technology would limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling offenders to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities. This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tactics are or are not deployed. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

If you require any further assistance please contact the CRU,

Kind regards

S.40(2) [redacted]
National Freedom of Information Referral Officer
National Police FOI & DP Central Referral Unit (NPFDU)
National Police Chiefs' Council
T. 01489 569826
A. c/o ACRO, PO BOX 481, PO14 9FS
S.31(1) [redacted]
[redacted]

-

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No.103/25 CRU Circulation (19/02/2025) - Officer Number Modern Slavery Offences - Including Advice
Date: 19 February 2025 12:26:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU. Advice is at the end of the message.

Log Number:000103/25
Case worker: S.40(2) [redacted]
Logged with: National
Sent from: S.40(2) [redacted]

Applicants Request

I am carrying out research into how the police respond to different types of Modern Slavery offences. Please could you provide me with the following information:

1, Number of officers currently serving within your force
2, Number of officers assigned or posted to teams which primarily (or exclusively) deal with child criminal exploitation (such as county lines).

3, Number of officers assigned or posted to teams which primarily (or exclusively) deal with child sexual exploitation.
4, Number of officers assigned or posted to teams which primarily (or exclusively) deal with sex trafficking (forced prostitution).

You may wish to add a footnote as to how your force deals with these issues of Modern Slavery in terms of staffing and resourcing. I am aware that certain forces have designated county lines teams however other forces may encompass a wider drugs squad which would include county lines activity.

CRU Advice:

The below advice is on the presumption that s12 is not relevant. Overall we see no immediate harm in releasing the information for questions 1 - 4.

The number for question 1 is in the public domain, however, we see no harm in providing an up to date number as per the date of the request.

For questions 2-4, our view is that releasing the number of officers who are assigned or posted to these teams is not harmful. It is a snapshot in time, with no indication of future staffing numbers, and doesn't represent the overall number of officers who are capable of dealing with these types of crime should the need arise. It does not therefore reveal capability or operational responsibility such as covert activity, as it is only revealing the number of officers per team at the present time.

If you require any additional assistance please come back to us.

Kind regards

S.40(2) [redacted]
Deputy Manager
National Police Freedom of Information and Data Protection Unit (NPFDU)
National Police Chiefs' Council

,NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
* S.40(2), S.31(1) [redacted]

-

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No.000107/25 CRU Circulation (26/02/2025) - Including Advice
Date: 26 February 2025 15:54:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Please see below advice in relation to the following:

Log Number:107/25
Logged with: National

Applicants Request

The information requested is:
1.Do you routinely support victims of trafficking and modern slavery to submit a reconsideration request to the Competent Authorities within the National Referral Mechanism (NRM) following a negative Reasonable Ground or Conclusive Ground decision?
2.If the answer to question 1 is negative, could you please provide a reason.
3.If you are not able to support the individual with submitting a reconsideration request, do you routinely signpost them to other organisations?
4.Can you provide the number of reconsiderations requests you have submitted for the year 2023 and 2024? Could you please provide this data breakdown by year?

CRU Advice

Thank you to those forces who have shared feedback.

From the feedback received thus far – Questions 1,2 and 3 are "No Information Held". The applicant is asking general questions, but the answers will not be found within information held in a record form.

To explain that further, s84 of FOIA relates to recorded information held by a public authority and that it does not extend to providing explanations unless the answers are already held in a recorded form.

"*Information is defined in section 84 of the Act as 'information recorded in any form'. The Act therefore only extends to requests for recorded information. It does not require public authorities to answer questions generally; only if they already hold the answers in recorded form. The Act does not extend to requests for information about policies or their implementation, or the merits or demerits of any proposal or action - unless, of course, the answer to any such request is already held in recorded form." (Day vs ICO & DWP – EA/2006/0069 Final Decision)*

Instead, I note that some forces have provided local knowledge-based responses from their business areas. Whilst this may be helpful for the applicant, we advise caution on providing information outside of the Act unless it is harmless to do so. As such, please ensure that your business areas are signing off any knowledge based responses beforehand.

For Q4 - subject to any s40(2) concerns, we see no harm in providing a number, if held.

Kind regards,

S.40(2)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)

From: NPCC CRU Mailbox
To: S.31(1) [redacted]
Subject: Log No.131/25 - Items purchased with £500 to officers - CRU Circulation (01/03/2025) - Including Advice
Date: 03 March 2025 14:15:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU today. Advice is at the end of the message.

Log Number: 131/25
Case worker: S.40(2) [redacted]
Logged with: PSNI

Applicants Request:

1 - A list of all items bought by officers and police staff which were claimed under the Universal Offer of £500 to each officer/staff member to provide security and reassurances to them and their families following the 2023 data breach.

2 - The total cost of all items bought by officers and police staff which were claimed under the Universal Offer of £500 to each officer/ staff member to provide security and reassurances to them and their families following the 2023 data breach.

Note: for clarity the universal offer I am referring too is in reference to a statement issued by Deputy Chief Constable Bobby Singleton in a media statement issued on Saturday 1st February 2025.

***Force Comments**:*

We would be grateful for views on release of data for Q1. Data is held but could in our opinion meet section 38. Plus requires review of 20k lines of items to asses individual harm.

CRU Advice:

Thank you for your comments. We agree in principle with your consideration of s38 for question 1. In this instance, the offer of £500 was made to help secure the safety of officers in the wake of the data breach which occurred. Depending upon what has been purchased, identifying unique or specialist purchases could, by extension, expose specific plans which have been put in place by individuals to protect themselves from physical harm. Whilst it would be a generic list of procurements, which on the face of it carries a lower risk of identifying who had made them, there may be some very specific purchases made which, if disclosed, could be used on its own or in conjunction with other known information to place an individual's safety at risk. In those circumstances, those purchases would require redaction, and s38(1) would be the relevant exemption to rely upon.

As I am sure you are aware, blanket exemptions are not accepted by the ICO, so it would not be advised to consider applying s38(1) to all the information in a blanket fashion. Instead, a review of all the information must be undertaken to assess where any harm was realised and redact only that information. This brings me onto the 20k lines of items which require assessment. This is clearly an high volume of information which require review in order to establish harm. It may therefore be that you need to consider if doing so, i.e. reviewing and preparing the information for release would present an unreasonable burden to the force. If so, s14 is of relevance.

As you are likely aware, s14 does not work to the same '18 hours of work' rule as s12; it is instead for practitioners to determine case by case whether or not, based on what needs to be done to prepare the material for release (in this case to identify whether any one of the 20,000 lines contains information which would risk the safety of an individual) it would take so long that, even factoring in any public interest in the information being made available, the amount of work required to review, redact and prepare the information would present an unreasonable burden to the force. The ICO provide guidance on single burdensome requests here, which offers a good guide for practitioners in deciding whether s14 is appropriate, we direct you to that in the first instance. In essence, it describes the main points to consider as:

- the requester has asked for a substantial volume of information; ***and***
- you have real concerns about potentially exempt information, which you are able to substantiate, if asked to do so by the ICO; ***and***
- you cannot easily isolate any potentially exempt information because it is scattered throughout the requested material.

If you have to manually review 20,000 records, have real concerns that exempt information would be contained within those lines and that release of any such information would cause real and actual harm to individuals, and finally that there would be no tangible way to identify that material in any way other than a manual review of each line individually, then the above points would be met and s14 would appear to be a realistic option.

Be advised that public interest needs to be factored into any decisions taken to apply s14 and it should be mentioned that this has been considered in any rationale you provide in your response – albeit a specific public interest test does not need to documented. In some exceptional cases, regardless of how long it would take to complete the work required, the public interest favouring disclosure of requested material is so substantial that it outweighs any burden that may be placed on a PA. It is, as I said, a matter for practitioners to decide, but we do not believe any such level of public interest exists in respect of this request.

At this stage therefore, our thoughts are that s14 would be the first consideration. Whether you proceed with that is ultimately your call based on whether you are satisfied that, if challenged, you could sufficiently support your standpoint. If you do not feel that is the case, then the material held will require full review and relevant redaction under s38(1).

-
Kind regards

S.40(2)
[redacted]
National Freedom of Information Referral Officer
National Police FOI & DP Central Referral Unit (NPFDU)

National Police Chiefs' Council

NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]
[redacted]

-

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No. 137/25 - Ghost Guns/3D printed firearms - CRU Circulation (06/03/2025) - Including Advice
Date: 18 March 2025 14:33:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU today. Advice is at the end of the message.

Log Number: 137/25
Case worker: S.40(2) [redacted]
Logged with: National

Applicants request:

How many so-called ghost guns have you seized in 2025, 2024, 2023, 2022, 2021, 2020 and 2019?

How many 3D printed guns have you seized in 2025, 2024, 2023, 2022, 2021, 2020 and 2019?

How many components of ghost guns and 3D printed guns have you seized in 2025, 2024, 2023, 2022, 2021, 2020 and 2019?

How many incidents have you recorded involving ghost guns or 3D printed guns in 2025, 2024, 2023, 2022, 2021, 2020 and 2019? (Please give details of any incidents)

How many 3D printed weapons of any type have you seized in 2025, 2024, 2023, 2022, 2021, 2020 and 2019?

CRU Advice:

As with any request, the first consideration should be cost. In this case, if to even establish that information is held for this request would exceed cost, then s12(2) can be cited. As the request will otherwise be an NCND, s12(1) should not be relied upon as to do so effectively confirms

information is held. If s12(2) is not relevant then the following advice applies:

The national position on 3D printed firearms remains that an NCND approach is required by virtue of s23(5), s24(2) and s31(3).

Regarding ghost guns, we have consulted with the national policing lead for firearms as we are not aware a request of this nature has been received before. A ghost gun is, in essence, a homemade gun. The firearms lead has confirmed that the risks in confirmation or denial are the same for these types of weapons as for 3D printed firearms and thus the same NCND approach is required.

Regarding the final question, the number of seized 3D printed weapons of any type is requested. No definition of a weapon is provided, and while there are some obvious examples of what constitutes a weapon (knives, hammers, firearms etc.) by definition it can be anything which inflicts harm upon a person, making the question very broad.

Our advice is that this question will be captured under the NCND s23(5), s24(2) and s31(3). We have considered the fact that the request does not ask for any breakdown by weapon type, and only asks for a number. However, it is specific to 3D printed weapons, and numbers for that are likely to be low or zero. In cases where it is zero a NIH response would be required. It is the potential for a NIH response by some, while others may disclose information as held, that presents risk (in line with the harm cited for 3D printed firearms) from the perspective of revealing force intelligence and investigative focus on the seizure of these niche types of weapons.

Below is a form of words which is relevant to 3D printed firearms, while this will require slight amendment to make it case and force specific, the harm is fundamentally the same for all 3D printed weapons and therefore applies to this request.

In summary our advice is that if the request is not a s12(2), then a full NCND for the whole request is required by virtue of s23(5), s24(2) and s31(3).

S.31(1) **If you have taken, or are planning to take any other position, please notify the CRU and provide a copy of your draft response to us.**

Form of words:

Evidence of Harm:

Confirmation or denial that information is held would identify local level activity regarding the use and/or seizure of 3D printed weapons. In turn this risks identifying the level of police awareness of such weapons in the force area. When the request is made to multiple forces, there is a further risk in that confirmation or denial would reveal information which could be used to build a picture as to where national and local investigations and operations are taking place, and perhaps more pertinently where they are not, to combat the supply, distribution and use of these weapons. This mapping effect, created by forces either confirming information is held and citing a substantive exemption or, conversely, stating 'no information held', would undermine the effective delivery of operational law enforcement by revealing the intelligence picture of the force in respect of 3D printed firearms as well as compromising potentially

ongoing investigations, some of which may be covert.

Disclosure of information under the Freedom of Information Act 2000 (FOIA) is considered a release to the world at large and not a private transaction. Whilst not questioning an applicant's motives in this case, by making a public disclosure under FOI, it must be considered that as well as members of the public, criminals, including terrorists will be able to access the data released. It is widely known that organised criminal gangs and those involved in terrorist related activity monitor FOI disclosures closely for any information they can use to further their criminal activity.

The threat from terrorism cannot be ignored. It should be recognised that the international security landscape is increasingly complex and unpredictable. The UK faces a sustained threat from violent terrorists and extremists. Since 2006, the UK Government have published the threat level, based upon current intelligence that threat level to the UK currently is 'substantial, meaning an attack is likely.

https://www.mi5.gov.uk/threat-levels

Any information identifying the focus of policing activity that could be used to the advantage of criminal organisations, serious and organised crime groups and terrorists to undermine the operational integrity of policing will adversely affect public safety and have a negative impact on, not only law enforcement at a local level, but policing and operations at a national level the impact of which risks the national security of the UK.

Public Interest Considerations

Section 24 (2) National Security

Factors favouring complying with Section 1(1)(a)

Any information that would increase public knowledge in showing how resources are allocated in response to events would favour disclosure. This would also support the fundamental purpose of the Freedom of Information Act, which is to be more open and transparent in the way in which the police perform, making them more accountable for their actions. Releasing any details regarding the seizure of 3D printed firearms would provide reassurance to the public that the police are appropriately resourced in this area and would be in a position to respond to any National Security threats or incidents. Any information which would allow for more accurate public debate would be a positive factor for disclosure.

Factors against complying with Section 1(1)(a)

Whilst there is a public interest in providing reassurance that the police are appropriately and effectively dealing with threats posed by terrorist organisations, there is a strong public interest in safeguarding national security and the welfare and safety of the general public. Any disclosure (including confirming or denying information is held) has the potential to undermine ongoing and future operations to protect the Security of the United Kingdom, e.g. counter terrorism activity. The risk of significant harm or even death to the community at large would be increased.

The cumulative effect of terrorists gathering information from various sources would build a

picture of potential vulnerabilities at a local level. The more information disclosed over time will provide a more detailed account of the investigative focus of not only a force area but also the country as a whole. Any incident which results from such a disclosure would by default affect National Security.

Section 31(3) Law Enforcement

Factors favouring complying with Section 1(1)(a)

There is media reporting concerning the increase of these weapons, 3D guns appearing on British Streets which in itself is a factor supporting confirmation or denial.

To confirm or deny that this information is held would make members of the public more aware of the threat of certain offences and the forces ability to deal with them. Improved public awareness may lead to more intelligence being submitted to police about possible further instances of 3D- printed firearms use and any acts of criminality or perceived terrorism as members of the public will be more observant to suspicious activity which in turn may result in a reduction of crime.

Factors against complying with Section 1(1)(a)

To confirm or deny that the requested information is held could compromise law enforcement tactics which would hinder the Police force's ability to prevent and detect crimes. Whilst such information on its own may be perceived as not harmful, any further information that may be already in the public domain or any that may be asked for in the future could be detrimental to forces and can contribute to the mosaic effect. The 'mosaic' effect is attune to the building up of a jigsaw, from public disclosures and other information, gradually filling in the pieces to form a complete picture. For criminals, including serious and organised crime groups and terrorists to gain easy access to such information would not only undermine the police's primary function of law enforcement but also place the public at significant risk of harm.

Balancing Test

To confirm or deny that any such information is held or not held would indicate levels of policing activity at force level which could allow individuals to evaluate levels of activity across individual force areas and exploit what may be considered as less active or resourced areas. If this information is disclosed it continually drip feeds in the pool of information publically available to criminals and terrorists who will use it to complete a full picture on how and where to undertake their criminal pursuits without fear of detection or apprehension.

The security of the country is of paramount importance. The police will not divulge any information that would place the safety of officers or the public at risk or undermine national security. Whilst there is a public interest in the transparency of policing, and in this case providing assurance that the police service is appropriately and effectively engaging with the threat of activity involving weapons, there is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations. It is not in the best interests of the security of the country, individual forces or the public in general to put such information into the public arena where it could be used by those wishing to cause harm. It is

our opinion that for these issues the balancing test for confirming or denying that this information is held, not made out.

No inference can be taken from this refusal that information does or does not exist.
Kind regards

S.40(2)
[redacted]
National Freedom of Information Referral Officer
National Police FOI & DP Central Referral Unit (NPFDU)
National Police Chiefs' Council

NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]
[redacted]

-

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No.140/25 CRU Circulation (28/02/2025) - Including Advice
Date: 28 February 2025 16:00:00
Attachments: image001.png
image002.png

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU. Advice is at the end of the message.

Log Number:140/25
Case worker: S.40(2) [redacted]
Logged with: National

Applicants Request:

Please provide me with the following information on web traffic data to the following domains from devices used by all members of staff within your constabulary.

- chat.deepseek.com
- deepseek.com

Please provide the number of visits to each domain from January 20th, 2025, until February 6th, 2025.

Clarification to some forces:

Regarding my recent FOI requesting web traffic data on Deepseek usage, please accept my request for adjustment.

Instead of a single figure for the time period, please provide daily figures for web traffic within the date range (20-01-2025 until 06-02-2025).

CRU Advice:

Advice is provided on the assumption the information can be retrieved within cost limits. If s12 is applicable there is no harm in responding as such.

This request is asking for the number of visits your force has made to 2 named websites, over a set period of time, and for some forces broken down into a daily figure. The websites concerned are both 'large language models' originating in China, offering similar services as other AI language models such as ChatGPT.

There are open source media articles that discuss the somewhat controversial release of Deepseeks AI model What is DeepSeek - and why is everyone talking about it? - BBC News. Regardless, this request is asking only for the number of visits and assuming your force has not identified any reason to prevent visits to the site or restrict access, we can see no immediate harm in providing the figures or confirming NIH.

S.31(1) [redacted]

Kind regards

S.40(2) [redacted]
Deputy Manager
National Police Freedom of Information and Data Protection Unit (NPFDU)
National Police Chiefs' Council

,NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.40(2), S.31(1) [redacted]

-

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Log No.157/25 CRU Circulation (21/03/2025) - Including Advice
Date: 25 March 2025 10:08:00
Attachments: image001.png
image002.png
Update to - RE Log No.99524 CRU Circulation (12112024) - - Palantir - OS.msg

---

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Please see below advice in relation to the following:

Log Number:157/25
Logged with: National

Applicants Request

I'm seeking copies of any and all of the following documents in relation to your organisation's use of services provided by Palantir Technologies UK Ltd.

A list of current and past contracts, with start and end dates (where applicable) Any and all Data Processing Arrangements Any and all Data Sharing Agreements Any and all Data Protection Impact Assessments

I note that many UK police forces have previously declined to confirm or deny the existence of information relating to Palantir. However, police forces including Bedfordshire and Leicestershire have since publicly confirmed using the company's services, setting a precedent for disclosure.

Additionally, Palantir is a well-known provider of products that rely on artificial intelligence. The NPCC's Covenant for Using Artificial Intelligence in Policing, endorsed by all UK police forces, states that "all use of AI will be subject to 'Maximum Transparency by Default'".

CRU Advice

Practitioners may recall the advice to maintain NCND for CRU 995/24 (attached). The same advice is still in play now.

In short, it is the need for consistency in response as to when FOI is used to work out exactly what products or tools are being used, and by which forces.

Kind regards,

S.40(2)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: Update to - RE: Log No.995/24 CRU Circulation (12/11/2024) - - Palantir - OS
Date: 09 December 2024 14:44:00
Attachments: image001.png
image002.png
IR Advice Log No.00175022 CRU Circulation (29112022) .msg

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

Apologies for having to wait and chase on this one. The decision taken is to continue the stance previously given in 2022 which we also held at IR stage (CRU 1750/22 – S.40(2) refers). Whilst applicant and motive blind I think it is reasonable to suggest that S.31(1) [redacted]

In brief, the continued approach is :

- if your force has placed a formal disclosure regarding the use of Palantir technology into the public domain then you can confirm information is held and exempt it via s21, providing a link to the information in the public domain. A partial NCND s31(3) and s24(2) will also be required for any information that may or may not be held in relation to Palantir software used for covert purposes..
- If your force has not formally acknowledged use of Palantir software then a full NCND is required via s31(3) and s24(2).

I have attached the previous advice and IR advice for 1750/22 which gives further explanation as to the rationale for the decision.

In addition, a form of words kindly supplied by the MPS is below to assist. Reference to the MPS needs to be removed and replaced accordingly.

Section 24(2) National Security and Section 31(3) Law Enforcement

Section 1 of the Act places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is

held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of the Act requires that we provide the applicant with a notice which: a) states that fact; b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption(s) apply.

The MPS needs to be alert to requests for certain types of information, and there is a need for consistency when neither confirming nor denying whether information is held in order to protect policing information.

Factors in favour of disclosure:

Confirming or denying whether the requested information is held would enable the public to have a better understanding of the type of policing tools and tactics employed by the MPS in carrying out their law enforcement role. This would give more confidence to the public that we are using (or, as the case may be, not using) policing tools and tactics to help us detect and prevent crime appropriately.

Factors against disclosure:

To confirm or deny whether any other information relating to the use of a particular investigative tool is held would harm the integrity of sensitive policing tactics used to prevent and detect crime and safeguard national security.

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying if a particular policing tool of this type (in this case Palantir Technologies) is used by the Met as part of an investigative process is different from confirming if, in principle, commercial tools generally are used to assist with searches against information that may be found online.

It is well established that police forces use publically available data in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means. However, given the sensitive areas in which tools of this type may be used and the Met's role in counter-terror investigations, to disclose if any particular tools are used would allow criminals and other adversaries to focus on evaluating the particular capabilities of a particular tool, With this knowledge it would allow criminals and other adversaries to take steps to counteract a specific tool – be it adjusting how they interact and present themselves to take advantage of any weaknesses or gaps in capability they identify. At a simple level, if a policing tool doesn't search 'X 'social media site or was unable to identify 'Y' format of images and criminals can establish this, they will exploit this position. The Met's more sophisticated adversaries may be able to go further and take more proactive measures to undermine the tool and/or its provider, and a specific confirmation allows efforts to be focused accordingly.

This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tools are or are not deployed. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police

tactics, operations and future prosecutions as criminals could counteract the measures used against them.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

Balancing test

Accordingly, in a position taken in common with other law enforcement agencies, confirming or denying if the Met uses Palantir Technologies would lead to an increase of harm to covert investigations and compromise law enforcement. This outweighs the benefits to disclosure, not least as disclosure would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public. Therefore it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

If it exists, the disclosure of this information to the public by the MPS would undermine the integrity of police investigations and operations and in maintaining confidence in the MPS.

The effective delivery of operational law enforcement is of paramount importance to the MPS in their duty to ensure that the prevention and detection of crime is carried out and the effective apprehension or prosecution of offenders is maintained.
Therefore it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

Kind regards,

S.40(2)
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1)

From: NPCC CRU Mailbox
Bcc: S.40(2), S.31(1) [redacted]
Subject: IR Advice Log No.001750/22 CRU Circulation (29/11/2022)
Date: 21 December 2022 09:31:00
Attachments: image009.jpg
image001.png
image004.jpg
image005.jpg

Good morning

Many forces have received an internal review request for this national FOI with regards to the use of Palantir software. The original advice is shown at the bottom of this email which we continue to standby. The IR grounds are provided by the requestor are:

S.40(2) [redacted]

S.40(2) [redacted]

The National Policing Lead guidance is that 'We do not confirm or deny that particular software is used. This is on the basis that if this were to be disclosed it would provide those with malicious intent, information that could assist them in hacking into police systems, making forces more vulnerable, and thereby compromising effective delivery of operational law enforcement and national security.'

Whilst the public interest in openness and transparency is acknowledged, particularly in terms of maintaining the trust and confidence of the public whom the police serves, in respect of detailing particular software used by the police the public interest in maintaining the exemption from the duty to confirm or deny outweighs the public interest in confirming or denying. Operational policing relies heavily on information technology and is a crucial asset accorded the utmost protection. The benefit of maintaining the NCND principle as regards this and all similar requests submitted to police forces outweighs the benefit in confirming or denying the information requested by the requestor is held.

S.31(1) [redacted]

Therefore the continued approach is :

- if your force has placed a formal disclosure regarding the use of Palantir technology into the public domain then you can confirm information is held and exempt it via s21, providing a link to the information in the public domain. A partial NCND s31(3) and s24(2) will also be required for any information that may or may not be held in relation to Palantir software.

- If your force has not formally acknowledged use of Palantir software then a full NCND is required via s31(3) and s24(2).

I hope this is helpful, please make contact if you have any questions.

Regards

S.40(2)
[redacted] | National Police Freedom of Information and Data Protection Unit Manager | National Police Chief's Council
Telephone: S.40(2), S.31(1) [redacted]
Address: NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS

Subject: Log No.001750/22 CRU Circulation (29/11/2022) - Including Advice

OFFICIAL - SENSITIVE
POLICE EYES ONLY
Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Dear All,

The following FOI request has been logged in the CRU today - Please let us know if you have received it. Advice is at the end of the message.

Log Number:001750/22
Case worker: [redacted]
Logged with:Durham Constabulary
Sent from:Max Colbert

Applicants request:

Dear Durham Constabulary,

I'm writing to you under the Freedom of Information Act (2000) to ask that you please disclose to me if your constabulary has, at any point in the last 5 years, purchased or trialled software by Palantir Technologies, either direct from the government or crown commercial services, or via a third party entity (for instance, Capgemini).

i'll note that Palantir policing software is currently listed as able to purchase on the government webpage:

At this point there is a long link to a website which needs checking out by cyber security experts and should not be opened until declared safe.

and that previously the Police trialled them as far back as 2010 as part of a consortium agreement between Cheshire, Norfolk, Suffolk, the Met, and Northamptonshire as part of the Multi-Force Shared Services - which ran on a programme joint built by Oracle and Palantir on a software that was called (outside of the MFSS) T-Police - this software was purchased through Capgemini, and again the Met in 2012 used them during the London Olympics. The Met also trialled them between 2014-15 as one of three vendors providing "predictive policing" solutions, and as late as 2020 the force listed Palantir on it's ICT digital spend for "policing the capital".

So if their software in any capacity has been used by police from 2017 to present this is the

information I would like please.

CRU Advice:

We would initially like to draw forces attention to the link provided by the applicant and ensure they use discretion before opening the link by checking with their cyber security unit to ensure it is safe to open.

Thereafter, our advice in relation to this request is below:

We are aware that previous disclosures have been made by the MPS who trialled Palantir crime mapping products in 2016 - this is in the public domain so can be confirmed.
However, this request is in relation to any software purchased or trialled from Palantir via government or crown commercial services, or via a third party entity S.31(1) [redacted].

The applicant is asking if your force has purchased or trialled any software within the last 5 years, he has not asked for a breakdown of the software name, time period or what it is used for.
In this instance, if your force has placed a formal disclosure into the public domain (for example T-Police or crime mapping) then they can confirm information is held and exempt it via s21, providing a link to the information in the public domain.
A partial NCND s31(3) and s24(2) will also be required for any information that may or may not be held in relation to covert software.

For those forces who have not formally acknowledge use of Palantir software a full NCND is required via s31(3) and s24(2). See below for a form of words:

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying that any other information relating to the covert software and its uses would show criminals what the capacity, tactical abilities and capabilities of the force are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities.
Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of covert software would lead to an increase of harm to covert investigations and compromise law enforcement. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.
The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level, based upon current intelligence and that threat is currently categorised as SUBSTANTIAL.
The UK continues to face a sustained threat from violent extremists and terrorists. It is well established that police forces use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.
Confirming or denying whether any information is or isn't held relating to the covert software offered by specific companies would limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling offenders to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities. This detrimental

effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tactics are or are not deployed. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them. Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

Kind regards

S.40(2) [redacted]
Deputy Manager
National Police Freedom of Information and Data Protection Unit (NPFDU)
National Police Chiefs' Council
S.31(1) [redacted]
Address: NPFDU, c/o ACRO, PO BOX 481, PO14 9FS
S.40(2) [redacted]

From: NPCC CRU Mailbox
To: S.31(1) [redacted]
Subject: RE: OFFICIAL-SENSITIVE [CRIMINAL JUSTICE PARTNERS]: FW: FW: FW: [FOI/13882]
Date: 26 March 2025 11:28:00
Attachments: image001.png
image002.png

OFFICIAL – SENSITIVE

POLICE EYES ONLY

Not to be distributed outside of the Police network or other agencies without prior authorisation from the CRU

Good morning,

I believe your ref 13882 pertains to CRU 161/25, which is the following FOIR:

1. The number of current authorizations for directed surveillance or communications data acquisition targeting individuals identified as journalists or lawyers.
2. Any policies or guidelines in place regarding the approval process for surveillance operations involving journalists or lawyers.
3. The number of instances in the past 12 months where surveillance or communications data acquisition involving journalists or lawyers was considered but not authorized, if such records exist.
4. Any internal audits or reviews conducted in the past 24 months regarding the use of investigatory powers in relation to journalists or lawyers.
5. The total budget allocated for operations involving surveillance of journalists or lawyers in the current fiscal year, if such a specific budget exists.

Thank you for the notes on the referral, which are as follows:

Request numbers 1,2,4 are available in the publicly available information outlined below.
A report was published on the use of covert and investigatory powers by the PSNI in respect of journalists and lawyers (see Covert Powers Report | PSNI)
https://www.psni.police.uk/about-us/our-publications/covert-powers-report
The use of Covert Powers are governed by the Codes of Practice issued by the Secretary of State:

- **Communications Data Code of Practice (2018)**
- **Interception of Communications (2022)**
- **CHIS Code of Practice (2014)**
- **Covert Surveillance and Property Interference Code of Practice (2014)**
- **Interception of Communications Codes of Practice**
- **Equipment Interference Code of Practice (2016)**

There is also information on the McCullough Review commissioned by the Chief Constable available here The McCullough Review | McCullough Review
Q3 and 5 – is believed that confirming or denying of the information held would represent a significant risk to investigations, law enforcement activity and national security.
Additionally the information on statistics is held for future publication by the Investigatory Powers Commissioner in their annual report in an aggregated format across the UK.

CRU Advice

Q1 – I am not sure I agree that the information is already in the report. This request asks for the "current" number of authorisations, which I interpret as the number of live authorisations as per the date of the FOI request. On that basis, my initial view is that the response should be NCND s24(2), 30(3), 31(3) and 40(5).

Q2 – I agree that the report covers this at page 18 onwards – "Authorisation for Communications Data"

Q3 – I would welcome your views as to why Q3 attracts NCND? Alternatively, could this be a Cost refusal? I ask this as I am not sure why there would be a need to keep a central record of applications which didn't get authorised.

Q4 – As per your comments.

Q5 – Is a budget allocated as specific as this? Again, I welcome your views as to why NCND is being considered. Lastly, aggregated data for an annual report representing the Police Service as a whole doesn't appear relevant for this request, so I cannot advise on s22 consideration.

These are my initial thoughts and I welcome further discussion; perhaps over Teams if that is easier?

Kind regards,

S.40(2) [redacted]
Freedom of Information Referral Officer
National Police Freedom of Information and Data Protection Unit
National Police Chiefs Council
NPFDU PO Box 481, Fareham, Hampshire. PO14 9FS
S.31(1) [redacted]
[redacted]