IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Advisory Notice 1/2023

Oversight of the UK-US Data Access Agreement

Published: 13 FEB 2023
Version: 1.0

A. Introduction

1. This Advisory Notice is made and published by the Investigatory Powers Commissioner pursuant to s.232(2) Investigatory Powers Act 2016. Its purpose is to provide advice and information to public authorities and to the general public as to the approach that Judicial Commissioners and the Investigatory Powers Commissioner's Office will take to keep under review compliance by UK public authorities with the UK-US Data Access Agreement pursuant to s.229(3A) IPA, including the review function relating to relevant targeting decisions and relevant targeted communications data authorisations.

B. Interpretation

2. This Advisory Notice will adopt the following abbreviations:

   COPO – Crime (Overseas Production Orders) Act 2019.

   DAA – Data Access Agreement. The Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime.

IPA – Investigatory Powers Act 2016.

IPC – Investigatory Powers Commissioner.

IPCO – Investigatory Powers Commissioner's Office.

JC – Judicial Commissioner

Major modification – adding, varying or removing the name or description of a person, organisation or set of premises to which a warrant relates.

Minor modification – adding, varying or removing any factor specified in the warrant in accordance with s.31(8) IPA.

Relevant targeting decisions – decisions to target a new individual relating to a targeted interception warrant. These are either:

a. major modifications that add or describe a person, organisation or set of premises to which the warrant relates;
b. minor modifications falling within the descriptive subject matter that have the effect of identifying a person, organisation or set of premises falling within the description; or
c. a decision to target a new person, organisation or set of premises falling within the descriptive subject matter and factors provided by the warrant.

OCDA – Office for Communications Data Authorisations. Responsible for considering requests for TCD under powers delegated by the IPC.

Order - a legal instrument (e.g. a warrant, modification instrument or communications data authorisation) issued under the domestic law of the Issuing Party requiring the disclosure or production of data.

Parties – the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America.

TCD – Targeted Communications Data. Falling within Part 3 IPA.

UKDA – United Kingdom Designated Authority.

RA – Requesting Agency. The UK public authority requesting data under the DAA.

RPP – Receiving Party Person

C. Background

3. On 3 October 2019 the Governments of the United Kingdom of Great Britain and Northern Ireland and the United States of America signed the DAA. The DAA provides for direct requests to be made for data held by telecommunications providers in the other party's jurisdiction for the exclusive purpose of preventing, detecting, investigating, and prosecuting serious crimes, including terrorism.

4. There are no new powers required to give effect to the DAA. Requests to US telecommunication providers must be compliant with domestic law. This includes obtaining, as appropriate, either a targeted interception warrant, TCD authorisation, or an overseas production order for the data being sought.

5. IPCO has a statutory function to oversee the UK's use of the DAA, including where the Crime (Overseas Production Orders) Act 2019 is being used.

D. The Legal Framework for Oversight

6. Article 5(2) of the DAA requires that "*Orders subject to this Agreement shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate or other independent authority prior to, or in proceedings regarding, enforcement of the Order*". IPCO is one of the independent authorities providing this review and oversight function.

7. This function is set out in s.229(3A) IPA, which provides that "*The Investigatory Powers Commissioner must, in accordance with the Agreement between the Government of the United Kingdom and the Government of the United States of America on access to electronic data for the purpose of countering serious crime dated 3rd October 2019, keep under review the compliance by public authorities with the terms of that Agreement.*".[1]

8. The review and oversight function is discharged by providing an audit of the use of the DAA by public authorities and an additional review in cases relating to:

    a. relevant targeting decisions; and

    b. TCD authorisations which have been authorised internally by the applicant authority.

9. The DAA sets out the mandatory targeting, minimisation and processing restrictions and requirements in relation to the electronic data. The Home Secretary is accountable for UK compliance. Therefore, the Home Office, as required by the DAA, has set up the UKDA to, among other things, review and certify for compliance a public authority's DAA requests. The IPC's functions under s.229(3A) IPA will provide further independent assurance as to public authorities' compliance and s.235 IPA provides the powers required for IPCO to investigate, inspect and audit as appropriate.

10. The DAA also provides that Orders subject to the DAA must be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of a Covered Offence. Article 1(5) DAA states:

    "Covered Offense means conduct that, under the law of the Issuing Party, constitutes a Serious Crime, including terrorist activity."

[1] s.229(3A) IPA was inserted by the Functions of the Investigatory Powers Commissioner (Oversight of the Data Access Agreement between the United Kingdom and the United States of America and of Functions Exercisable Under the Crime (Overseas Production Orders) Act 2019) Regulations 2020

11. Serious Crime is defined as *"an offense that is punishable by a maximum term of imprisonment of at least three years"* (Article 1(14) DAA). For the UK, this includes the definition of crime as set out in s263(1) IPA:

    "crime" means conduct which -
    (a) constitutes one or more criminal offences, or
    (b) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences

12. The domestic statutory purpose of an Order need not necessarily be that of "serious crime" and could, for example, be that of "national security" so long as the data sought is for the purpose of the prevention, detection, investigation, or prosecution of a "Covered Offense".

E. Additional Review - The Judicial Commissioner Role

13. Where a warrant naming an individual has been approved by a JC, under the terms of the IPA, that targeting will already be compliant with Article 5(2) DAA without any additional process. However, use of a general descriptor or class of persons in a thematic warrant would permit the targeting of a new person, organisation, or set of premises falling within that class without further JC approval being required. To ensure UK targeted interception warrants remain compliant with the Parties' interpretation of Article 5(2) DAA, the IPC's new statutory function will oblige a JC to review the necessity and proportionality statements for a relevant targeting decision when an individual is targeted for the first time under a warrant, including if IPCO has reviewed the decision to target that individual under a different warrant or previous TCD authorisation.

14. The review of any relevant targeting decisions and TCD authorisations must occur as soon as reasonably practicable. RAs should therefore submit these to a JC as soon as reasonably practicable after the internal authorisation is granted. A JC will review these as soon as reasonably practicable. If a JC, in effect, 'refuses' the application or submission, the collection of the data must cease, and any data already received must be destroyed.

15. When reviewing relevant targeting decisions or TCD authorisations the RA must provide the JC with the case for having made their decision. A JC will consider the facts and the necessity and proportionality of the activity. Where possible, the JC will also consider specific DAA compliance issues such as whether the acquisition of data relates to a "Covered Offense". The JC will scrutinise the Order requiring additional review. If the JC has any objections, these will be communicated to the RA.

16. For relevant targeting decisions made by way of minor modification, the RA must provide the JC with the application for an authorised minor modification. The modification application should state the authorised subject matter as set out in s.17 IPA and provide the information as required by s.31 IPA for the original targeted interception warrant. (This is to enable the JC to consider whether the modification falls within that permitted by the warrant). Applications for all relevant targeting decisions must include a necessity and proportionality justification. A similar process will be followed for relevant targeting decisions made by way of major modification which (unlike minor modifications) are already required to be notified to IPCO under the IPA.

17. The application detailing the relevant targeting decision or TCD authorisation should stand on its own without the need for a JC to cross reference other material, such as the associated warrant. However, IPCO may request that an RA provides the original warrant and any renewal instrument with the approval request. This will be based on the level of detail included within the modification application or submission. JCs reserve the right to request sight of any document they consider necessary in order to discharge their function to review a relevant targeting decision.

18. When reviewing the necessity and proportionality case, JCs will be guided by Advisory Notice 1/2018 as to the approach they will adopt.[2] At this stage JCs will not be assessing compliance with the targeting requirements of the DAA,[3] including whether an RPP has been intentionally targeted. This is because the UKDA's processes in certifying a request for data under the DAA should be sufficient to secure compliance in this regard. IPCO will oversee this through its inspection of public authorities and will notify the UKDA should it discover any issues of concern.

19. A public authority must respond to any request for further information as soon as reasonably practicable. It is the IPC's expectation that, if a JC objects to (i.e. in effect, 'refuses') a relevant targeting decision or TCD authorisation as a result of the additional review, a public authority will act expeditiously to cease collection and delete any product obtained. There is no route of appeal to the IPC following an objection.

F. IPCO Inspection/Audit

20. All UK Issuing Parties are in scope for inspection and audit. This includes public authorities that utilise COPO and the intercepting authorities set out in s.18 IPA.

21. IPCO will determine its review period for inspection and audit. Inspections and audits will take place at least annually. Public authorities that have requested, received, processed and/or disseminated DAA data within that review period will be inspected and audited by IPCO.[4] In addition, IPCO may inspect and audit the UKDA's role where relevant to the compliance with the DAA.

22. IPCO will inspect and audit the UK Issuing Parties against the relevant Home Office DAA policies (which includes the targeting and minimisation procedures that have been approved by the US Department of Justice) and agreed interpretation of the DAA by the Parties. For clarity, IPCO inspections and audits do not remove the need for RAs to have their own internal monitoring controls to ensure compliance.

23. IPCO will decide the focus of any audit. Initial focus will be on establishing individual public authority compliance with the DAA and standalone audits will be carried out. However, the intention is to incorporate the inspection and audit into IPCO's regular interception and TCD inspections. From time-to-time IPCO may also decide to undertake cross-cutting audits focusing on a particular aspect of the DAA or common concern across multiple public authorities.

[2] Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners.
[3] Articles 4 and 7.
[4] Unminimised data means data which has not been processed to apply the minimisation procedures required by Article 7 DAA.

24. Inspections and audits will aim to establish if the controls and governance put in place by public authorities are sufficient to provide assurance that they are operating in compliance with the terms of the DAA.

25. IPCO will also inspect and audit DAA compliance with overseas production orders issued under COPO. However, the IPC will not keep under review the exercise of any function by a judicial authority. IPCO will therefore not review the decision of a judge to issue an overseas production order but may review the veracity of the information presented to the judge and whether any product obtained is consistent with the terms of the Order and the DAA.

26. Audits will examine relevant records, systems and policies that are held or used by the RAs and UKDA. IPCO staff and JCs may also speak with individuals involved in the process to test that the controls and governance in place are compliant with the DAA. Where necessary, the IPC will liaise with US Covered Providers or other non-UK parties to establish compliance, investigate any breach, or address any concern.

27. RAs are expected to keep sufficient records that cover the following:

    a. DAA requests;
    b. Pre and post targeting checks;
    c. DAA acquired data;
    d. Minimisation and dissemination of DAA data
    e. System configuration and specifications;
    f. Directive controls documentation, such as training syllabus, attendance, guidance and policies;
    g. Monitoring controls – internal audit methodology and results;
    h. Governance arrangements – structures and meeting notes.

28. IPCO will keep public authorities' DAA tasking under review to assure it relates only to activity that can legitimately be authorised for DAA use (e.g. a "Covered Offense" as explained in paragraphs 10 and 11 above).

29. The UKDA is responsible for providing compliance certification information to the IPC. It is also responsible for the collection, collation and validation of the statistical information required by the IPC.

30. IPCO staff and JCs undertaking inspections and audits will require access to the systems used to request and process DAA data and to the individuals who perform any role within that process.

31. IPCO will produce a report for each inspection and audit undertaken. A summary of findings for the period under review will also be published in IPCO's annual report. The UKDA is responsible for sharing the annual report with the USDA. [5]

32. When undertaking and reporting on inspections and audits, IPCO will comply with s.229(6) IPA. This means that IPCO will not act in a way which the Commissioner considers to be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime or the economic well-being of the UK. All records and reports will be handled at the appropriate Government Security Classification.

[5] This is a requirement under article 12(4) DAA.

G. Breaches

33. Breaches of the DAA have been defined by the Parties as:

    a. **Reportable breach** – conduct amounting to the unauthorised intrusion into the privacy of an individual or entity (including RPP), whether knowingly made or through incorrect application of the [targeting and minimisation] procedures, or which represents a systematic weakness in process, procedure or supporting technology. Reportable breaches are notified to the IPC in order to facilitate any necessary inquiries and for any remedial action to prevent similar breaches in the future.

    b. **Recordable breach** – conduct amounting to a breach of the [DAA] that occurs despite the application of appropriate policy and procedures, or which occurs as a result of a change in circumstances, for instance, a targeted non-RPP who travels to the United States. Recordable breaches of the [DAA] will be documented and made available for audit by IPCO at their regular inspections.

34. RAs are responsible for notifying the IPC of any reportable and recordable breaches. These will be reviewed during inspection and audit of the relevant public authority. The IPC may also decide to undertake an investigation into the circumstances of individual breaches that are of particular concern.

35. These definitions of breaches under the DAA are in addition to the relevant error regime under the IPA which will also apply and which IPCO will continue to inspect. This means a particular breach could be both a breach of the DAA and an error under the IPA.