nafn gov.uk
Data & Intelligence Services

IPA
Investigatory Powers Act
for Communications Data

GENERAL AWARENESS BRIEFING

Issue 1
June 2019

Contents

Introduction

Wendy Poole
Chair

Mark Astley
Head of Service

Dear Colleagues

Criminal and fraud investigatory work is a hugely rewarding profession, with the capacity to have significant impact on the lives of others, managing risk and making decisions that affect people on a daily basis. As practitioners you are entrusted with powers which enable you to perform your jobs, and with those powers come both responsibility and accountability.

Changes in technology, criminal behaviour and the tools available to assist you to do your job have required changes in the law, and the Investigatory Powers Act 2016 has brought legislation in this area not just up-to-date but ready for the digital future to come.

We want to support you by providing clarity on the legislative context for investigatory powers to help you make better decisions and play your part in ensuring investigations are a success.

This briefing pack will allow you to familiarise yourself with the changes the IPA will bring overall and summarises the key changes across communications data capabilities.

This document contains a summary of capability changes, as well as guidance, standardisation and consistency for the Communications Data application process appropriate to the relevant roles.

INVESTIGATORY POWERS ACT 2016 OVERVIEW

WHAT IS IT?

The Investigatory Powers Act (IPA) governs how we use the investigatory powers available to us. These powers provide for the lawful acquisition of communications data including the who, where, when, how and with whom of a communication but not the content (i.e. what was said).

The IPA is world leading legislation that provides unprecedented transparency and substantial privacy protection. It transforms the law dealing with investigatory powers, strengthening safeguards and introducing oversight arrangements.

The IPA brings together all of the powers already available to law enforcement, the security and intelligence agencies (SIAs) and wider public authorities (WPAs) to obtain communications and data about communications.

The IPA creates a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.

WHY NOW?

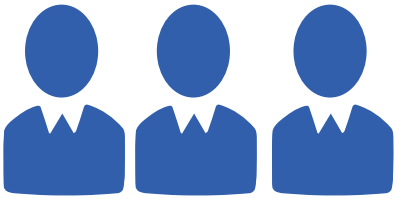
The Act builds on the work of the comprehensive review carried out in 2015/16 by David Anderson QC, the then Independent Reviewer of Terrorism Legislation, the Intelligence and Security Committee of Parliament (ISC), and a panel convened by the Royal United Services Institute (RUSI). They made 198 recommendations between them.

The review agreed investigatory powers remain vital to law enforcement, SIAs and WPAs. Collectively, they proposed reforms to the way these powers are overseen and recommended the introduction of consistent safeguards and greater openness.

An explicit provision for the acquisition of Communications Data means public authorities can remain effective in the fight against crime.

THE IPA AIMS TO:

Better protect the public



Better protect those using investigatory powers and;

Increase public confidence in how public authorities use the investigatory powers available to them

THE CHALLENGE

Technology is increasingly embedded in our daily lives, changing the shape of society and the nature of the crimes we investigate.

7 years
AFTER RIPA received royal assent, the first iPhone was released.

Today over **4 billion** people are connected to the internet.

90% of data on the internet today has been created in the **last 2 years** and within **5** there will be over **50 billion** smart **connected devices**, all developed to collect, analyze and share data.

Communications technology has evolved rapidly over the last twenty years and the rate of change will only increase. That evolution has brought with it huge challenges for criminal and fraud investigations. The increasingly complex world of communications technology and the changing ways in which we communicate with each other, technologies cross communications platforms and geographical boundaries all make it more difficult for us to tackle the serious threats that we all face.

It can be easy to lose sight of why criminal and fraud investigations need to be able to use investigatory powers especially in the haze of negative publicity around, for example, the difficulties mistakes in their use can cause for real people, criticism of internal processes or the allegation that oversight is weak. But powers to acquire communications data, intercept communications and interfere with equipment are indispensable to us as we work to keep people safe across the United Kingdom every day.

60% of adults have multiple connected devices. On average we spend **6 hours per day** on the internet and over **2 hours** on social media.

95% of all **serious crime investigations** involves an element of communications data. Digital **data** is now **fundamental** to the prevention and **detection** of **crime**.

THE NEW LEGISLATION

UNPRECEDENTED TRANSPARENCY

- Ensuring effective regulation and world leading oversight;
- Being as clear as possible in the language it uses including definitions and terminology;
- Ensuring that law enforcement, SIAs and WPAs have access only to the powers they need to keep the country safe and prevent and detect crime.

SUBSTANTIAL PRIVACY PROTECTION

- Ensuring independent authorisation for the acquisition of the Communications Data with the setup of the new Office for Communications Data Authorisation (OCDA);
- Introducing protection for journalistic sources;
- Introducing new offences and penalties for misusing investigatory powers.

The Investigatory Powers Act commenced on 11 June 2019 and is now the main legislation governing communications data. This includes the acquisition of communications data by UK public authorities including law enforcement agencies, intelligence agencies, local authorities and wider public authorities. It brings the relevant powers together but does not fully replace pre-exisiting legislation - so care will need to be taken to ensure the correct legislative basis is used for operations, as the Investigatory Powers Act affects the way investigations are conducted.

The IPA does the following:

- Introduces a number of new offences. If you are using CD powers you must ensure you know what these offences are so that you can avoid acting unlawfully.
- Changes the way we use related powers in other legislation. If you use the wrong legislation the activity will not be authorised and the operation will be impacted.
- Introduces opportunities to improve decision-making and streamline processes, however, it also introduces a new, more robust oversight regime, which means that there will be greater external scrutiny of the use of these powers.

IMPACT ON OTHER LEGISLATION

The Investigatory Powers Act is not a like for like replacement for existing legislation - many aspects of those Acts remain in place. It does, however, change the way you use the powers covered in the Act including the acquisition of CD.

The Investigatory Powers Act is, therefore, your first point of reference for use of this power.

REMOVAL OF JUDICIAL APPROVAL FOR LOCAL AUTHORITIES

The introduction of the Office for Communications Data Authorisations (OCDA) means the acquisition of communications data by local authority officers is no longer subject to judicial approval by a magistrate or sheriff.

There is a requirement for a local authority making an application to ensure someone of at least the rank of the Service Manager is aware the application is being made before it is submitted to OCDA.

INVESTIGATORY POWERS COMMISSIONER'S OFFICE

The IPA introduces the powerful new role of the Investigatory Powers Commissioner (Lord Justice Fulford) who is heading up the new oversight regime, which will be delivered through the Investigatory Powers Commissioner's Office (IPCO). IPCO also oversees the use of investigatory powers in RIPA. IPCO's role covers:

- **Authorising and approving the use of investigatory powers.** In relation to communications data, Judicial Commissioners sitting within IPCO will typically have no involvement with applications. However, they are required to approve authorisations where the objective of the application is to identify or confirm the identity of a journalist's source.

- **Inspecting public authorities on their use of the powers.** This is done by a number of Subject Matter Experts (SME) Inspectors.

- **Informing Parliament and the public about the need for and use of powers.** This is mainly the responsibility of the Investigatory Powers Commissioner.

INTRODUCTION OF OCDA

The Office for Communications Data Authorisations (OCDA) is the first organisation of its kind in the world and commenced its operations in March 2019. OCDA assesses Communications Data applications from public authorities and will make decisions about those applications that strike a fine balance between protection of privacy and risk to public safety.

The rules around accessing Communications Data are tightly controlled. Under the Investigatory Powers Act, OCDA will be responsible for ensuring that any applications made by relevant authorities in the UK are assessed independently, rigorously and in line with newly strengthened legislation.

OCDA will act as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards, and challenging where required.

Local authorities must submit all their communication data applications, via, NAFN for the consideration of OCDA. All applications must be authorised by OCDA prior to any communications data being acquired on behalf of a Local Authority.

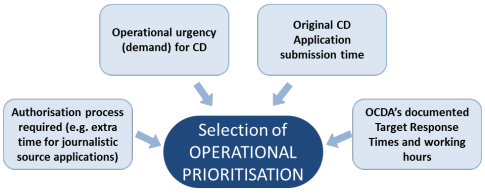
WORKING WITH OCDA

The SPOC role becomes more important with the introduction of independent authorisation. SPOCs are required to:

- Provide quality assurance checks to ensure that applications consistently comply with IPA standards and to a sufficient level to meet OCDA and IPCO scrutiny;
- Monitor those applications which are returned for rework or rejected by OCDA and determine the reasons why;
- Provide organisational and/or individual training as and where necessary sharing best practice advice and support;
- Be the point of contact between public authorities and OCDA; *(NOTE: Applicants will not be able to contact OCDA)*.

OPERATIONAL PRIORITISATION

To enable NAFN to convey to OCDA the operational urgency for the acquisition of data and ensure that it is appropriately triaged and handled to meet these demands, a new "Operational Prioritisation" has been introduced which is similar to Telecommunication Operator CDSG grades but allows a finer level of distinction between "Grade 3" applications.



SERVICE LEVEL EXPECTATIONS

OPERATIONAL PRIORITISATION	DEFINITION	SERVICE LEVEL EXPECTATION
PRIORITY 1 **IMMEDIATE THREAT TO LIFE OR SERIOUS HARM**	An immediate threat of loss or serious harm to human life including the wider statutory purposes outlined in Subsection 7 (c) of S 61A of the IP Act relating to the prevention of death of a person, the prevention of injury to a person, the prevention of damage to a person's physical health, the prevention of damage to a person's mental health and/or mitigating any injury or damage to a person's physical or mental health. This includes situations where a person (P) has died or is unable to identify themselves because of a physical or mental condition and there is an immediate need to identify the person 'P' or 'P's' next of kin or other person connected with 'P' or an immediate need to establish the reasons for 'P's' death or condition. Or a credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost. **[Equivalent to CDSG Grade 1. DO NOT submit to OCDA, internal authorisation under S61 or S61A only]** **NOTE: local authorities may NOT select Priority 1**	N/A Authorised by requesting Authority
PRIORITY 2 **URGENT OPERATIONAL NECESSITY**	An urgent operational requirement where the urgent acquisition of CD will directly assist the prevention or detection of the commission of a serious crime, or the making of arrests or the seizure of illicit material, or where that operational opportunity will be lost. Or any of the scenarios described for Priority 1 which whilst urgent do not require immediate action. **[Equivalent to CDSG Grade 2. Must be submitted to OCDA]**	Within 6 Working Hours
PRIORITY 3 **ROUTINE (TIME CONSTRAINT ON APPLICATION)**	Matters that are not urgent but include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early acquisition of CD will directly assist in the prevention or detection of that crime or safeguarding and preservation of human life. **[Equivalent to CDSG Grade 3. Must be submitted to OCDA]**	Within 1 Working Day (15 Working Hours)
PRIORITY 4 **ROUTINE**	Matters that support a specific line of investigation into a crime or incident but are not urgent and do not meet any time critical issues. The acquisition of communications data as a matter of course will assist in that investigation. **[Equivalent to CDSG Grade 3. Must be submitted to OCDA]**	Within 4 Working Days (60 Working Hours)

NOTE: Target Response Times are for early go-live and refinement is expected over time

IN SUMMARY

THE IPA

- Provides for the powers under which law enforcement, the security and intelligence agencies, local authorities and wider public authorities can acquire communications data.
- Replaces many of the provisions in RIPA 2000.
- Introduces a world-leading oversight regime with the creation of the Investigatory Powers Commissioner's Office and introduces additional safeguards for private information.

IT AIMS TO:

- Better protect the public;
- Better protect those using the investigatory powers and;
- Increase public confidence in how the public authorities use the investigatory powers available to them.

IT DOES THIS BY:

- Ensuring effective regulation and world-leading oversight - the IPA establishes the new Investigatory Powers Commissioner. The commissioner and their office will carry out a thorough and robust regime of inspections and thematic investigations;
- Being as clear as possible in the language it uses including definitions and terminology;
- Ensuring that public authorities have access only to the powers they need to keep the country safe and prevent and detect crime;
- Introducing enhanced protection for journalistic sources where CD applications must also be approved by a Judicial Commissioner before action may be taken;
- Introducing new offences and penalties for misusing investigatory powers.

IPA

Investigatory Powers Act for Communications Data

SUMMARY OF CHANGES - JUNE 2019

YOU NEED TO BE AWARE OF THE FOLLOWING CHANGES:

- New offences for unlawful acquisition and disclosure of CD; S11 and S82;
- Revised statutory purposes for the acquisition of CD (as per RIPA amendments November 2018);
- New terminology for CD; Entity Data and Events Data, Authorising Individuals and Designated Senior Officers;
- Judicial approval required for applications identifying or confirming the identity of a journalist's source;
- New option to seek guidance on novel or contentious circumstances;
- Public authorities required to retain OCDA decision documents;
- New statutory powers for the authorisation of CD application and Independent Authorisation; S60A, S61 and S61A;
- The requirement for public authorities to have emergency SPOC provision;
- Internet Connection Records;
- Serious crime definitions for the acquisition of Events Data;
- Ability to create CD applications for testing, maintaining or developing CD acquisition systems or capabilities;
- SROs required to review Excess Data from telecommunication operators where acquired.

COMMUNICATIONS DATA SUMMARY OF CHANGES

NEW OFFENCES

Unlawfully Obtaining Communications Data S11

This offence applies to anyone within a Public Authority. To be an offence, unlawfully obtaining or providing CD must be either done knowingly (i.e. acting voluntarily and intentionally) or recklessly (e.g. with obvious/foreseeable consequences).

Making an honest mistake is not an offence.

Telecommunications Operators (TO) Unlawful Disclosure S82

This offence applies to anyone working directly or indirectly for the TO and prohibits them from disclosing the existence of a CD request. It is incumbent on the Applicant to make clear whether or not disclosure is permitted, as disclosing with the permission of the relevant public authority is a reasonable excuse to this offence.

STATUTORY PURPOSES

The IPA has brought all the statutory purposes together in one place and the purposes under the IPA are largely the same as under RIPA albeit with some minor alterations. The available IPA Statutory Purposes are as follows:

- In the interests of national security;
- For the applicable crime purpose;
- In the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- In the interests of public safety;
- For the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- To assist investigations into alleged miscarriages of justice; and,
- Where a person ("P") has died or is unable to identify themselves because of a physical or mental condition to assist in identifying P, or to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

KEY NEW TERMINOLOGY: ENTITY AND EVENT

Under the IPA some definitions are different, there are new terms:

Under RIPA CD was broken down into three sub-categories: traffic data, service use information and subscriber information.

Any data falling outside these definitions was considered to be content. The Act updates the definition of communications data to provide for technologically neutral, modernised definitions:

ENTITY DATA	EVENTS DATA
• Entity Data' broadly replaces 'Subscriber Data' [RIPA, s 21(4)(c)]	• Events data identifies or describes events which consist of one or more entities engaging in an activity at a specific time or times.
	• Event Data refers to both Traffic Data (S.21(4)(a)) and Service Use Information (S.21(4)(b)) under RIPA.
	• Where the purpose of the acquisition is to prevent or detect crime, and the data required is events data, the offence or conduct of the offence being investigated must meet at least one of the definitions of serious crime.

JUDICIAL APPROVAL REQUIRED FOR APPLICATIONS RELATING TO JOURNALISTIC SOURCES

Where the purpose of a CD application is to identify a journalistic source, these must first be authorised by an OCDA Authorising Officer for local authorities or DSO for all other organisations but must also be approved by an IPCO Judicial Commissioner. The Applicant and SPOC should pay special consideration to these applications and inform their Senior Responsible Officer.

The IPA does not alter the existing processes for CD applications that may feature sensitive professions including medical doctors, lawyers, journalists, parliamentarians, or ministers of religion. If the CD could contain information relating to any of these professions this must be noted in the application.

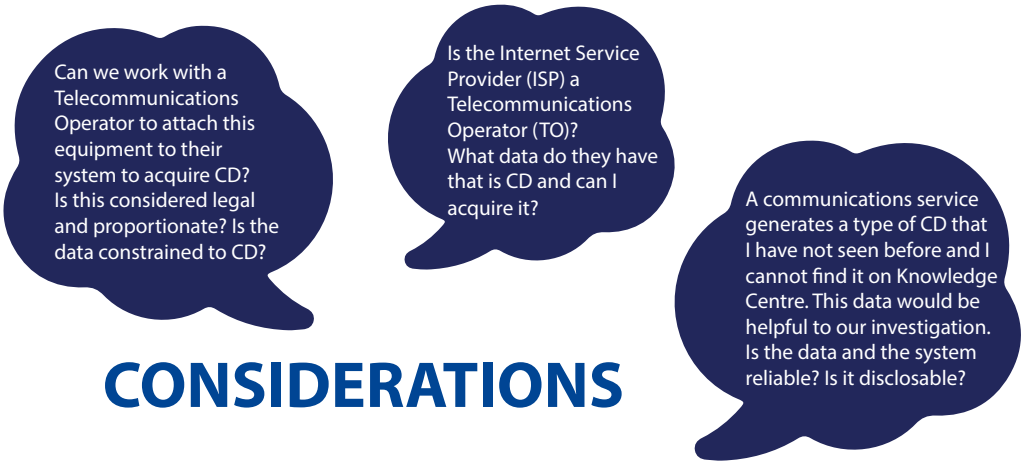
NOVEL AND CONTENTIOUS APPLICATIONS

As technology changes and as the sophistication of investigations increase, there will be circumstances where the potential acquisition of CD may be considered novel or contentious. The IPA provides the opportunity for public authorities to seek guidance ahead of progressing with any conduct to acquire CD although this is not mandatory. The decision to seek guidance is a matter for the Public Authority.

The Public Authority must ensure their Senior Responsible Officer is made aware and supports the course of action of the Public Authority. There are again considerations and processes that the SPOC must be aware of and familiar with which are documented in the next section. Refer to section 8.45 of the Code of Practice.

WHAT COULD BE NOVEL OR CONTENTIOUS? APPLICATIONS THAT REQUIRE:

1. Confirmation of the legal boundaries of CD acquisition as they stand; or
2. Where technology and acquisition techniques have evolved confirming where legal boundaries of CD acquisition lie.



PUBLIC AUTHORITIES REQUIRED TO RETAIN OCDA DECISION DOCUMENTS

OCDA will only retain for a limited period of time the CD applications which are sent to them and of Decision Documents that they issue back to public authorities. This is due to the degree of sensitivity and risk arising from the accumulation of these documents in a central database. Therefore, public authorities are required to keep records of both the CD applications that they issue as well as the decisions received from OCDA.

NEW STATUTORY POWERS FOR THE AUTHORISATION OF CD APPLICATIONS AND INDEPENDENT AUTHORISATION

Section 60A of the Act provides for the independent authorisation of communications data requests by the Investigatory Powers Commissioner (IPC). The Office for Communications Data Authorisations (OCDA) performs this function on behalf of the IPC. An authorising officer in OCDA can authorise any lawful request, for any of the specified purposes from any listed Public Authority. OCDA will not consider applications in 'Threat to Life' circumstances at the point of commencement. OCDA is open seven days a week, between the hours of 0700-2200.

EMERGENCY SPOC PROVISION

The purpose of the CD SPOC is to ensure only lawful, necessary and proportionate and viable applications for CD are made. Public authorities are expected to provide SPOC coverage for all CD acquisitions that they can reasonably expect to make. In exceptional cases where a SPOC is not available – such as sudden illness – then public authorities should limit the risk by using collaboration arrangements with other authorities (see S78 IPA). In these exceptional cases, the authority will be expected to report to IPCO the circumstances and reasons before their next inspection.

INTERNET CONNECTION RECORD (ICR)

PLEASE NOTE: ENTITLEMENT TO ICR IS NOT EXTENDED TO LOCAL AUTHORITIES.

The IPA allows public authorities (but not local authorities) to acquire Internet Connection Records (ICRs). An ICR provides details of the internet service that a specific device has connected to (e.g. a website or instant messaging application). It does not provide full browser histories or details of every web page visited, content of an Instant Message, or details of a message recipient, or any activity of a particular website. Refer to "Appendix 1: Definition of CD" for further detail.

SPOCs have some additional steps to be aware of where the conduct of an application requires the acquisition of ICRs.

S.62 of the IPA allows for the acquisition of ICRs if certain conditions are met. Chapter 9 of the CD Code of Practice provides additional information on the considerations that must be taken into account regarding the acquisition of ICRs.

GUIDANCE, STANDARDISATION AND CONSISTENCY

The benefits of introducing standardisation and consistency guidance for Applicants, SPOCs and Authorising Officers/Designated Senior Officers are assessed as improved efficiency, greater compliance with the law, higher quality of applications and scalability of best practice.

The risk of not embedding CD application standards will likely result in applications being sent back for rework if the necessity and proportionality case is not clear, or understandable to an independent authoriser. This could cause delays and affect operational effectiveness with negative impacts on the public.

THERE ARE KEY PRINCIPLES THAT SHOULD BE CONSIDERED BY EVERYONE INVOLVED IN THE PROCESS:

- Never refer to another application, document or system for the purposes of describing the full necessity and proportionality case, as an independent authoriser will not have access to locally held documents or systems. Each application should be able to stand alone when reviewed. E.G. **DO NOT** use statements such as 'Refer to Intelligence Reports or URN: XXX/12345/1 for the details of the investigation'.

- You may refer to another application, document or system where the purpose is to validate the communications address(es) included in the application. Although the independent authoriser will not have access, it is the Applicant and the SPOC's responsibility to check that the addresses are accurately validated based on source material.

SERIOUS CRIME THRESHOLD

From the 1 November 2018, an amendment to legislation came into force adding a serious crime threshold to the acquisition of event data[1].

WHAT DOES THIS MEAN?

This means that where an application is for the crime statutory purpose 60A(7)(b) to acquire event data, the crime must be a serious crime.

WHAT COUNTS AS A SERIOUS CRIME?

- An offence that is capable of attracting a prison sentence of 12 months or more (age 18+ years for England age 21+ years for Scotland and Northern Ireland).
- An offence by a person who is not an individual (i.e. a corporate body)
- An offence falling within the definition of serious crime in section 263(1) of the Act (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose)
- An offence which involves, as an integral part of it, the sending of a communication
- An offence which involves, as an integral part of it, a breach of a person's privacy.

Examples of offences that do not meet any of the definitions of serious crime include:

- Certain immigration offences under the Immigration Act 1971;
- Some sections of the Public Order Act which do not amount to violence (including using offensive words or causing a fear of violence);
- Driving offences, such as: joy riding, driving when disqualified, failure to stop or report an accident and driving when unfit to do so through drink or drugs; and
- Some sections of the Consumer Protection Act 1987 i.e. furnishing false information in response to notice, or to enforcement officer.

The Home Office publishes a list of 'notifiable' offences recorded by England & Wales police forces which may be helpful for confirming if the maximum sentence for an offence is 12 months of more[2]. The latest version can be found at www.gov.uk/government/uploads/system/uploads/attachment_data/file/721599/count-notifiable-offences-jul-2018.ods

[1] There is no change to the acquisition of subscriber data.
[2] For Scotland or Northern Ireland organisations, offence categorisation and maximum sentencing values may vary.

CD APPLICATION PROCESS

APPLICANT

1) Create a CD application as normal recording the statutory purpose of 60A(7)(b) for the applicable crime purpose.

EXAMPLE

This application is to support an investigation into fly-tipping under the Environmental Protection Act 1990. This meets the 12+ month's imprisonment definition of serious crime because the offence has a maximum sentence of five years.

2) On the application, record as part of the necessity case:
- a description of the offence(s) under investigation; and
- a justification for the seriousness of the offence (record which serious crime definition is met and how it is met, or record that the crime is not serious)

LOCAL AUTHORITY ONLY

APPROVED RANK OFFICER

DEFINITIONS OF SERIOUS CRIME

- 12 Month's+ Imprisonment: an offence that is capable of attracting a prison sentence of 12 months or more.
- Corporate Body: an offence by a person who is not an individual (i.e. a corporate body).
- Section 263 Offence: an offence falling within the definition of serious crime in section 263(1) of the Act (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose).
- Communication Offence: an offence which involves, as an integral part of it, the sending of a communication.
- Breach of Privacy: an offence which involves, as an integral part of it, a breach of a person's privacy.

3) Check that the public authority is permitted to use the recorded statutory purpose.

SPOC

4) Determine the conduct to satisfy the applicant's need (the type of data that is required)

5) If event data is required and the statutory purpose is crime, check the applicant has recorded:
- a description of the offence(s)
- a justification for the seriousness of the offence(s)

If not, return the application for rework.

6) Check the public authority is permitted to use the recorded statutory purpose

7) If the application is for event data and the statutory purpose is crime, check the seriousness of the crime has been justified. If not, reject or return the application for rework.

OCDA

STANDARDISATION AND CONSISTENCY

GUIDING PRINCIPLES FOR APPLICANTS

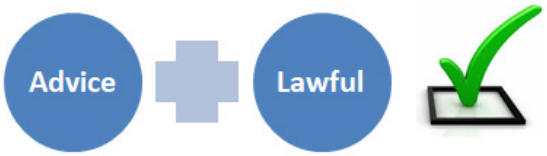
1 KEEP **ALL** APPLICATIONS SIMPLE, LEGAL AND CONCISE	
2 AVOID ACRONYMS AND ABBREVIATIONS UNLESS THEY ARE EXPLAINED FIRST	• *NFA (no further action) or* • *CT (Counter Terrorism or Council Tax!)*
3 USE STANDARD TERMINOLOGY TO DESCRIBE THE MAIN SUBJECT IN YOUR APPLICATION	• *Victim, Witness, Complainant, Vulnerable Person (other than the victim), Next of Kin, Suspect or Associate.*
4 CLEARLY STATE THE CRIME, OFFENCE AND PURPOSE AT THE START OF THE APPLICATION	• *This application is to support an investigation into burglary under the Theft Act or* • *To support an investigation into fraud under Section 3 of the Fraud Act.*
5 BE SPECIFIC ABOUT DATES OF INTELLIGENCE WITHIN THE APPLICATION; THIS DOES NOT HAVE TO COVER ALL INTELLIGENCE FOR THE WHOLE INVESTIGATION OR ENQUIRY.	• *Intelligence from [date/month/year] indicates that this device is attributed to the suspect.*
6 DO NOT MAKE REFERENCE TO ANOTHER APPLICATION, DOCUMENT OR SYSTEM IN PLACE OF COMPLETING A FULL NECESSITY AND PROPORTIONALITY CASE.	• *OCDA's independent authoriser will not have access to locally held documents or systems.* • *Each application should be able to stand alone when reviewed.*
7 BE SPECIFIC ABOUT HOW YOU HAVE OR HAVE TRIED TO ATTRIBUTE THE IDENTIFIER TO THE PERSON SUBJECT OF THE APPLICATION.	• *Open source checks on Google and Facebook have identified the telephone number as being linked to the suspect… or* • *Checks across intelligence systems have revealed no links or attribution for the suspect.*
8 CLEARLY STATE THE OBJECTIVE OF YOUR APPLICATION. **DO NOT** NAME THE SERVICES OR PRODUCTS FROM THE SERVICE PROVIDERS.	• *This application is required to help identify the location of the suspect between the relevant times and to identify associates who may also be involved in this offence.*
9 ENSURE ALL APPLICATIONS ARE CHECKED FOR SPELLINGS AND GRAMMAR BEFORE SUBMISSION. THESE DOCUMENTS MAY BE DISCLOSED.	• *Use MS Word or the spell-check functions on workflow to check the spelling and grammar before submission.*

10 **ALWAYS** CONSIDER THE VICTIMS' RIGHTS TO PRIVACY WHEN DESCRIBING EVENTS WITHIN APPLICATIONS. THESE CAN BE HIGH LEVEL DESCRIPTIONS AND DO NOT NEED TO CONTAIN GRAPHIC DETAILS OF OFFENCES.

STANDARDISATION AND CONSISTENCY

GUIDING PRINCIPLES FOR SPOCS

PROVIDE CLEAR ADVICE ON THE INTERPRETATION OF THE INVESTIGATORY POWERS ACT, PARTICULARLY WHETHER AN AUTHORISATION IS APPROPRIATE.



PROVIDE ASSURANCE THAT AUTHORISATIONS ARE LAWFUL UNDER THE ACT AND MEET THE SERIOUS CRIME THRESHOLD WHERE EVENTS DATA IS REQUESTED.

Consider

CONSIDER AND, WHERE APPROPRIATE, PROVIDE EXPLICIT ADVICE ON POSSIBLE UNINTENDED CONSEQUENCES OF THE APPLICATION. THIS INCLUDES EXCESS DATA, IMPLICATIONS AROUND SENSITIVE PROFESSIONS AND COLLATERAL INTRUSION.

- *A request for copy bills may result in the acquisition of the full billing period when only a selection of dates within that period may have been necessary.*

Explain

EXPLAIN WHY THE SERVICE(S) RECOMMENDED SUPPORT THE OBJECTIVE(S) OF THE INVESTIGATION.

- *Events data will support the investigation by showing the locations and helping to attribute the device by analysing its use and patterns.*
- *Events data can assist in identifying other victims and possible accomplices.*

Add Value

ADD VALUE IN COMMENTS, CONSIDERATIONS AND RECOMMENDATIONS, AS PRESCRIBED IN THE CODE OF PRACTICE UNDER THE ROLES AND RESPONSIBILITIES OF THE **SPOC**.

WHERE APPROPRIATE FLAG ANY ISSUES AROUND QUALITY E.G. SPELLING AND GRAMMAR TO THE APPLICANT FOR ACTION. THIS ACTION MAY SIT OUTSIDE OF THE APPLICATION PROCESS, DEPENDING ON LOCAL PROCESSES IN PLACE.

STANDARDISATION AND CONSISTENCY

GUIDING PRINCIPLES FOR AUTHORISING OFFICERS AND DESIGNATED SENIOR OFFICERS

THE AUTHORISING OFFICER/SENIOR DESIGNATED OFFICER IS AN EUROPEAN CONVENTION OF HUMAN RIGHTS ROLE AND CONSIDERATIONS SHOULD ALWAYS OBJECTIVELY REVIEW AN INDIVIDUAL'S RIGHT TO PRIVACY.

AVOID USING GENERIC TEXT OR PHRASES SUCH AS "THE DATA SHOULD BE HELD IN ACCORDANCE WITH POLICY."

EXPLICITLY, STATE THE CRIME/OFFENCE THAT YOU UNDERSTAND IS BEING INVESTIGATED.

- *This application is supporting an investigation into counterfeit goods under the Consumer Protection Act*
- *This application is supporting an investigation into fraud under section 2 of the Fraud Act.*

CLEARLY RECORD THAT YOU HAVE FULLY CONSIDERED AND UNDERSTOOD THE APPLICATION.

Record

CLEARLY RECORD THAT NECESSITY HAS BEEN UNDERSTOOD AND CONSIDERED.

CLEARLY RECORD THAT PROPORTIONALITY HAS BEEN UNDERSTOOD AND CONSIDERED.

CLEARLY RECORD THAT CONSIDERATION HAS BEEN GIVEN TO ANY POTENTIAL FOR THE AUTHORISATION TO RESULT IN UNINTENDED CONSEQUENCES.

- *I have carefully considered the issue of collateral intrusion and I am satisfied that the efforts to reduce such intrusion and negate the effects of this request are in place. These are X, Y, Z etc.*

BE SPECIFIC WHEN IDENTIFYING HOW THE SERVICE REQUESTED WILL SUPPORT THE OBJECTIVE OUTLINED IN THE APPLICATION.

Specific

FOR APPLICATIONS INTO CERTAIN PROFESSIONS, EXPLICIT CONSIDERATION MUST BE RECORDED TO COVER ANY UNINTENDED CONSEQUENCES OF SUCH APPLICATIONS AND WHETHER THE PUBLIC INTEREST IS BEST SERVED BY THE APPLICATION.

NOVEL / CONTENTIOUS

CLEARLY SET OUT WHY YOU CONSIDER THE APPLICATION TO BE NOVEL AND CONTENTIOUS AND INCLUDE WHAT LEGAL ADVICE HAS ALREADY BEEN OBTAINED AND WHY THIS IS CONSIDERED A LAWFUL REQUEST.

IPA

Investigatory Powers Act
for Communications Data

GLOSSARY

GLOSSARY OF TERMS

Term	Definition
Approval	For CD applications where the purpose is to identify or confirm the identity of a journalistic source, the Judicial Commissioner (JC) upon reviewing an Authorising Individuals Authorisation will either "approve" or refuse the authorisation (see refusal definition below).
Collaborative Organisation	An organisation that has a formalised collaboration agreement in place under the provisions of the Act.
"Collateral Intrusion"	The risk of obtaining communications, equipment data or other information about persons who are not the targets of the interference activity. Under IPA and existing legislation the risk of collateral intrusion must be identified for every application and steps taken to reduce it.
Communications Data (CD)	CD is information about communications: the 'who', 'where' 'when', 'how', and 'with whom' of a communication but not what was written or said (i.e. not content – see definition below). Generally it is data that may be acquired from a Telecommunication Operator (TO).
Telecommunications Operator	A person who offers or provides a telecommunications service to persons in the UK or controls or provides a telecommunication system which is wholly or partly in the UK or controlled from the UK. This term replaces the previous term of Communication Service Provider (CSP).[1]
"Content"	"Content" is any element of a communication or the data attached to it or associated with it that might reasonably be considered to be the meaning of the communication. Obtaining such data would constitute Targeted Intercept. For the exact wording of the definition of 'content', consult Part 9 of the IPA (Section 261).
Investigatory Powers Commissioner's Office (IPCO)	The independent body that oversees compliance with the IP Act and surveillance powers contained in RIPA and other legislation.

[1]**Consult Part 9, Chapter 2 (10) of the IP Act for the definition in full.**

Judicial Commissioner (JC)	Members of the judiciary selected to provide independent review of IPA authorisations, based at IPCO.
Law Enforcement Agency (LEA)	Public authority with the power to authorise and enact warrants, listed at Schedule 6 of the IP Act (Tables 1 and 2).
"Legal Privilege"	(a) in relation to England and Wales, has the same meaning as in the Police and Criminal authority with the power to authorise and enact warrants, listed at Schedule 6 of the IP Act (Tables 1 and 2). (b) in relation to Scotland, means – (i) communications between a professional legal adviser and the adviser's client, or (ii) communications made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings, which would, by virtue of any rule of law relating to the confidentiality of communications, be protected in legal proceedings from disclosure, and (c) in relation to Northern Ireland, has the same meaning as in the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)) (see Article 12 of that Order).
'Necessity'	One of the key tests applied in relation to use of all police powers. 'Necessity' refers to how requisite a tactic or course of action is, for example in relation to other less intrusive options.
'Proportionality'	The following guidance is provided in Section 3.14 of the Code of Practice: "When granting an authorisation the Authorising Officer must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest."
Refusal	Potential decision by an Authorising Officer or Judicial Commissioner (alternative to approval). The 'refusal' relates to the authorisation granted by the AO and means that the activity either cannot commence or must cease as soon as practicable (if already commenced under the urgency provision).

Urgent	There is no definition of what constitutes an 'urgent' requirement in the IP Act, however the Codes stipulate that urgency would involve an imminent threat to life or serious harm, or an application relating to an opportunity with limited time to act.
Investigatory Powers Tribunal (IPT)	The IPT is has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers. It is independent from the government, made up of members of the judiciary and senior members of the legal profession.
Technical Advisory Board (TAB)	Advisory panel including members appointed by the Secretary of State. For a full explanation of the role and remit of the TAB, consult Section 244 of the IPA (Part 8).
Technology Advisory Panel (TAP)	Panel that provides advice to the Information Commissioner (IC), the Secretary of State and the Scottish Ministers about the impact of changing technology on the exercise of investigatory powers whose exercise is subject to review by the Commissioner, and the availability and development of techniques to use such powers while minimising interference with privacy. For full detail of the purpose and remit of the TAP consult Section 246 of the IPA (Part 8).

NOTES...

Contact Us:

Telephone
0161 342 3480

Email
spoc@nafn.gov.uk

nafn.gov.uk
Data & Intelligence Services