IPCO
Investigatory Powers Commissioner's Office

OCDA
Office for Communications Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2022

HC 364

IPCO
Investigatory Powers Commissioner's Office

OCDA
Office for Communications Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2022

Presented to Parliament pursuant to section 234(6)&(8) of the Investigatory Powers Act 2016

Ordered by the House of Commons to be printed on 26 March 2024

Laid before the Scottish Parliament by the Scottish Ministers 26 March 2024

HC 364

SG/2024/3

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at info@ipco.org.uk

978-1-5286-4592-8

E03026099 03/24

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Letter to the Prime Minister

The Rt Hon Rishi Sunak MP
Prime Minister
10 Downing Street
London
SW1A 2AA

24 November 2023

Dear Prime Minister,

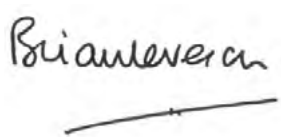
I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) from 1 January to 31 December 2022.

This report includes information on the use of covert powers by UK authorities, setting out the details required under section 234 of the Investigatory Powers Act 2016 (IPA). It is for you to determine, in consultation with my office, whether the report can be published in its full form without releasing material which would be contrary to the public interest or prejudicial to national security, to the prevention or detection of serious crime, to the economic wellbeing of the United Kingdom or to the discharge of the functions of those authorities which I oversee.

As in previous years, I have written to you separately regarding certain sensitive details which I believe should not be published for reasons of national security.

It is clear that the public authorities I oversee continue to take seriously their duty to comply with the law when exercising investigatory powers. While my report identifies and sets out some issues and areas of concern, this does not detract from the strong culture of compliance, dedication and professionalism in the authorities I oversee in undertaking this vital work.

Yours sincerely,



The Rt Hon Sir Brian Leveson
The Investigatory Powers Commissioner

1. Introduction by the Investigatory Powers Commissioner, Sir Brian Leveson

I am required by section 234 of the Investigatory Powers Act 2016 (IPA) to report annually to the Prime Minister on the functions of the Judicial Commissioners. As before, I have also included information on the operation of the Office for Communications Data Authorisations (OCDA), for which I am also responsible. I will use this introduction to set out some general observations arising from my oversight of the use of investigatory powers, as well as setting out some specific matters which are covered later in the report but which are useful to highlight.

This 2022 report covers my third full year as the Investigatory Powers Commissioner (IPC). I am particularly pleased to have the opportunity to reflect on the five-year anniversary of the creation of the Investigatory Powers Commissioner's Office (IPCO). The role of the IPC was created in the IPA alongside an overhaul of the way investigatory powers were authorised and overseen. IPCO was born out of the merger of three existing oversight bodies[1] and came into full operation in November 2017. OCDA became fully functional in March 2019.[2]

Bringing together three organisations to create IPCO, each with their own separate remits, structures, cultures and histories, and pulling together OCDA's functions was not without challenge. My predecessor, Sir Adrian Fulford, deserves credit for leading both organisations through these early years and for laying the foundations for the work we now do. Five years on, I am extremely proud of both organisations as we continue to provide independent and respected oversight, providing assurance to the public and Parliament that privacy safeguards are applied. This is testament to the hard work, diligence, resilience and commitment demonstrated by all those who work across both organisations. I would like to record my thanks to them all; without their advice, support and expertise, I would not be able to discharge my functions.

Since 2017, a number of factors, including the pandemic, new legislation, litigation and, of course, the ever-changing technology landscape, have tested and informed how we work. I am pleased at how we have continued the work we do. However, as well as looking back and recognising what we have achieved, I consider it vital, as I start my second term as IPC, to look forward. At the end of 2022, therefore, I commissioned two projects. The first is looking at how IPCO delivers its oversight, learning from our own experiences and those of others, so I can be sure it is as robust and effective as it can be within the currently available resources. The second project is to look at how IPCO and OCDA work together, reflecting on the maturity of the two organisations and how resources are already being shared. My intention is formally to merge the two organisations into one, for administrative purposes, while protecting the independence of the decision-making and oversight functions of each. I will report further on these projects in my 2023 report.

1 The Office of Surveillance Commissioners (OSC); the Interception of Communications Commissioner's Office (IOCCO); and the Intelligence Service Commissioner's Office (ISComm).

2 OCDA was formed in 2018 as a result of the Data Retention and Acquisition Regulations 2018 (which amended the Investigatory Powers Act 2016 in order to achieve compliance with EU law).

General observations

Since the IPC was created, the oversight functions for which I am responsible have expanded to cover new areas. That process of expansion continues. In October 2022, the UK-US Data Access Agreement came into force. Judicial Commissioners were given an additional responsibility to provide independent assurance on the necessity and proportionality of data requests made by UK authorities to US telecommunications operators.[3] There are also plans, through the Data Protection and Digital Information Bill, to transfer the casework review functions relating to the retention of biometrics to my remit. For these new functions, and for any other future considerations, I have made it clear that, while it is for the Government and Parliament ultimately to decide the functions of the IPC, any decisions must not compromise or undermine the high level of scrutiny and oversight that we provide. While I accept there is merit in not creating a plethora of judicial oversight bodies, IPCO's core mandate is in relation to the oversight of covert investigatory powers and major diversification from this would have an impact on the important work we do. I therefore reiterate what I said in my 2021 report that any new functions should be considered carefully and the appropriate resources, both in terms of Judicial Commissioners, technical expertise and staff, must be provided.

As I have stated in my last two reports, I believe it is important that the functions undertaken by the IPC should all be set out in statute. I was pleased, therefore, that in December 2022, the regulations came into effect which placed on a statutory basis my oversight of the Government Communications Headquarters' (GCHQ) Equities Process and of compliance by the National Crime Agency (NCA) and the Metropolitan Police Service (MPS) with *The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees*.[4] I am grateful to the Home Office for facilitating this. More recently, I am pleased that the then Secretary of State for Defence has agreed that my oversight of the use of covert human intelligence sources (CHIS) and surveillance in overseas operations by the Ministry of Defence (MoD) should also be recognised in statute. We will work with the Government to find an appropriate vehicle for this to be achieved.

Over the last two years, my officials have engaged with the Home Office on its statutory review of the IPA. This review was carried out in accordance with section 260 of the IPA, which requires the Secretary of State to prepare a report on the operation of the Act five years after Royal Assent. This report was laid before Parliament on 9 February 2023.[5] In parallel, the Home Secretary appointed Lord Anderson of Ipswich KBE KC to conduct an independent review of the Act.[6] Although I consider policy matters generally to be for the Government and, ultimately, Parliament, given the matters within scope of these reviews I have provided views on the practical operation of the Act and the potential implications of issues raised where it is appropriate to do so. It is particularly important, in my view, to ensure that, where change to the current arrangements has been mooted, this should ensure that the right balance is struck between safeguarding privacy and delivering operational utility.

As an oversight body with a specialised remit, the value we can draw from other regulatory and oversight organisations, both domestically and internationally, should not be underestimated. Given the limitations on travel over the last two years, it was particularly pleasing in 2022 to resume face-to-face meetings with both our European and Five Eyes counterparts. The opportunity to discuss how we do our work and share areas of best practice is of enormous value in strengthening our oversight approach.

---

3 See: paragraphs 2.2-2.4.
4 See: https://www.legislation.gov.uk/uksi/2022/1299/made
5 https://www.gov.uk/government/publications/report-on-the-operation-of-the-investigatory-powers-act-2016/home-office-report-on-the-operation-of-the-investigatory-powers-act-2016-accessible-version
6 See: https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2

Finally, in this section, it would be remiss of me not to mention artificial intelligence (AI). Inevitably, AI and machine learning will play an increasingly significant role in the work of the organisations we oversee, particularly for the intelligence agencies. It is critical, therefore, that we properly understand such developments, can see what impact they may have on oversight and, in particular, how we might be able to use the power of AI to enhance oversight. I have asked the TAP to look at this as a priority for 2023, to help us identify how this directly impacts our work and our immediate next steps. Members of the Technology Advisory Panel (TAP), together with my officials, will liaise with public authorities as necessary to ensure that compliance and safeguards are considered as an integral part of any policy or technological development rather than left as an afterthought.

Matters arising in 2022

Overall, I am satisfied that public authorities take seriously their responsibilities for the use of covert investigatory powers and are exercising their functions in accordance with relevant legislation and Codes of Practice. Refusals of applications by Judicial Commissioners continue to be low. Although I have been challenged on this, on the basis that this demonstrates a failure of robust oversight, it is, in reality, because Judicial Commissioners have been rigorous in their approach. The relevant agencies quickly came to understand the careful scrutiny that will be applied to applications and, as a result, are scrupulous in their preparation to ensure that the requirements of the legislation are addressed to the standard expected. It is also the case that, where Judicial Commissioners have concerns about an application, they will normally request further information before making a final decision.

I am aware that using investigatory powers is only a small part of the work of many of the authorities we oversee. For some public authorities, we have seen recent widespread criticism and adverse commentary on other areas of their work. It is not my place to comment on matters outside my remit but, for the areas for which I do have oversight, my Inspectors repeatedly report high levels of professionalism and dedication in the organisations they visit. All of this is critical to the successful application of these particularly intrusive powers.

Given that I oversee over 600 public authorities, it should not be expected that we inspect every occasion on which covert investigatory powers are used each year. Furthermore, as over 380 inspections were conducted in 2022, it is not proportionate to provide a summary of every inspection in this report. There are, however, a small number of issues from this year to which I would like to draw particular attention. These are:

- **Records Product Management:** Since our data assurance programme was commenced in 2019, I have seen a considerable improvement in public authorities' understanding of their responsibilities for data handling, retention and destruction. Where concerns remain, my Inspectors will continue working with those public authorities to ensure that good practice is embedded. [See: paragraphs 2.17-2.22].
- **Litigation:** In Chapter 3, I have set out the legal developments that have had a bearing on the work of IPCO and OCDA. Of particular significance are the implications for oversight arising out of the *Big Brother Watch* and *Liberty* judgments.
- **Legally privileged material:** Following an in-depth investigation across all three intelligence agencies of the handling of legally privileged material which has no intelligence value but is included within material that does and which therefore needs to be retained, I concluded that the process used by MI5 was not compliant. Work is underway to address this complex issue and I will report further on this next year. [See paragraphs 8.34-8.36].

- **The Principles:** 2022 was the third year since The Principles have been in force and, in general, we found there to be a high level of compliance. One concern did arise in relation to the use of thematic authorisations in certain circumstances by the NCA. I am pleased that this has now been addressed and the cases in question are now considered individually by ministers. [See paragraphs 12.26-12.28].
- **Covert Human Intelligence Sources (Criminal Conduct) Act 2021:** Following its implementation in the autumn of 2021, we have kept a close eye on the use of Criminal Conduct Authorisations (CCAs), both through quarterly reviews and our regular inspections. Following the identification of some concerns about the breadth of some CCAs and their underlying CHIS authorisations, I wrote to the relevant national working group setting out my expectations. I am also pleased to see that the updated Code of Practice has now been published.[7] As well as providing guidance on the use of CCAs, the Code includes a requirement to notify me within seven days of an authorisation of a vulnerable adult or a juvenile CHIS. This enables my Inspectors to carry out a review as early as possible to ensure that the necessary safeguards are in place. [See: from paragraphs 13.14].
- **Thematic report of targeted equipment interference (TEI):** Following a range of inspections in 2022, we have produced a report drawing together the key findings and areas for improvement in the use of TEI by police forces and law enforcement agencies (LEAs). We have set out more detail on this in Chapter 13. [See: from paragraph 13.26]. We have found this type of report to be of particular value, both in helping my Inspectors determine the structure of forthcoming inspections and in influencing policy and operational change to processes.
- **Management of intercept material:** For a number of years, I have been flagging concerns about performance and compliance issues in the system used by LEAs to manage intercept material. The project to develop a replacement system is underway, led by the Home Office, and this absolutely must be given the highest priority. The shortcomings of this system once again came to the fore at the end of 2022 when it was identified that some collected data could not be deleted. Further details on the bespoke investigations on this issue will be set out in my 2023 report. [See: paragraphs 13.40-13.42].
- **UK National Authority for Counter-Eavesdropping (UK NACE):** During the inaugural inspection of UK NACE in late 2021, we identified a number of errors relating to the acquisition of communications data. This led me to conclude that the authority was not competent lawfully to exercise its internal authorisation powers until sufficient measures were put in place to address these serious issues. I recognise the considerable effort that have been made to address the inspection findings and, following a further visit by Inspectors in December 2022, I was content that responsibility for authorisations should be returned to the organisation. [See: paragraphs 14.15-14.19].
- **Prisons:** The introduction of a new Authorised Communications Controls and Interception Policy Framework (ACCIPF) document will provide clearer direction and guidance on the authorised interception and monitoring of prisoner communications. I hope this will address the concerns I have flagged in previous reports about the arrangements for interception in prisons. [See: paragraphs 16.4 and 16.13-16.16].
- **Home Office error:** Following the identification of an error in relation to the signing of out-of-hours warrants at the Home Office in 2021, I am content that this issue has now adequately been addressed, with revised processes in place to avoid reoccurrence of the issue. [See: paragraphs 17.3 and 18.9].

7 See: https://www.gov.uk/government/publications/covert-human-intelligence-sources-code-of-practice-2022

2. Developments in 2022

Overview

2.1 This chapter provides an overview of the key policy and operational developments during 2022 which had an impact on the responsibilities and functions of the Investigatory Powers Commissioner (IPC) or the workings of the Investigatory Powers Commissioner's Office (IPCO) and/or the Office for Communications Data Authorisations (OCDA).

The UK-US Data Access Agreement

2.2 The UK-US Data Access Agreement (DAA) entered into use in October 2022.[8] Our oversight function is comprised of additional reviews of specific relevant targeting decisions and a more general audit of public authorities' compliance with the requirements of the DAA. Judicial Commissioners review the necessity and proportionality of certain minor modifications of targeted interception warrants[9] and internal authorisations for targeted communications data (CD) that are for the purpose of acquiring data pursuant to the DAA.

2.3 A programme of inspections to audit wider compliance with the DAA by those public authorities requesting data will commence in early 2023. These inspections will focus initially on a review of controls and governance at those public authorities, with more detailed testing activity to follow later in the year.

2.4 Our oversight of the DAA also extends to those public authorities who obtain overseas production orders issued under the Crime (Overseas Production Orders) Act 2019. We will report further on this in our 2023 report.

Schedule 3 to the Counter-Terrorism and Border Security Act 2019

2.5 Through the National Security Act 2023, the Government has amended the primary legislation for the retention powers under Schedule 3 to the Counter-Terrorism and Border Security Act 2019 by changing the definition of "protected material" so it no longer includes confidential business material. Under the original wording of Schedule 3, confidential business material fell within the definition of protected material, including material that has been acquired in the course of a trade and is held in confidence.

2.6 This change replaces the requirement for the IPC to authorise the retention of copies of confidential business material with a new Counter-Terrorism Police authorisation procedure, requiring an officer of at least the rank of superintendent to authorise access to

8 See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Advisory-Notice-1_2023-UK-US-DAA-Advisory-Notice-13-February-2023-4.pdf

9 This is a decision to target a new person, organisation or set of premises falling within the descriptive subject matter details provided by a warrant.

such material. This change brings Schedule 3 into line with the authorisation process under Schedule 7 to the Terrorism Act 2000.

2.7 Given the change aligns the definition of protected material with the categories of material that receive special protection in the Investigatory Powers Act 2016 (IPA), we were supportive of this proposal.

2.8 A report on the operation of the IPC's current functions under Schedule 3 will be made to the Home Secretary separately.

Definition of communications data

2.9 The acquisition of communications data (CD) is the most widely used investigative power, yet is arguably the most difficult to apply due to the complex and ambiguous definition of CD in section 261(5) of the IPA. This is due in part to the decision to draft the legislation in technology-neutral terms in an attempt to future-proof the Act. As we set out in our 2021 report, application of the definition has posed real operational difficulties for the CD community and we continue to advocate for legislative change.

2.10 Following discussions between IPCO, OCDA and the Home Office, guidance to assist with the interpretation of the definition of CD, as well as the definition of a telecommunications operator (TO), was formally "launched" in March 2022 at the International Communications Data and Digital Forensic conference.[10] The need for such guidance stemmed from what became colloquially known as the *IPA versus DPA* (Data Protection Act 2018) issue, which we have discussed in detail in our past three annual reports.

2.11 The *IPA vs DPA* question concerns the determination by public authorities whether they are seeking to acquire CD (as defined in the IPA) and thus require a CD authority under Part 3 of the IPA, as opposed to making a request for disclosure, normally relying on an exemption under the DPA. The former compels a TO to provide the requested data, whereas the latter requests voluntary provision of the data. Significantly, the CD Code of Practice prohibits the use of the DPA to circumvent requesting CD under the IPA. The distinction hinges on the correct application of the definitions of CD and TO. It is vital public authorities get this distinction right, as the IPA also criminalises the act of knowingly or recklessly obtaining CD from a TO without a lawful authority, such as a Part 3 IPA authorisation.

2.12 Application of the CD definition has been practically challenging not only for public authorities, and TOs, but also OCDA in that it can only grant authorisations for data that is clearly defined as CD, which often requires case-by-case analysis. If there is any ambiguity whether data meets the CD definition, either by the public authority, TO or OCDA, the operational consequences could be significant. For example, we have previously seen public authorities faced with a TO refusing to disclose CD without an IPA authorisation, but OCDA declining to grant such on the basis that it does not meet the definition of CD. The guidance aimed to provide public authorities, TOs and OCDA with a consistent approach to determine whether data falls within the definition of CD or not.

10 The guidance was published in April 2023. See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1151389/REDACTED_Guidance_on_Definition_of_Communications_Data.pdf

2.13 During 2022, a programme of training was carried out across public authorities. This was intended to ensure that authorities were:

- aware of the guidance;
- actively working to adopt the principles in the guidance into their working procedures; and
- assisting staff in relevant business areas to make the necessary changes.

2.14 One of the effects of the guidance has been to make it clear that many companies are partial TOs, despite them possibly not previously recognising themselves as such. Some of these TOs have, understandably, taken a cautious approach by refusing to release data to public authorities without an IPA authorisation compelling them. This has particularly been the case where it is difficult to determine whether data relates to their telecommunications service (i.e., is CD) or another "real world" service (i.e., is not CD).

2.15 By way of example, a high street bank may be a partial TO. The bank's core service is banking, but it additionally provides a telecommunications service by virtue of its website and online banking facilities. A bank will hold certain data for every customer (i.e., both in branch and online customers – an example might be a customer number) in order to deliver its banking service. That same data may be required to provide its online banking service (i.e., the telecommunications service, with a customer number possibly forming part of the login credentials for its online banking portal). This data may therefore be held by the bank as "dual/multipurpose data". In this scenario, whether that data falls within the definition of CD is likely to depend on the *purpose* for requesting that data, and whether the data relates to either the *provision* of or *use* of the telecommunications service. For example, if a public authority was requesting the dual/multipurpose data with the intention of obtaining CD, then such information would be capable of being requested under a CD authorisation. However, it is unclear whether the same data could be requested relying exclusively on the DPA or if it must first be ascertained if the customer banks online or not. We consider that a DPA request can also be relied upon for dual/mixed use data as there is an argument that the bank is not acting in the capacity of a TO in respect of this data unless it is specifically being requested to query its data holdings in that capacity. It can often be difficult to reach a conclusion if the public authority is not familiar with how the relevant business operates.

2.16 What this means in practice is that a bespoke, case-by-case approach is needed for different TOs. This involves looking at the types of data they hold as well as how the TO holds that data, particularly in relation to what is often called "subscriber" or "account data". This is extremely difficult for public authorities, TOs and OCDA routinely to apply and maintain operational effectiveness and, in our view, supports the need to examine the definition of CD as a priority. We are pleased this need has been recognised by the Home Office and that options to address this complex issue are being considered.

Records Product Management (data assurance)

2.17 During 2022, we continued to monitor the progress made by public authorities in complying with the Safeguards chapters of the 2018 Home Office Codes of Practice. This was an integral part of our routine inspections and, where necessary for larger organisations or where progress has been disappointingly slow, we conducted bespoke visits.

2.18 In the vast majority of cases, public authorities were well advanced in completing the key actions we provided as a guide. These included completing data pathways, mapping processes, policy development and training staff. We have seen commendable progress by

some law enforcement agencies (LEAs), such as South Wales Police, South Yorkshire Police and the Metropolitan Police Service, and in several local Councils such as Worcester City and Worcestershire County, Leicestershire County and Cheshire West and Chester.

2.19 Where progress has been slow, we will often follow up with an interim visit to ensure action is taken.

2.20 At the end of 2022, the IPC wrote to all LEAs, through the National Police Chiefs' Council (NPCC) to provide an update on overall progress and to make clear his expectations for the following year. That communication also addressed the specific question of how long material relating to covert human intelligence sources (CHIS) should be retained. While accepting the need for a duty of care beyond the cessation of an individual's authorisation as a CHIS, the IPC provided a clear direction that deferring an initial review of whether to destroy any material beyond five to ten years was contrary to the requirements of the CHIS Code of Practice.

2.21 Our 2022 inspections identified some positive actions towards attaining good levels of compliance. These included (among others):

- identifiable and engaged ownership at senior levels;
- officers trained to recognise their personal responsibilities as to the management of material acquired through their use of covert tactics;
- establishing a clear plan for review, retention and disposal (RRD) and its ownership at the outset of operations or activities;
- maintaining a clear audit trail of the RRD process;
- adapting or procuring IT management systems which have RRD processes "built-in" by default; and
- implementation of centralised storage solutions.

2.22 In 2023, we will be looking for evidence that the retention, review and destruction of the product obtained through the use of covert tactics has become business as usual. We will do this through the random sampling of documentation and IT management records, to identify whether the required policies, processes and awareness among officers and staff are having a meaningful impact.

Operational purposes

2.23 The UK intelligence community (UKIC) continues to rely on the full range of operational purposes in the vast majority of its bulk warrants issued under the IPA. We were satisfied that the bulk warrants we reviewed in 2022 included operational purposes that met the statutory test.

2.24 The IPA requires the Prime Minister to review the list of operational purposes annually. This last happened in September 2022.

Raising concerns with IPCO

2.25 No new disclosures of information were made to IPCO during 2022. The guidance document *Disclosing Information to IPCO*, was published on our website in 2022.[11]

11 See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/2022-08-Disclosing-information-to-IPCO.pdf

3. Relevant litigation in 2022

Overview

3.1 This chapter sets out the main legal developments and cases that have had a bearing on the work of either the Investigatory Powers Commissioner's Office (IPCO) or the Office for Communications Data Authorisations (OCDA) in 2022.

Technology Environments ("the MI5 data handling") case

3.2 Since 2019, we have reported on the compliance problems identified in a certain technology environment at MI5, including the response to those problems by MI5, the Home Office and IPCO. In January 2020, Liberty and Privacy International brought a new claim in the Investigatory Powers Tribunal (IPT) against MI5 in relation to this matter ("the MI5 data handling claim"). The claimants alleged (among other things) that MI5 had failed fully and frankly to disclose the absence of certain safeguards within the technology environment to the Secretary of State and to Judicial Commissioners when applying for warrants and that the Secretary of State had failed adequately to investigate the deficiencies within the environment in the context of deciding whether to issue warrants. The claimants also applied to amend and re-open a separate, existing claim regarding MI5's handling of bulk personal datasets (BPD) and bulk communications data (BCD) ("the BPD/BCD claim") on the basis of the deficiencies that existed within the technology environment during the period at issue. In February 2020, that application was stayed pending determination of the MI5 data handling claim and the issue of remedies in the BPD/BCD claim was adjourned.

3.3 In July 2021, the IPT made a statutory request for assistance of the IPC, seeking to confirm whether any further potentially relevant material was held by IPCO. In response to that request, we provided a number of documents to the Tribunal in December 2021. The substantive hearing in the MI5 data handling claim took place in July 2022 and the judgment was published on 30 January 2023.[12]

3.4 The IPT accepted that there were substantial failures in MI5's Handling Arrangements. In particular, the Tribunal found:

- that it was of particular importance that the person granting the warrant was given full information about any significant non-compliance issues;
- that the Secretary of State for the Home Department did breach their duty by not making adequate enquiries as to whether the statutory safeguards were or were not being met; and

12 *Liberty, Privacy International v Security Service, Secretary of State for the Home Department* [2023] UKIPTrib 1

- that, although there was no evidential basis to find that any officers of MI5 sought to hide information, the failure to notify IPCO until February 2019 was a serious misjudgement.

3.5 The IPT commended the robust steps taken by the IPC once his office had been alerted and the investigations that subsequently were carried out. We are pleased that this demonstrates the effectiveness of the safeguards regime and the adequacy of the measures available to the IPC. The fact that this case was brought, and indeed the judgment itself, is also part of that effective regime.

3.6 The IPT also decided that there was no substance in the assertion that the systemic failings demonstrated that the legal regime was not in accordance with the law, or that any relevant evidence gave rise to any valid challenge to the effectiveness of the Investigatory Powers Act 2016 (IPA).

Big Brother Watch and others v United Kingdom

3.7 Following the European Court of Human Rights' (ECHR) judgment in May 2021,[13] the Government Communications Headquarters (GCHQ) confirmed that it had implemented an agreed solution for the internal approval of its use of strong selectors under bulk interception. This new approach will mean that such targeting cannot take place without prior approval from a senior GCHQ officer. Targeting and these approvals will be subject to our inspection and audit.

3.8 The Home Office published in March 2023 a proposal for a Remedial Order under section 10 of the Human Rights Act 1998 (HRA) to address the Article 10 ECHR violation identified in the judgment. Ultimately, this will require authorisation to be obtained from a Judicial Commissioner prior to an analyst selecting for examination any content where the purpose is to acquire confidential journalistic material or identify a source of journalistic information. We have been clear that this legislation must be prioritised in order to remedy the Article 10 violation and enable GCHQ to operate in full compliance with the ECHR.

3.9 The Home Office is also reviewing the list of operational purposes to consider whether these can be used to categorise selectors. As the judgment was considering facts which predated the enactment of the IPA, the effect of specified operational purposes was not considered by the Court in the judgment. It is our preliminary view that categorisation by operational purpose may be sufficient to comply with the terms of the judgment. We await the outcome of the Home Office's review and will consider the conclusions in due course.

R (on the application of Eric Kind) v Secretary of State for the Home Department

3.10 Following the 2021 judgment of the Divisional Court in *R (on the application of Eric Kind) v Secretary of State for the Home Department*, we have been working with the Cabinet Office to address the issues identified in the judgment relating to the vetting process for applicants for roles within IPCO. In June 2021, the Cabinet Office conducted a review of the arrangements for adverse security checks of those offered employment by IPCO. In 2022, it was recommended that the Cabinet Office sponsored Security Vetting Appeal Panel be offered as a route of appeal for these checks, to which the then-chair, Baroness Hallett, agreed. We continue to work with the Cabinet Office on the detail of the arrangements and we will update on progress in our 2023 report.

13 See: http://www.bailii.org/eu/cases/ECHR/2021/439.html

Liberty v SSHD and SSFCA [2022] EWHC 1630 (Admin)

3.11 In May 2022, the High Court considered whether certain powers in the IPA were contrary to "the e-Privacy Directive"[14] and the EU Charter of Fundamental Rights,[15] in the light of the recent judgments of the Court of Justice of the European Union (CJEU) in *Privacy International v Secretary of State for the FCO*[16] ("*Privacy International*") and *La Quadrature du Net & Ors v Premier Ministre & Ors*[17] ("*La Quadrature*").

3.12 The issues before the Court fell broadly into two categories. First, Liberty (the Claimant) challenged aspects of Part 4 of the IPA, read with Part 3, concerning communications data (CD). Secondly, Liberty challenged aspects of the provisions relating to "bulk powers" in Parts 5, 6 and 7 of the IPA.

3.13 The Court declared that the powers in the IPA were compatible with retained EU law with one exception. The Court found that section 61 of Part 3 of the IPA (read together with Schedule 4) was incompatible insofar as it permitted the security and intelligence agencies to obtain access to CD (retained under Part 4 of the IPA) for the "applicable crime purpose" without prior authorisation by a court or other independent body.

3.14 Generally, the agencies operate in the field of national security, but they are also empowered to prevent and detect serious crime: in other words, for ordinary criminal purposes which may not relate to national security. Where the agencies are carrying out the same functions as law enforcement, the Court found that they should be subject to the same legal regime.

3.15 Following the judgment of the High Court, the Home Office laid in draft "The Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers)" Regulations 2022.[18] The Regulations remove the ability of the agencies to acquire CD for serious crime purposes by virtue of section 61 of the IPA, which permitted internal authorisation in non-urgent cases. They will, however, still be able internally to authorise urgent CD acquisition made under section 61A.

3.16 Following approval by resolution of each House of Parliament, these Regulations came into force on 1 January 2023. From 1 January, the agencies have needed to apply to OCDA, under section 60A of the IPA, for targeted CD requests for exclusively serious crime purposes. OCDA worked closely with the Home Office and the agencies to prepare for a smooth implementation.

3.17 In July 2022, Liberty was granted permission to appeal to the Court of Appeal on limited grounds.

---

14 Parliament and Council Directive 2002/58/EC (as amended by Parliament and Council Directive 2009/136/EC)

15 Article 7, Article 8 and Article 11.

16 Case C-623/17. Judgment given by the Grand Chamber of the CJEU on 06 October 2020: [2021] 1 WLR 4421.

17 Joined Cases C-511/18, C-512/18 and C-520/18. Judgment given by the Grand Chamber of the CJEU on 06 October 2020: [2021] 1 WLR 4457.

18 See: The Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers) Regulations 2022 (https://www.legislation.gov.uk/ukdsi/2022/9780348240641)

Operation VENETIC

3.18 Operation VENETIC was the National Crime Agency (NCA) operation to penetrate the encrypted and supposedly secure Encrochat communications platform. In 2020, the NCA applied for a targeted equipment interference (TEI) warrant from IPCO for this purpose. 2021 saw the beginning of significant litigation concerning this operation, with a major focus on whether the conduct to penetrate the Encrochat platform constituted or included the interception of "live" or stored communications. This was relevant because, while the product of a TEI warrant can be admitted in evidence, such a warrant can only authorise conduct in respect of stored communications. This is in contrast with a targeted interception warrant which could authorise the interception of "live" communications, but the product from which is subject to a statutory restriction preventing it from being admitted as evidence.

3.19 In *R v A, B, C, D* the Criminal Division of the Court of Appeal held that the conduct in question was in respect of stored communications and, therefore, that the right authorisation was obtained.[19] Other related proceedings continue in both the criminal and civil courts – including a case before the IPT.

19 [2021] EWCA Crim 128

4. Protecting confidential or privileged information

Overview

4.1 The Investigatory Powers Act 2016 (IPA) and its Codes of Practice provide additional safeguards for certain forms of confidential and legally privileged information. Judicial Commissioners have a statutory role in authorising and overseeing the acquisition and retention of such material. Safeguards are also set out in the Police Act 1997, the Regulation of Investigatory Powers Act 2000 (RIPA),[20] the Covert Surveillance and Property Interference Code of Practice and the Covert Human Intelligence Sources (CHIS) Code of Practice to protect confidential and privileged information acquired from the use of such techniques.

Legal Professional Privilege (LPP)

4.2 Legal Professional Privilege (LPP) protects against the disclosure of confidential communications and other material attaching to such communications. It enshrines the right to seek legal advice and conduct litigation in confidence. Material subject to LPP may include conversations or written advice, which can arise between an individual or organisation and a professional legal adviser. In some circumstances, privilege may attach to confidential communications between an individual and a third party.

4.3 In all applications, we expect consideration to be given to the likelihood of obtaining material subject to LPP. We expect consideration to be given to the public interest in protecting the confidentiality in privileged communications balanced against the public interest in obtaining the material. We would also expect to see how any material will be handled if it is obtained.

4.4 In our 2021 report, we set out our concerns that law enforcement agencies (LEAs) were not setting out in full their considerations on the likelihood of obtaining material subject to LPP. This continued to be a focus of our inspections in 2022, particularly in relation to intrusive surveillance, and, following a discussion in January 2022 with the Investigatory Powers Commissioner (IPC), Chief Constable Mark Roberts, the National Police Chiefs' Council (NPCC) Lead for Covert Legislation and Guidance, wrote to all Chief Constables, Covert Authorities Bureau (CAB) Managers and Senior Responsible Officers. His letter explained that LPP should not exclusively be limited to first-hand conversations between subjects and their professional legal advisors and that, in certain contexts where information has been provided or made available in confidence, such as when an individual discusses legal advice received with immediate family or close friends, privilege may not be considered to have been waived generally.[21]

---

20 The Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) regulates the use of surveillance and CHIS in Scotland.

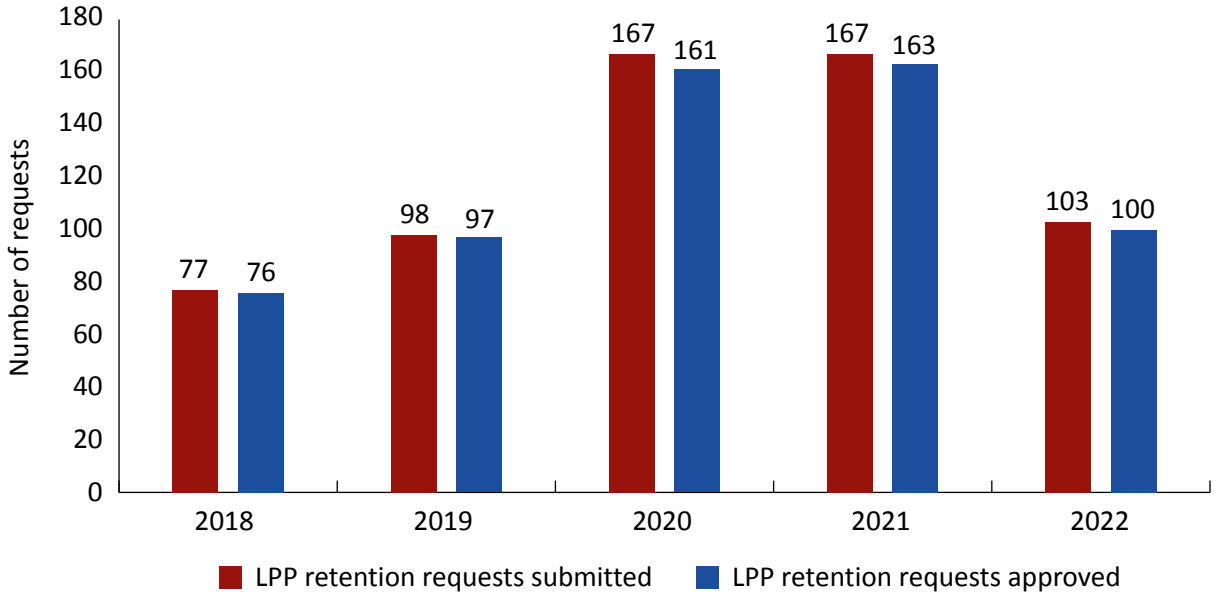
21 This is, in part, based on obiter comment in *Turner v R* [2013] EWCA Crim 642, see paragraph 26.

4.5 We are pleased to have seen an overall improvement in the considerations of acquiring LPP material over the last year. Despite this, we continue to receive late notifications from LEAs that LPP has been retained, other than for the purpose of its destruction. It is important that all cases are reported to the IPC as soon as practicable.

4.6 In the event that public authorities do obtain LPP material in their exercise of investigatory powers, they must inform the Investigatory Powers Commissioner's Office (IPCO) if they wish to retain that material for a purpose other than destruction. When making their decision as to retention, the Judicial Commissioners will take into account the material, its proposed use and the handling conditions in order to determine whether the public interest in retaining it outweighs the public interest in the confidentiality of the material.

4.7 In 2022, 103 applications were made in relation to the retention of LPP material. Of these, 100 were approved.

Figure 4.1 Number of requests submitted and approved for the retention of LPP material, 2018 to 2022



Confidential journalistic material and sources of journalistic information

4.8 Journalistic freedom is protected under Article 10 (freedom of expression) of the European Convention on Human Rights. We would expect all relevant applications to consider the necessity and proportionality of any request in that context. We expect these applications to be rare.

4.9 Confidential journalistic material and sources of journalistic information are subject to specific safeguards, which are designed to respect the freedom of the press. All applications made under RIPA and IPA should set out whether the purpose of the application is to obtain confidential journalistic material or identify sources of journalistic information. All applications should also state the likelihood of such material being obtained.

4.10 The acquisition of communications data (CD) by LEAs relating to journalists and sources of journalistic information is covered in Chapter 13.

4.11 Looking at the use of other powers, our inspections have not identified any concerns in relation to the handling of journalistic material. The number of applications to acquire journalistic material in other powers will always substantially be smaller than those seeking to acquire CD (due to the relative volume of total applications) and all applications will have been subject to the double lock approval by a Judicial Commissioner. As with all authorisations, it must be necessary and proportionate to conduct the proposed interference or interception and so the test that must be satisfied here is no different. However, we expect additional consideration to be given to the confidential material that may be obtained and to the need for there to be an overriding requirement in the public interest to satisfy the threshold in this context. We would also expect applications to give some consideration to how confidential material would be handled and the extent to which such material is expected to be relevant to the investigation.

4.12 Under the RIPA Codes of Practice, applications to conduct surveillance and use CHIS where there is a likelihood of obtaining journalistic material must be subject to an additional level of internal scrutiny and be authorised at a more senior level. We would expect any relevant application to include details of how this sensitive material would be protected.

4.13 In 2022, 49 applications were made for warrants under the IPA where the purpose was to obtain material which the applicant authority believed would relate to confidential journalistic material. Applications relating to sources of journalistic information might either be for warrants, which must all be considered by a Judicial Commissioner (even if not relating to journalistic sources), or for CD, which would also be subject to judicial approval under section 77 of the IPA. Under section 77, the Judicial Commissioner must consider the public interest in protecting a source of journalistic material (i.e., ensuring that there is an overriding requirement for Article 10 purposes). In 2022, there were 31 warrant applications to identify a journalistic source and a further 30 CD applications were considered under section 77.

Additional safeguards for health records

4.14 The intelligence agencies may apply for a specific bulk personal dataset (BPD) warrant to retain and examine a dataset which includes health records. Any such applications are subject to an additional safeguard in that the case for retention and examination must be judged by the Secretary of State to be exceptional and compelling. We are unable to publish any details of whether, and to what extent, this power was used. However, we can confirm that we have not identified any issues of non-compliance or made any recommendations in relation to these safeguards.

5. Communications and engagement

Overview

5.1 Communications and engagement activities of the Investigatory Powers Commissioner (IPC) increased throughout 2022, as meetings became easier following the Covid-19 pandemic. In addition, with the increase in face-to-face conferences, staff across the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) contributed to professional development and learning events across the UK.

5.2 International engagement also increased during 2022, with more meetings, conferences and delegation visits than previously seen. For the first time, we organised and hosted the European Intelligence Oversight Conference (EIOC) in London; oversight representatives of 16 countries gathered to discuss accountability, transparency and how the development of technology impacts on our work.

5.3 Following a successful launch of the new IPCO website in 2021, we have been able to share updates, inspection statistics and publications. From the beginning of 2022, quarterly newsletters, sent to all organisations we oversee, were published on the website. Quarterly inspection statistics were also issued, providing a breakdown of our inspections categorised by organisation type.

5.4 We strive to engage effectively with external parties in an effort to enhance accountability, impact and transparency; the latter remains a priority for both organisations and the IPC himself.

5.5 A more detailed schedule of the IPC's public engagements is found at Annex D.

UK engagement

Public authorities

5.6 Throughout 2022, the IPC met with the head of each of the UK intelligence agencies, as well as Directors within the warrant granting departments (WGDs). He presented at events including the International Communications Data and Digital Forensics conference (ICDDF) and the Serious and Organised Crime Exchange (SOCEX). The IPC also discussed his role with a group of lawyers at the National Crime Agency (NCA).

5.7 Our Inspectors delivered numerous training sessions in 2022, including sessions organised by the College of Policing or other continuing professional development (CPD) events organised internally by a public authority. Two of our Inspectors hosted drop-in sessions at the Internet, Intelligence and Investigations Conference, subsequently joining a follow-up working group at the College of Policing. Another Inspector delivered training at the National Single Point of Contact Managers' Forum.

5.8 We continue to send our quarterly newsletter to public authorities, highlighting good practice, process updates and legislative changes.

Independent bodies

5.9 The IPC continued to meet with independent bodies in 2022, including the Investigatory Powers Tribunal (IPT) and His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS). In addition, the IPC met with the Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner, Professor Fraser Sampson, as well as the Information Commissioner, John Edwards.

Others

5.10 In 2022, the IPC met with ministers and Members of Parliament with a specific interest in our work, including the Chair of the Intelligence and Security Committee (ISC), the Secretary of State for Defence, the Shadow Home Secretary and the Shadow Security Minister.

5.11 The IPC continued to engage with non-governmental departments (NGOs) throughout 2022. Correspondence was exchanged on specific issues, and face-to-face meetings were held with Reprieve and Privacy International.

International engagement

5.12 2022 saw a significant rise in international engagement as pandemic restrictions eased across the UK and globally.

5.13 We hosted a number of international delegations on their visits to the UK. The IPC, along with our team leads, spent time with these groups to discuss our various ways of working and what we can learn from each other.

5.14 We continued to engage with fellow oversight bodies of other jurisdictions. The IPC met individually with representatives from the Netherlands, Norway and Australia. He also presented at the annual conference of the Norwegian oversight body in Oslo.

5.15 Groups of oversight organisations gathered for the Five Eyes International Oversight Review Council (FIORC) in Washington, the International Intelligence Oversight Forum in Strasbourg and the EIOC, which, as mentioned at 5.2, was hosted this year by the IPC in London.[22]

5.16 Returning to meeting together in person added substantial value to our international engagement. Discussions often focused on transparency and technological advancement, as such challenges are usually faced by many in the room. In addition, dialogue continues through joint working groups and collaborative projects that aim to enhance oversight procedure and share good practice.

22 See: https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-partnerships/icig-fiorc; and https://www.ipco.org.uk/news/uk-hosts-european-intelligence-oversight-conference/

6. Technology Advisory Panel

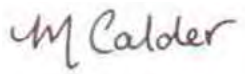
6.1 In accordance with section 246(6) of the Investigatory Powers Act 2016 (IPA), the Technology Advisory Panel (TAP)'s annual report to the Investigatory Powers Commissioner (IPC) must be copied to the Secretary of State. The 2022 report was submitted in 2023 and is reproduced below.

Foreword from Dame Muffy Calder, Chair of the TAP

The ability to meet again in person during this past year, especially to attend inspections, make visits, attend and give briefings, and offer technical advice and support, has been very welcome. This has enabled the TAP to make progress in several areas that had to be paused during the worst of the pandemic; it has been a productive and busy year.

The relationship with the Investigatory Powers Commissioner Sir Brian Leveson, the Judicial Commissioners, and all of the staff at the Investigatory Powers Commissioners Office (IPCO), continues to be very positive and constructive. We welcome their requests and their interest in our independent programme of work.

I thank Sir Bernard Silverman for his outstanding efforts to establish and lead the TAP since its inception. I took over the role of Chair from him during this past year and thank everyone at IPCO for their support.



Dame Muffy Calder, FRSE FREng, Chair of the Technology Advisory Panel

Remit of the Technology Advisory Panel

6.2 The Technology Advisory Panel (TAP) was set up under the Investigatory Powers Act 2016 ("the Act") (paras 246-247). Establishing and maintaining the TAP is a responsibility of the IPC but the TAP may also give advice to relevant Ministers. The TAP has a dual function under the Act: to advise about the impact of changing technology, and to advise about the availability and developments of techniques to use investigatory powers while minimising interference with privacy. In the definition of the panel's remit, "technology" is taken to be interpreted broadly, to include all relevant areas of science and mathematics. The remit of the Panel does not extend to consideration of matters of law, partisan politics or moral philosophy. The TAP is not a decision-making body, and its advice cannot constrain any decision of the IPC or of any part of the Government.

Membership of the TAP

6.3 The Chair of the TAP as of 1 March 2022 is Professor Dame Muffy Calder, Vice-Principal and Head of the College of Science and Engineering at Glasgow University, and previously the Chief Scientific Adviser for Scotland. She is Professor of Formal Methods (Computing Science). TAP members during 2022 were:

- Daryl Burns, who has worked in cryptography and cyber security for over 30 years and was Deputy Chief Scientific Advisor for National Security;
- John Davies, who has an extensive technical background in both government and private industry roles;
- Professor Derek McAuley, Professor of Digital Economy in the School of Computer Science at the University of Nottingham;
- Professor Richard Mortier, Professor of Computing & Human-Data Interaction at Cambridge University, and President of Christ's College;
- Professor Sarvapali Ramchurn (Gopal), Professor of Artificial Intelligence, Turing Fellow, and Fellow of the Institution of Engineering and Technology. He is Director of the UKRI Trustworthy Autonomous Systems hub and Co-Director of the Shell-Southampton Centre for Maritime Futures; and
- Sir Bernard Silverman FRS, formerly Chief Scientific Adviser to the Home Office and Emeritus Professor of Statistics at Oxford University. Sir Bernard was Chair of the TAP until 1 March 2022 and remains as a Panel member until July 2023.

6.4 Sir Bernard stepped down from his role as TAP Chair during 2022. He was recruited as the inaugural Chair of the TAP in 2017 and has been responsible for creating the Panel and shaping the direction of the TAP, a completely new entity under the Investigatory Powers Act 2016 (IPA). Sir Bernard was reappointed to act as a Panel member until July 2023.

6.5 The IPC appointed Professor Dame Muffy Calder to take on the role of TAP Chair as of 1 March 2022. Given the technical background and security clearance required for this role, an internal candidate was selected; Dame Muffy has been a member of TAP since 2018.

6.6 TAP members are remunerated at an agreed daily rate. During 2022 members contributed an average of 20 days each to TAP duties. The TAP is supported by a Secretary who is a part-time (50%) civil servant.

6.7 In the interests of transparency, the TAP aims to publish as openly as possible. The biographies of all TAP members are shown on the IPCO website, and a Register of Interests of panel members has been compiled and published on the website and is reviewed on an annual basis or where significant changes need to be noted. This is to prevent any potential conflict of interest. Where security considerations allow, advice and guidance given to the IPC and his staff are published openly.

Activities undertaken by the TAP and its members during 2022

6.8 As we have emerged from the pandemic, arranging meetings and briefings has proved easier and in particular, participating in visits and discussions at a higher classification level has been much more feasible.

Review of the Investigatory Powers Act 2016

6.9 TAP members have continued to participate in discussions with IPCO and the Home Office in relation to the five-year review of the IPA.

Meetings

6.10 Formal panel meetings took place in January, March, (virtual meetings), April, June, September and December 2022 (in-person meetings). All meetings and actions were recorded formally.

6.11 Formal biannual meetings between the IPC and the Chair of the TAP took place in June 2022 and November 2022. The IPC's Chief Executive was also present. Both meetings were recorded formally.

6.12 At the March IPCO Day event, Sir Bernard Silverman described the process of inaugurating the TAP in 2019.

6.13 A member of the TAP attended an inspection of the Equities Process.

6.14 TAP members participated in a number of IPCO inspections including at the Secret Intelligence Service (SIS), the Government Communications Headquarters (GCHQ), the National Crime Agency (NCA), HMP Glenochil, the UK National Authority for Counter Eavesdropping (UK NACE) and TARIAN, the Welsh Regional Crime Unit.

6.15 Members of the TAP attended relevant elements of the ICDDF22 (International Communications Data and Digital Forensics) Hybrid Event held in March.

6.16 The TAP Chair gave two introductory sessions about the TAP to four new Judicial Commissioners , explaining the TAP's role and how the TAP works with IPCO. The TAP also gave briefings to the Judicial Commissioners on Speaker Recognition and Internet Connection Records (ICRs). The TAP is always available to respond to technical questions from the Judicial Commissioners.

6.17 TAP members joined a small oversight sub-group being given updates on modern developments in computer power and capabilities by the UK intelligence community (UKIC).

Metrics of Intrusion

6.18 Following a TAP paper on Intrusion Key Concepts issued last autumn 2021, further work on this topic has continued. A planning session took place at Glasgow University in April to prepare for a June workshop on Metrics of Intrusion with the IPC, other IPCO representatives, and one external expert, Dr Marion Oswald, a lawyer from Northumbria University who has extensively researched the topics of privacy and intrusion.

6.19 The June workshop was well-received with wide ranging discussions on privacy and how to measure and compare levels of intrusion, with the aim of getting all parties to consider how judgements are made about the relative intrusion of different methods and whether this can be aided by metrics. The session was a mixture of presentation and small group working to explore the attendees' experience and how they judged levels of intrusion in practice.

6.20 A formal outcome from this workshop was the creation of two short papers, (an Aide-Memoire and a longer guidance paper), detailing factors for IPCO to consider when dealing with potential intrusion. As this is a subject of great interest to several parties, the TAP Chair has now briefed a number of people on this topic. The two papers have been shared with external parties and will be published on the IPCO website in due course along with a request for any feedback. A further paper concentrating on communications data in this context is being prepared for the Office for Communications Data Authorisations (OCDA).

6.21 Following this workshop, Dame Muffy, alongside Dr Marion Oswald, has been working with the Centre for Emerging Technology and Security (CETaS) on a research project on "Assessing Proportionality of Privacy Intrusion of Automated Data Analysis". This research commission from CETaS (C) covers a cross-disciplinary network of experts from across the UK under the Turing Institute. Muffy and Marion are involved in this research commission (under the aegis of their academic roles) but will draw the TAP into this work. There is a two-fold role here: i) CETaS is commissioning research on automation and Machine Learning and proportionality from Muffy and Marion (plus TAP) and ii) Muffy has a voice and involvement with the CETaS Governing Board. A range of Interviews took place during October 2022 and research is ongoing.

Publications

6.22 The formal TAP Annual Report for 2021 was finalised. An OFFICIAL SENSITIVE version was sent to the Home Secretary, the Scottish Cabinet Secretary for Justice and IPC and an unclassified version was sent to IPCO for publication in the full IPCO report.

6.23 An unclassified paper on the Cloud, written as a general guide for IPCO, was published on the IPCO website.

6.24 A small amendment was made to the TAP Working Protocol (the agreement between the IPC and the TAP Chair). This, along with the TAP Strategy and the TAP's annually reviewed Register of Interests, is available on the IPCO website.

Technical support and advice

6.25 Technical support was provided to several inspections and other IPCO discussions. TAP members accompanied inspections at SIS and GCHQ and HMP Glenochil, as well as visiting UK NACE and TARIAN, the Welsh Regional Crime Unit, at the request of IPCO for technical support. A number of ad-hoc queries by Inspectors, IPCO Legal and Judicial Commissioners were addressed informally. Examples of the queries addressed to the TAP included:

- The TAP was asked by IPCO to give technical advice in relation to an LPP material handling issue arising from one of the Intelligence Agencies. This assisted the IPC to reach a regulatory position on the issue.
- The TAP was asked to provide technical support to IPCO on an issue emerging from an Intelligence Agency in relation to Bulk Communications Data. This requested a simple explanation for the Judicial Commissioners (JCs) and advice on the level of collateral intrusion.
- A TAP member responded formally on behalf of the Chair to a classified letter on a specific subject.
- Following an earlier inspection of bulk powers at GCHQ, the IPCO Inspectorate requested that the TAP pursue a specific topic and provide technical advice to the Inspectorate prior

to the next inspection of these powers in Spring 2022. A TAP member provided some written technical advice to IPCO.

- The TAP was asked to support IPCO by joining discussions at the NCA and at the Metropolitan Police in relation to new Targeted Equipment Interference (TEI) technical capabilities being developed. Technical demonstrations were given to the TAP following the initial meetings and the topics have been thoroughly discussed across IPCO/TAP.
- The TAP was requested to assist IPCO in ensuring the technical accuracy of proposed more consistent wording for warrant applications in relation to a specific technique widely used by police forces.
- The TAP was asked by the Inspectorate to advise on a Directed Surveillance Authorisation (DSA) question which had arisen in the SE Regional Organised Crime Unit (SE ROCU).
- The TAP was asked to attend the IPCO inspection at the NCA to give technical support as required to the Inspectors and JCs.
- IPCO requested TAP assistance in determining whether specific technical devices could be classed as "computers". A further request related to telematics and whether specific components should be considered as Comms Data.
- IPCO has requested a paper from the TAP on Two-Factor-Authorisation (2FA).
- IPCO has asked for some TAP advice on cryptocurrencies.

6.26 A TAP member carried out some work at the IPCO Chief Executive's request, to consider what technical knowledge is required by the Inspectorate.

6.27 Briefings and papers were prepared at the request of the IPC and IPCO inspectorate or at the TAP's own volition on the following topics:

- A briefing plus a paper on the Cloud, written as a general guide for IPCO and published on the IPCO website.
- Following a query from IPCO, a paper explaining Hashing Functions for internal IPCO purposes was written and made available to IPCO.
- Speaker recognition. The TAP created a non-technical summary for IPCO on this topic.
- Following a technical briefing from an expert on Telematics and also on 5G/6G, a short summary paper was produced for IPCO.

Visits, External Briefings and Liaison

6.28 TAP members visited various locations for briefings and discussions including:

- The TAP received a briefing from IPCO on the Bilateral Agreement between the United States and the United Kingdom.
- The TAP attended an in-person meeting with staff from Canada's National Security and Intelligence Review Agency (NSIRA) Secretariat. This was a follow-up to an earlier online meeting in 2021 and was a valuable discussion. The TAP has agreed to continue meeting with NSIRA online every six months and had a further very useful discussion in December 2022, covering a range of topics including Metrics of Intrusion.
- The TAP held very useful meetings/discussions with Professor Alex van Someren, Chief Scientific Officer for National Security, and with Professor Paul Taylor, Chief Scientific Officer for Police, both of which covered the role of the CSAs and the role and activities of the TAP, focussing on a few current pieces of work.

- Dame Muffy had a further discussion with Alex van Someren, Chief Scientific Advisor for National Security, on when publicly available datasets, rather than synthetic, are required for research. A further meeting for the TAP to discuss this with Alex took place and the TAP Chair took an action to raise this topic at the Prime Minister's Council for Science and Technology.
- The TAP wished to explore developments of 5G/6G technology in more detail and arranged a visit to a major Telecommunications Provider to hold technical discussions on this topic, especially the challenges arising from recent and planned technological developments.
- The TAP received a technical briefing from an expert in Telematics, a topic likely to be of increasing importance.
- A TAP member accompanied IPCO representatives at the EIOWG (European Intelligence Oversight Working Group) meeting in Berne in March. The following EIOWG meeting took place in London in October and the TAP used the opportunity to hold technical discussions with their European counterparts. The TAP Chair attended the subsequent higher-level EION (European Intelligence Oversight Network) meeting and gave a presentation on Metrics of Intrusion as well as making a presentation on technology in oversight with a Norwegian colleague.
- The TAP was given an update by the NCA on the status of the trial of Internet Connection Records.
- TAP members visited UK NACE to gain an understanding of their role.

Ongoing discussions

6.29 A frequent call on the TAP is to explain the technical workings of devices and to clarify which aspects of law apply to them. The definition between TI, TEI, DSA, and elements covered by the CMA is not always black and white. The TAP held a workshop on "Interpreting Technical Language in the IPA" with members of the IPCO Legal team to discuss the nuances between these elements.

7. The Office for Communications Data Authorisations

Overview

7.1 The Investigatory Powers Commissioner (IPC) is responsible for both the Office for Communications Data Authorisations (OCDA) and the Investigatory Powers Commissioner's Office (IPCO). OCDA operates out of offices in Manchester and Birmingham, from 7.00am to 10.00pm, seven days a week, with a total current complement of approximately 100 staff.

7.2 OCDA's mission has two strands:

- to protect the human rights of individuals from unjustifiable intrusions by the State as an independent body authorising access to communications data (CD) when it is lawful, necessary and proportionate; and
- independently to assess, in a professional and efficient manner, the lawful acquisition of CD by a public authority in order to meet its function of protecting the public.

Managing operations effectively

7.3 We began 2022 continuing to manage the impact of Covid-19. This saw several changes in health and safety guidance which affected our working practices, in particular for staff attending the office. We continued our regular dialogue with the authorities who submit applications to keep them up to date with our operational approach.

7.4 Following the removal of the remaining restrictions in March 2022, we trialled the hybrid working approach which had been originally scheduled to commence in 2021. The trial explored the security implications of staff continuing regularly to work from home while maintaining a regular office presence to consider the higher classification applications.

7.5 The trial proved to be a positive move for us in managing our volumes effectively. The flexibility helped mitigate some of the impact caused by the increased level of staff turnover during the early part of 2022 and enabled us to continue to manage the volume of applications well within service level expectations.

7.6 The trial also successfully tested amended operating hours for higher classification submissions and, following discussions with the relevant authorities, our office operating hours of 8:00am to 6:00pm (weekdays) and 8:00am to 4:00pm (weekends) were set as business as usual.

Workflow

7.7 Our analysis of applications submitted in previous years was once again invaluable in helping us estimate the increase in volumes expected during 2022. We discussed with colleagues from IPCO and across the CD community factors that could affect application

numbers. These factors included changes to legislation, new CD gathering techniques or operational resource changes.

7.8 As shown in table 7.1, the total number of applications received in 2022 was 270,842. Throughout the course of the year, we received consistently more applications than the corresponding period in 2021. The final figure was 10% higher than in 2021.

7.9 The table also shows a year-on-year decrease in the proportion of applications being returned for rework or rejected. This demonstrates the continual improvement in quality of applications for CD by submitters and is likely in part due to the feedback they receive from both OCDA and IPCO.

Table 7.1 Applications submitted to OCDA, 2020 to 2022

		2020		2021		2022	
Total applications		226,383		245,272		270,842	
Decisions made		223,322	98.6%	242,535	98.9%	266,755	98.5%
Of which	Authorised	199,482	88.1%	222,009	90.5%	245,125	90.5%
	Returned	23,596	10.4%	20,244	8.3%	21,529	7.9%
	Rejected	244	0.1%	282	0.1%	100	0.04%
Withdrawn		3,051	1.3%	2,736	1.1%	4,087	1.5%
Applications with no decision at year end (31 December)		10	0.0%	1	0.0%	0	0.0%

7.10 One reason given for the increase in application numbers is the increased law enforcement focus on County Lines criminality, where we see a continuing reliance upon CD for investigative purposes.

7.11 In 2022, we saw the first test of the full OCDA appeal process when a rejected CD application went through all appeal stages. The application centred around the threshold of the legal term "grossly offensive" when considering malicious communications. Although there had been discussion between us and the relevant police force, it was agreed that consideration by the IPC was required. A thorough review of the facts was undertaken and the IPC upheld the decision to reject the application. This first test of the process in its entirety has caused us to review the various stages and, following discussions with the public authorities, a new process with amended timeframes and improved instructions will be issued in 2023.

Returns for Rework (RfR)

7.12 In our 2021 report, we set out the reasons why applications were returned to the requesting authority when the Authorising Individual (AI) was not satisfied that the case for obtaining CD was fully and completely made out. The number of applications we returned for rework during 2022 was an illustration of the level of scrutiny that was applied to each and every application. Despite the ongoing pressures of the pandemic and the high volume of applications received, the data shown below provides assurance that our high quality of case consideration has remained consistent.

7.13 Table 7.2 highlights that of the 27,197 applications returned for rework to the submitting authority, the primary reason for doing so was that an AI did not believe the application met the necessity requirements. Some of the other reasons given were more technical

in nature but all related in some way to inadequacy or lack of clarity in the information provided in the application. The information on returns for rework is shared regularly with law enforcement and public authorities to help them get applications right first time.

Table 7.2: Returns for Rework (RfR) reasons, 2020 to 2022

	2020		2021		2022	
Reason	Number of Returns for Rework	Proportion of Returns for Rework	Number of Returns for Rework	Proportion of Returns for Rework	Number of Returns for Rework	Proportion of Returns for Rework
Necessity	2,832	12%	4,389	18%	4,720	17%
Proportionality	2,832	12%	2,988	12%	4,135	15%
Dates/Times	2,596	11%	3,516	15%	3,669	13%
Consequential ticked/not ticked	1,888	8%	1,383	6%	2,129	8%
Accuracy	1,652	7%	1,922	8%	1,725	6%
Consequential Justification	1,652	7%	1,805	8%	1,667	6%
Attribution	1,416	6%	1,244	5%	1,657	6%
Collateral intrusion	1,180	5%	1,000	4%	1,592	6%
Forward facing	944	4%	952	4%	1,025	4%
Data Type	944	4%	587	2%	695	3%
Other (up to 21 categories)	5,663	24%	4,183	17%	4,183	15%

Note: Applications can be returned for rework for more than one reason. Therefore, the total number of Returns for Rework reasons exceeds the number of applications returned in table 7.1.

Organisational development

7.14 In early 2022, we delivered improvements to our bespoke case management system which were developed in conjunction with Home Office technical colleagues who specialise in CD. The changes have already been beneficial in minimising the number of avoidable errors and have contributed to increasing our efficiency.

7.15 Throughout 2022, we continued to assist with training and awareness as part of the National Single Point of Contact (SPoC) Accreditation course delivered by the College of Policing. This allows us to meet face-to-face with newly recruited SPoC officers from all law enforcement agencies (LEAs) and wider public authorities (WPAs). Such an introduction ensures that key aspects of OCDA's work and the basic requirements sought in reviewing CD applications were clearly outlined to this group of officers who perform a key role in the CD authorisation process.

7.16 We published the second edition of the OCDA Operational Digest in January 2022. The Digest shares relevant parts of the evolving internal guidance for our AIs with the wider community of SPoCs and Senior Responsible Officers in public authorities. It details the minimum standards expected by OCDA in relation to the practice and the presentation of applications for the acquisition of CD. The second edition contained important updates

on guidance in relation to proportionality, collateral intrusion, privileged and confidential information and the offence of Misconduct in Public Office.

7.17 In the latter part of 2021, we had invited some external analysis and challenge to our decision-making process through a piece of collaborative work with the University of Essex. Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens undertook a series of semi-structured interviews with OCDA operational staff regarding the organisation and their role. This report was finalised in early 2022. Following an internal review of the findings, we focussed on three themes emerging from the report: defining our independence; maintaining consistency of our considerations; and mitigating against AIs developing a law enforcement mindset. These themes have been used to develop an action plan led by our staff, the aim of which is to help us stay true to our mission.

7.18 We continued to manage staff turnover by completing our largest recruitment campaigns for AIs since our formation. The removal of Covid-19 restrictions also enabled a return to a dedicated face-to-face induction programme for new starters, helping to build stronger relationships between colleagues at work. These new staff have been vital in ensuring we could cope with the demand towards the end of 2022 and the predicted increases in the coming year.

7.19 In summary, 2022 posed a number of challenges to OCDA, all of which were handled effectively. We look forward to continuing to discharge our role in 2023, in what will hopefully be our first fully operational year without pandemic restrictions.

8. MI5

Overview

8.1 Throughout 2022, we conducted a series of inspections across the full range of investigatory powers used by MI5. In addition, MI5 provided regular briefings to our Inspectors and Judicial Commissioners on evolving methodology and complex technologies. These briefings continue to help us identify areas for closer scrutiny at our inspections.

Findings

8.2 As has been the case in previous years, we continue to assess that there is a good level of compliance across MI5 in respect of its use of investigatory powers. MI5's use of these powers and our inspection findings are discussed in greater detail below.

8.3 In our 2021 report, we flagged our concerns about particular weaknesses in the authorisation by MI5 of directed surveillance. It is reassuring that significant steps have been taken to remedy this issue, although we note that, given the need to deploy new training, processes and some new technology, it will take some time to reach full compliance.

8.4 Last year, we started an in-depth review across all three intelligence agencies of the handling of legally privileged material which has no intelligence value but is included within material that does have intelligence value. Following an extensive investigation including a series of detailed briefings and a review of previous correspondence on this matter, the IPC ultimately concluded that the MI5 process was not compliant. In response to the IPC's investigation, MI5 has now commenced a review of its process and we expect to be able to provide an update on progress in next year's annual report.

Covert human intelligence sources

8.5 In line with previous years, based on the records reviewed, MI5 covert human intelligence sources (CHIS) compliance remained strong, with no areas of non-compliance found during the annual inspection conducted in October 2022.

8.6 Some progress has been made with providing Inspectors with access to the necessary CHIS records to enable us to conduct our review, that must be kept in accordance with the Regulation of Investigatory Powers (Source Records) Regulations 2000 and paragraphs 7.4 to 7.7 of the CHIS Code of Practice.[23] In some cases, we were provided with the records necessary for us to conduct our review, but not in all of the cases that we selected for

23 See: https://www.legislation.gov.uk/uksi/2000/2725; and https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1123687/Revised_CHIS_Code_of_Practice_December_2022_FINAL.pdf

review. This was due to our requirements not being understood fully by some of the MI5 staff responsible for the compilation of the records prior to the inspection. A more consistent approach is still required and we continue to work with MI5 to ensure that all of the necessary records are made available for future inspections.

8.7 Overall, CHIS activity was managed highly professionally. Much evidence was seen of the serious considerations that MI5 gives to the risks and appropriateness of this intrusive activity when considering authorisation.

8.8 In 2022, we commenced an investigation into an historical CHIS case. We will report on this further in our 2023 report.

8.9 MI5's use of Criminal Conduct Authorisations (CCAs) for CHIS has been closely inspected. We found its use of such authorisations were necessary and proportionate thus far.

8.10 While we are unable to confirm or deny whether MI5 has recruited any juvenile CHIS, we are satisfied that it has the appropriate policies and practices in place regarding the recruitment and running of juvenile CHIS and also regarding the obtaining of confidential material.

Directed surveillance

8.11 MI5 processes for the authorisation and then on-going review of directed surveillance continued to present some weaknesses. We saw evidence of some Authorising Officers (AOs) giving insufficient regard to their responsibilities under the Regulation of Investigatory Powers Act 2000 (RIPA), as well as a failure by applicants adequately to record surveillance outcomes in some of the cases inspected. MI5 has made important investments to address these issues; these have started to have a positive impact on compliance but it will take some time for these to become embedded across the organisation.

8.12 MI5 continued to develop additional means of surveillance to respond efficiently to diverse and hard-to-detect threats to UK national security in a manner that was RIPA compliant. This is a complex area and we found that MI5 was taking appropriate measures to expand its capabilities while remaining compliant with the legislation.

Targeted interception (TI), targeted equipment interference (TEI) and property interference

8.13 MI5 continued to make use of combined warrants under Schedule 8 to the Investigatory Powers Act 2016 (IPA) and we therefore conducted combined inspections looking at targeted interception (TI) and targeted equipment interference (TEI) authorisations. A number of MI5 warrants are multi or combined warrants and they often include property interreference where this activity is necessary and proportionate. Property interference warrants are therefore inspected as part of the TI and TEI inspections.

8.14 Overall, we were satisfied that MI5 had achieved a high level of compliance with the IPA in these areas.

Thematic warrants

8.15 During inspections, we examined a number of thematic warrants where applications had been made for both major and minor modifications to add new subjects and factors. All

of the modifications we reviewed were properly authorised and consistently completed to a high standard, with a clear rationale for adding or removing factors. Each modification we saw clearly demonstrated the necessity and proportionality case, as well as linking the new factor or individual to the subject and purpose of the warrant. If there was any change in potential collateral intrusion as a result of a new factor being added, this was clearly addressed. We saw good evidence that factors were being deleted promptly when no longer required, demonstrating good housekeeping.

Specificity of thematic warrants

8.16 The Codes of Practice allow for some thematic warrants in specific cases to use a general description of the people who are subject to the warrant rather than name or describe them all individually. This is because it has not been reasonably practicable to include all the details at the time of authorisation due to factors such as the speed and pace of the investigation. It needs to be made clear within the application why this approach is justified and this is assessed by Judicial Commissioners on a case-by-case basis. MI5 has a number of these thematic warrants which include a general descriptor of subject matter details. An example of where this approach might be necessary could be MI5's immediate response to a terrorist incident that has occurred where not all of those involved have been identified. We examined many of these in detail and we tested the necessity for the general descriptor in the accompanying paperwork and during briefings from operational teams. We found that MI5 was using this to an appropriate standard and, in the cases we examined, that the uses of a general descriptor were all justified.

Communications data (CD)

Bulk communications data (BCD)

8.17 In 2021, due to Covid-19 restrictions we were unable to undertake an in person inspection to examine the work of the internal audit team which assesses the justifications made by staff to examine BCD.

8.18 In 2022, however, we had extensive engagement with this team during our inspections of BCD, bulk personal datasets (BPD) and data safeguards. The team updated us on the progress it had made in establishing additional audit capabilities and assessing compliance of, for example, MI5's recorded justifications to undertake the examination of BCD and BPD. The team also briefed us on how its work is making a significant contribution to checking and assuring compliance within the now-adopted "three lines of defence" model.

8.19 Our return to full on-site inspections in 2022 meant we were able to access the system used by MI5's investigators and analysts to record why the examination of specific data is both necessary and proportionate. Taking account of the expanded capability of the internal audit team, we concentrated on examining requests that sought data on individuals who held a profession that possibly handled confidential information, to ensure applicants justified any higher degree of intrusion or infringement of rights. Our audit concluded that the examination of BCD, during this time period, was justified and no requests to examine data raised concerns for us.

8.20 Overall, we concluded that MI5's recorded justifications for undertaking the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality.

Targeted communications data

8.21 The business areas focusing on acquisition of targeted CD were working to a high standard. Applicants' justifications were satisfactorily completed and were supported by strong internal governance procedures.

8.22 Our inspection of the system used by MI5 to acquire targeted CD allowed us to conduct a search across applications that referenced crime in their justifications, as these may require external authorisation. Examination of these requests revealed each had correctly recorded a statutory purpose of national security and an appropriate business area, such as international terrorism – meaning that these were all appropriately authorised internally.

Bulk personal datasets (BPD)

8.23 We suggested to MI5 that, as part of the renewal process for BPD warrants, there should be an assessment of how a particular dataset enriches the services' data systems, rather than each dataset being assessed in isolation. This would enable a fuller consideration of necessity and proportionality and provide an assessment of the aggregate impact upon privacy. MI5 initiated work to review how it reports the value derived from a BPD in its BPD warrant submissions, as well as to detail how MI5 will convey value derived statements within its BPD warrants in the future.

8.24 Consistent with our findings in 2021, MI5 continues to achieve a high level of compliance in this area.

8.25 No areas of non-compliance were identified. We made several observations, either to highlight areas of good practice, to fine tune the internal oversight regime, or to ensure that we are briefed on developing projects that could have an impact on compliance.

Safeguards

Background

8.26 The IPA requires compliance with safeguards concerning the retention and disclosure of material (for example, material obtained under an interception warrant), the retention and examination of material under the various bulk powers and with specific safeguards to be applied to certain sensitive categories of data (for example, items subject to legal privilege, confidential journalistic material, health records, sources for journalistic material, etc.). The IPA Codes of Practice contain guidance for practitioners in the application of these safeguards.

8.27 It should be noted that certain safeguards, if breached, can attract criminal sanction (for example, those relating to the examination, without lawful authority, of material relating to BCD, BPD, bulk interception (BI) and bulk equipment interference (BEI)).

Internal audit capabilities

8.28 There are some BPD systems in operational use where the internal audit team had limited or no auditing capability. This meant that, in the case of these systems, MI5 is less able to identify mistakes or procedural deficiencies and put remedial measures in place. Furthermore, the internal audit team had no visibility of a particular stand-alone system used to retain and examine a specific BPD. We made a recommendation for a review of this position and will revisit this area of work in 2023.

Handling Arrangements

8.29 The programme of work initiated within MI5 in response to the Donnelly Review included an initial review of the Handling Arrangements covering warranted data which the Home Secretary is required to approve under the IPA as a precondition of issuing warrants. MI5 and the Home Office are progressing this and we will provide further detail in our 2023 report.

Implementing the "three lines of defence" model for compliance

8.30 MI5 continued with its implementation of the "three lines of defence" model during 2022. We explained the concept of this model in our 2021 report.

8.31 We focused our attentions during 2022 on the approach MI5 took to implementing its second and third lines of defence. In relation to identifying and mitigating compliance issues, we undertook a deep-dive into its workings and the modelling used to identify compliance issues, the assessment of risks posed and its actions to undertake mitigation.

8.32 MI5 plans to develop an end-to-end approach to managing risks and issues. There is a clear structure for identifying, escalating and managing risk and issues, all of which are collated through one central point to ensure any issues that cut across different branches were not lost.

8.33 However, as we commented in our previous report, maintaining the model will require significant, sustained resource over the longer term. This is particularly relevant when compliance issues relating to IT systems are identified, as rectifying these are often costly and, assuming there is financial resource available, also take considerable time to implement effectively.

Legally privileged material

8.34 Legally privileged material can sometimes be acquired which has no intelligence value but is attached to non-privileged material that does (or might) have intelligence value and which needs to be retained. Last year, following concerns that either MI5 or IPCO may have previously misunderstood one another, we commenced an in-depth review of how this material was handled, exploring options for a common, compliant approach with MI5 and the other intelligence agencies.

8.35 The IPC concluded that the process currently used by MI5 was not compliant with the IPA. At present, MI5 retains some of this type of material in a manner where it states that it is being retained solely for the purpose of destruction. However, when we tested the process in detail, we noted that this material remained searchable in certain circumstances and therefore could be made available to analysts without Judicial Commissioner approval being obtained for its continued retention. We therefore concluded that such material was being retained for a purpose other than destruction and, accordingly, that Judicial Commissioner approval for the retention of this sensitive category of material should have been sought.

8.36 It was reassuring to note that, although it could be viewed, a warning label was applied in the primary analytical systems and internal guidance and training provided to analysts on how to handle any legally privileged material that was attached to material of intelligence value. As a result, none of the LPP material being retained in this way had been used in intelligence reports. MI5 has agreed to commence a review of how best to remedy this complex issue. We will monitor progress and report further on this next year.

9. Secret Intelligence Service (SIS)

Overview

9.1 We completed a series of inspections of the Secret Intelligence Service's (SIS) use of investigatory powers, conducted at regular intervals throughout 2022. The majority of our inspections relate to its work overseas and this year we were pleased to be able to return to conducting physical inspections of two overseas stations. Due to global Covid-19 restrictions, these had been carried out remotely during 2020 and 2021. We find these inspections particularly valuable as we are able to speak to a range of operational staff and discuss the challenges that they face, as well as get a greater understanding of how they utilise their investigatory powers. In conjunction with our London-based inspections, this enabled us to consider the level of understanding of the statutory requirements across SIS.

Findings

9.2 Overall, we concluded that SIS continues to maintain a good level of compliance with the statutory requirements governing its use of investigatory powers.

9.3 However, we also concluded that progress in addressing previous findings of non-compliance with the Regulation of Investigatory Powers Act 2000 (RIPA) has generally been slower than we would have wished, with several persistent recurring issues. We will therefore be enhancing our oversight of SIS compliance with RIPA during 2023.

9.4 In 2022, we conducted a detailed review of SIS's legacy datasets which were wrongly retained and reported to us as relevant errors. SIS's work continues to remedy this issue and we will provide a further update in 2023.

Covert human intelligence sources

9.5 Based on the covert human intelligence source (CHIS) records that we examined during our inspection of SIS, we consider that the CHIS activity conducted under RIPA continues to be necessary and proportionate.

9.6 SIS makes good assessments of the core issues of necessity, proportionality, collateral intrusion and the security and welfare of its agents but needs to improve the ways in which it can demonstrate consistently that these considerations are in compliance with RIPA and are appropriately reflected in the records that must be kept. This issue arises in the main because much of SIS's core activity concerns the use of human sources, the majority of whom are authorised under section 1 of the Intelligence Services Act 1994 (ISA) (falling outside of IPCO's remit) rather than under RIPA. It is SIS policy to maintain a single set of core source management policies and processes. While this approach is understandable, it has led, on occasions, to some difficulty in translating those processes into one that fully aligns with some of the more specific statutory requirements of RIPA.

9.7 As noted in our 2021 report, SIS had delivered mandatory RIPA training to over 400 staff. We saw clear evidence of the benefit of this training in improving compliance across the organisation and also with the improved understanding shown by most Authorising Officers (AO) of their role and obligations when authorising this activity. Despite these improvements, a minority of AOs still need to be clearer about what conduct they are authorising and ensure adequate review of the activity takes place at the appropriate time.

9.8 We also noted in 2021 that SIS was planning to introduce an IT solution to aid the management of the RIPA compliance process (for both CHIS and directed surveillance authorisations (DSA)). As of late 2022, this solution remained under active development, with deployment expected during early 2023.

9.9 SIS has now commenced its use of the Criminal Conduct Authorisation (CCA) regime for CHIS. There have been no issues of compliance concern to date but we will keep this under regular review.

Directed surveillance

9.10 In 2021, we noted our concern around a number of broadly drawn DSAs relating to activity at the lower end of the intrusion scale where we concluded that, while we were satisfied that the activities carried out under the authorisation were proportionate, the authorisations themselves were too broadly drawn. We asked SIS to address this as a priority. While most of these kinds of DSA had subsequently been cancelled or revised, we were concerned to find that a number remained in place and had not yet been revised. We will continue to review these as a priority.

Targeted interception (TI), targeted equipment interference (TEI) and property interference

9.11 Property interference warrants are inspected as part of the TI and TEI inspections as most activity is now covered in combined or multi warrants. We were satisfied that SIS's conduct in reliance on the TI and TEI warrants was necessary and proportionate and fell within the ambit of the warrant. We identified a small number of areas in which SIS could make amendments to relevant warrants to improve their clarity, but otherwise had no concerns about SIS's activities under the authorisations that we inspected.

Communications data

9.12 SIS is able to query certain bulk communications datasets (BCD) that are retained by MI5 and the Government Communications Headquarters (GCHQ) but it does not retain BCD itself in any other format. During our other UK intelligence community (UKIC) inspections, we examined the applications made by SIS staff to examine BCD. As in previous years, we confirmed that these requests by SIS were made pursuant to one of SIS's statutory functions, were linked to a valid operational purpose and contained a justifiable necessity and proportionality case.

9.13 As a result of our inspection activity, we were content that the small number of targeted CD authorisations that SIS had made were compliant.

9.14 As in previous years, SIS evidenced a very well maintained and compliant process.

Bulk personal datasets (BPD)

9.15 SIS has matured in its approach to compliance with the IPA in respect of bulk personal datasets (BPD), especially in respect of the BPD data safeguards; it is now seeking to streamline its processes and identify practices that have become unnecessarily bureaucratic.

9.16 Our review of the justifications used to examine BPDs was conducted partly via a briefing from SIS's Compliance Monitoring Team and senior managers who contribute to maintaining SIS's compliance. We were informed by the auditors that the standard of justifications recorded were continuing to improve and we tested and inspected the evidence for this during our Safeguards inspection (see paragraph 9.27 below re internal audit capabilities).

9.17 In our 2021 report, we described how SIS had identified a number of legacy datasets that it held which, since the introduction of the Investigatory Powers Act 2016 (IPA), now constitute BPD. These had been retained in error without a relevant warrant to cover continued retention, as is required by the IPA. We also identified some serious gaps in SIS's capability for monitoring and auditing of systems used to query and analyse BPDs. During 2022, we reviewed SIS's progress dealing with legacy data and its internal audit capabilities as set out below (see paragraph 9.18 onwards and paragraph 9.27 onwards respectively).

Legacy data

9.18 Throughout 2022, SIS has been discussing the move towards a new media management tool and the deletion of old media. Through this process, SIS identified a small number of legacy files that may constitute BPD under the IPA. SIS concluded that the majority of these datasets should have been deleted and had been retained in error; these were subsequently reported to us as relevant errors. We undertook a detailed review of this matter during 2022 and were impressed with the work conducted to date to rectify this historical issue.

9.19 SIS has kept IPCO and the Foreign Secretary updated on the progress achieved throughout 2022.

9.20 We are continuing to work with SIS to monitor its progress in transitioning towards a modernised media management system and whether legacy BPD has been discovered and we will provide a further update on this area of work in our 2023 report.

Section 7 of the Intelligence Services Act 1994 (ISA)

9.21 SIS continues to demonstrate clear and careful consideration of the relevant factors when seeking authorisation to undertake activity under section 7 of the ISA, exercising sound judgement when considering complex operations, often in highly challenging circumstances. Internal records of decision making were also of a high standard and Ministers were briefed in a timely fashion in response to rapidly developing circumstances. We examined one case in particular which demonstrated the potential to yield a high intelligence dividend but was coupled with significant ethical, legal and operational issues. The case had been subject to a high degree of internal scrutiny and consideration by SIS before submission and we considered that the Foreign Secretary could conclude that the nature or likely consequences of acts done in reliance of this authorisation were reasonable.

9.22 Last year, we referred to the use of authorisations by SIS underpinned by internal records of reliance. SIS has simplified one of these authorisations in line with our previous recommendations. The new system uses a traffic light status with GREEN activities allowed under the authorisation, AMBER activities requiring internal authorisation and RED activities prohibited under this authorisation. We have recommended that applicants consistently adopt the terminology of the new system to maximise clarity about what is being authorised.

9.23 In our 2021 report, we also referred to a number of section 7 authorisations relating to a separate class of operations involving particularly complex legal issues. We looked at a number of such authorisations again this year. The standard of consideration remains high but SIS felt that there might be a better approach to setting out such submissions in future, with a greater emphasis placed on the extensive processes in place around the operational authorisation of this activity. We would be supportive of the proposed changes to such submissions if they help make the extent of the authorised activity clearer to the Secretary of State.

Overseas inspections

9.24 We examined the work undertaken by SIS at two of its overseas stations.

9.25 In the first country, we looked at a number of cases or activities authorised under the ISA and some that engaged "The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees". We made a single observation with regards to a possible detention case which had the potential to culminate in the death penalty under local law. We found that SIS had given extensive consideration to this case and had engaged with the Foreign, Commonwealth and Development Office (FCDO) in an appropriate manner. We observed that such cases underline the importance of SIS fully and clearly setting out all the facts so that the Secretary of State can make an informed decision (which is not to say that we felt SIS had failed to provide adequate information in this and earlier submissions). The extent of the risk and any uncertainty around local legal processes should fully be set out. While the need for the Secretary of State to fully be apprised of the facts is a general one, it is particularly relevant where there are uncertainties around the local legal system and ultimately the risk of the death penalty being applied.

9.26 In the second country, we examined the work undertaken by SIS involving the exchange of intelligence with local and Five Eyes partners in circumstances where The Principles were not engaged. We found all of the casework examined to be necessary in support of national security and reasonable in the circumstances. There were no cases that engaged The Principles during the period under review, but we were confident SIS officers in country and at headquarters were aware of the thresholds and would correctly identify when The Principles ought to be engaged and act appropriately.

Safeguards

Internal audit capabilities

9.27 Our 2021 review highlighted several areas of serious concern. We identified that there were some BPD systems in operational use where the Compliance Monitoring Team (CMT) had limited or no auditing capability; this means that, in the case of these systems, the CMT was unable to identify mistakes or procedural deficiencies and put remedial measures in place.

9.28 In 2022, we continued to monitor how SIS had progressed this work, meeting with senior members of the relevant teams. We were greatly impressed with the measures adopted to address issues raised in the ongoing review, which include:

- an increase in the staffing of CMT;
- an increase in the systems subject to audit either by means of an in-built audit capability or by retrospective manual intervention by the CMT; and
- an increase in the standards being achieved by users when completing their justifications to undertake examination of BPD.

9.29 SIS has impressed us in the way it has uplifted its audit capability, especially as many systems used in this activity pre-date the commencement of the IPA and were therefore not designed specifically to secure compliance with the provisions of the Act.

9.30 SIS also has some specific systems that, due to their age and origin, cannot be assimilated into the main systems. Such systems may only be accessed by a handful of analysts and require contemporaneous logs to be maintained registering why access to the material was necessary. The logs are then subject to manual examination by the CMT to verify that access was appropriate.

BPD Assurance Reporting

9.31 SIS has developed and implemented a mature process (originally commenced as a temporary measure to assist in its management and control of actions arising from our deep dives in 2021 and 2022) in relation to its audit capabilities and identification of errors that relate to the continued retention of legacy BPDs. The ongoing internal review process informs an internal report highlighting what is and what is not being achieved in a "dashboard" format. The process and the Assurance of Compliance Report assists SIS to assess its own compliance with, for example, the requirements of the IPA and the various Codes of Practice and its internal safeguards.

9.32 The process has been developed to implement the "three lines of defence model" to assist internal compliance and audit. We welcome this development as it greatly assists our oversight.[24]

Implementing the "three lines of defence" model for compliance

9.33 We noted SIS's maturing approach to the "three lines of defence model" and the development of a register of legal compliance risks. During our 2023 Safeguards inspection we will seek to examine how the register of legal compliance risks is formulated, how it assists SIS to identify and manage those risks at a team level and how these are escalated to panels, boards or steering groups within the organisation.

24 See: The three lines of defence | Position papers | Policy and research | IIAhttps://www.iia.org.uk/threelinesofdefence

10. Government Communications Headquarters (GCHQ)

Overview

10.1 Throughout 2022, we inspected the Government Communications Headquarters' (GCHQ) use of investigatory powers. Given the nature of GCHQ's core business, much of their operational activity is technically complex and we continue to receive regular briefings on its key areas of work, new capabilities and evolving technology. We find these briefings extremely useful and they continue to inform our inspection activity.

Findings

10.2 Overall, we concluded that there is a good level of compliance across GCHQ in respect of its use of investigatory powers. GCHQ's use of these powers and our inspection findings are discussed in greater detail below.

10.3 In previous years, we have outlined that our oversight of the Equities Process has been conducted on a non-statutory basis. With effect from December 2022, we are pleased to be able to report that our oversight of the Equities Process was placed on a statutory footing by virtue of the Investigatory Powers Commissioner (Oversight Functions) Regulations 2022.[25]

10.4 GCHQ has continued to make progress in implementing its response to the judgment in *Big Brother Watch v UK* and we are continuing to review and adapt our approach to inspecting how GCHQ makes use of its bulk interception (BI) powers.[26]

Covert human intelligence sources (CHIS) and directed surveillance

10.5 The inspection relating to CHIS and directed surveillance took place in December 2022. Several of the actions raised in the previous inspection had not fully been discharged and remain extant. These related to the need for individual CHIS risk assessments to be completed, for CHIS Authorising Officers (AOs) to specify the conduct they were authorising in a clear statement, and for better detail to be provided at review and renewal regarding what activity had been conducted and the value of this activity to the operation or investigation.

10.6 Two further actions were identified relating to the need for directed surveillance AOs to make a clear statement of the activity authorised and, in cases of the interception of communications with a directed surveillance authorisation under section 44(2) of the Investigatory Powers Act 2016 (IPA) (interception with the consent of the sender or

25 See: https://www.ipco.org.uk/what-we-do/additional-functions/equities-process/
26 See: from paragraph 3.7.

recipient). It would be better practice if the consent from the sender or recipient was evidenced in writing.

10.7 Notwithstanding the above actions, we were impressed with the improvements that have been made in the detail, specificity and AO's considerations in relation to directed surveillance.

10.8 In relation to CHIS, there had been a great deal of work undertaken to create a new IT system that would be the definitive repository of all records that are maintained regarding the management of CHIS cases. This system remains in development; however, it is expected that, when operational, it will replace and greatly improve on the previous record-keeping regime which was more fragmentary. We hope to be able to use this system for access to CHIS records in future inspections.

10.9 The 2021 legislative provisions for CHIS Criminal Conduct Authorisations (CCAs) have now been utilised by GCHQ and we were impressed by the thoroughness and quality of the authorisations in this regard.

Property interference

10.10 GCHQ has a small number of warrants issued under section 5 of the Intelligence Services Act 1994 (ISA) authorising interference with property. We were satisfied that the property to be interfered with under the warrants inspected could be objectively ascertained by GCHQ staff relying on these warrants. In all cases the activities authorised appeared necessary and reasonable.

10.11 We were made aware of an error with respect to one property warrant which had subsequently been remedied. However, it appeared that the error had not been reported to us as is required. We reminded GCHQ of the need to report errors in a timely manner and placed an action on GCHQ to report this formally and any other unreported ISA errors to us as a priority. GCHQ has since reported to us that there were no others.

Targeted interception (TI) and targeted equipment interference (TEI)

10.12 We were satisfied that GCHQ was achieving a high level of compliance with the IPA. We received comprehensive briefings from various teams and it was clear that compliance and continued necessity and proportionality of authorised activity is a focus for all staff involved.

Bulk interception (BI)

10.13 Due to a change in policy, GCHQ now records the necessity and proportionality justifications for its decisions to intercept particular bearers for target discovery purposes. It has also made changes to its processes to ensure that those bearers are not intercepted unless a necessity and proportionality justification is in place. The examples of those justifications that we reviewed during our 2022 inspection were completed to a high standard by GCHQ.

10.14 We reviewed a range of necessity and proportionality statements to justify promotion rules and concluded that these were of varying quality. While GCHQ had developed a new policy on the minimum required standards for these justifications, some of the samples reviewed

on our inspection did not meet these standards. We recommended GCHQ takes further steps to improve standards in this area.

10.15 Regarding selection for examination, we once again reviewed a sample of 200 necessity and proportionality justifications drafted by analysts. In 2022, we saw a significant improvement in the quality of these statements, compared with 2021. In 2022, 88% were passes, 11% were borderline and 1% failed to adequately explain the necessity and/or proportionality.

10.16 In 2022, GCHQ briefed us on some developing capabilities which would automate some of the decisions made at the early stages of bulk interception which GCHQ is currently making manually. Our assessment was that these capabilities will optimise GCHQ's collection of data through bulk interception; this should also mean that the bulk collection operation is more targeted overall (and therefore more proportionate), reducing the volume of data collected that is not of intelligence interest. This is a topic to which we will return in 2023, with the assistance of the Technology Advisory Panel (TAP).

The National Technical Assistance Centre (NTAC)

10.17 As part of our oversight of TI a one-day visit to the National Technical Assistance Centre (NTAC) was undertaken in August 2022. NTAC is responsible for the provision of lawful interception capabilities to the nine UK Interception Authorities,[27] managing the delivery of intercepted communications from telecommunication operators (TOs) and the processing and enrichment of that data. The purpose of the visit was to discuss developments in NTAC's role in supporting TI, including with regard to the UK-US Data Access Agreement (DAA). This covered the provision of TI material from a range of TOs (both overseas and UK) and the incidence and mitigation of any errors. NTAC also assists law enforcement to develop tools to process and maximise value from TI and non-TI data. We also used the visit to explore the basis on which data is shared, retained and deleted. We concluded that NTAC has effective systems and processes in place in respect of the provision of TI material.

Bulk equipment interference (BEI)

10.18 This year we examined a limited number of necessity and proportionality cases relating to activity conducted under BEI warrants, focussing our examination on business areas that would seek this activity on a less frequent basis. Overall, we found the standard of record keeping for activity conducted under BEI warrants to be of a high standard. Necessity and proportionality statements relating to action taken under BEI warrants were generally sufficient in content.

10.19 We continued to develop our inspection methodology in respect of newer capabilities authorised under BEI warrants. We addressed this at inspection through detailed briefings and discussions with the relevant teams, and by looking at a selection of the internal records of reliance that sit under the warrants, together with a selection of the necessity and proportionality statements.

10.20 EI operations are, by their nature, highly technical and complex, which means it is critical that BEI warrants clearly describe the conduct authorised. We found that GCHQ's operations were consistent with the descriptions in the BEI warrants which authorised them, but recommended that GCHQ reviews the wording of the conduct sections of the

27 GCHQ, SIS, MI5, the Ministry of Defence, His Majesty's Revenue and Customs, the National Crime Agency, the Police Service of Northern Ireland, Police Scotland and the Metropolitan Police Service.

warrants with a view to achieving greater alignment with the conduct actually described in the warrant applications themselves; this would improve clarity and consistency.

10.21 We also explored during the inspection whether caselaw in relation to BI, such as issues concerning Article 10 of the European Convention of Human Rights (ECHR), had any application in relation to BEI. As such matters are subject to ongoing live litigation, we have decided to postpone reaching a position in this regard until the conclusion of that litigation.

Communications data

Bulk communications data (BCD)

10.22 GCHQ's BCD systems and processes have been continually refined over the years and our inspection again confirmed that GCHQ is operating in full compliance with the requirements of the IPA.

Targeted communications data (CD)

10.23 Our inspection in 2022 concluded that processes used by GCHQ to acquire CD were working to a high standard. Applicants described in detail their justification of necessity and proportionality and these requests were supported by strong internal governance procedures. We identified a number of positive improvements in the working practices and development of staff within the Single Point of Contact (SPoC) cohort, who act as compliance gatekeepers.

Bulk personal datasets (BPD)

10.24 GCHQ's internal governance process for BPD is overseen by a Bulk Personal Data Panel, which meets to discuss contentious or complex issues relating to the retention of a dataset when required.

10.25 Following our inspection, we made a few observations but no formal recommendations. The systems and processes within GCHQ for managing the retention and examination of BPD are mature. We observed that members of staff had made a number of thoughtful and progressive changes to their compliance procedures, especially when handling BPDs. This process highlighted a few areas where GCHQ had improved its procedures, in particular in relation to internal audits, protective monitoring and governance.

10.26 Overall, the applications and directions authorising the examination of bulk material were drafted to a high standard and made explicit the reasons why it was necessary to undertake the conduct; regular renewals of search applications were also submitted when the searches took place over extended periods of time.

The Equities Process

10.27 During our inspection in January 2022, we continued to be satisfied that the Equities Process was working effectively and was producing reasoned decisions to either retain or disclose vulnerabilities, and that these were supported by appropriate evidence and recorded in sufficient detail. We were pleased to note that the Equities Oversight Committee (the senior group responsible for strategic oversight of the process, chaired by the Chief Executive of the National Cyber Security Centre) was now receiving more detailed written updates ahead of its meetings, compared to previous practice.

10.28 A theme emerging from the inspection was the extent to which the Equities Process touched on relevant operational activity conducted by other UK public authorities. Given that GCHQ operates the Equities Process on behalf of the whole of Government, we have asked for additional clarity about how GCHQ ensures that the Equities Process considers vulnerabilities that are discovered or acquired by other UK public authorities. We will report on progress made on this issue next year.

10.29 In December 2022, our oversight of the Equities Process was placed on a statutory footing by virtue of the Investigatory Powers Commissioner (Oversight Functions) Regulations 2022.

Section 7 of the Intelligence Services Act 1994 (ISA)

10.30 On the whole, we found GCHQ to be highly compliant with respect to activity conducted under section 7 of the Intelligence Services Act 1994 (ISA), and all documents were clear and well-structured.

National Cyber Force

10.31 This inspection was useful in helping us understand the command-and-control mechanisms that are in place at the newly formed National Cyber Force (NCF), including the way in which it relies upon warrants and authorisations obtained by GCHQ.

10.32 We received a series of excellent briefings on NCF activities, ranging from research and development, testing and training through to offensive cyber operations.[28] Staff were well informed and demonstrated good knowledge of the compliance regime. It was clear to us that appropriate consideration was being given to ensure that activities were necessary, proportionate, reasonable, that intrusion was minimised and that data was not retained any longer than necessary. We made one recommendation concerning the wording of a warrant submission, to ensure that GCHQ's risk mitigations are clearly presented and understood.

10.33 We concluded that the NCF had strong structures in place to oversee and manage offensive cyber operations in a compliant manner, and we were pleased to see evidence of the developing thinking around the interplay between offensive cyber operations and international human rights law.

Safeguards

10.34 The IPA safeguards inspection of 2022 focused on key issues identified during previous powers-based inspections (for example, BPD, BCD, BI etc.). This included reported errors and GCHQ's strategic compliance risk framework.

10.35 Overall, the inspection identified a very good level of compliance in the management of safeguards across all the required disciplines. The inspection team was given access to GCHQ's strategic risk assessment register, a comprehensive document continuously updated from the operational risks identified by diverse departments across the

28 Adding, deleting or manipulating data on systems or networks to deliver a physical, virtual or cognitive effect. Offensive cyber operations often exploit technical vulnerabilities, use systems or networks in ways that their owners and operators would not intend or condone, and may rely on deception or misrepresentation.

organisation. Here we were able to map out the risk framework and question the structure, which we found to be relevant and detailed.

10.36 We concluded that GCHQ's strategic compliance structure and overall compliance framework, in relation to safeguards in the IPA and the Regulation of Investigatory Powers Act 2000 (RIPA), were working to a good standard. It was clear from the material viewed and the briefings received that GCHQ maintains a high level of compliance with IPA and RIPA safeguards. Staff have the capability to raise a risk or compliance matter in the knowledge that it will be recorded and raised through solid procedures. The risks were well graded, assessed, and, when possible, mitigated at appropriate levels.

10.37 We noted a considerable and positive transformation in the management and administration of data shared with overseas partners. Responsibility for documenting, authorising and removing sharing streams now sits with one team and, with links to warranted material data, owners were able to confirm the legality of their request and if any Handling Arrangements were in place. Additionally, each request was risk assessed and reviewed, and only progressed on the authority of a policy and compliance manager.

10.38 In our last report, we highlighted how GCHQ had discovered the over retention of IPA material in a particular file storage area and had reported the matter to us as a relevant error. In December 2021, we undertook a deep dive inspection of this area with GCHQ and reported our findings in February 2022; we agreed a number of actions that GCHQ needed to complete to help prevent further issues. As previously indicated, the complexity of systems involved in GCHQ's programme of mitigation took time to design, resource and implement. However, GCHQ confirmed it had completed the work which would purge any over-retained data by January 2022. During the course of our inspections in 2022, we were given updates on the effectiveness of remedial work and examined the minutes of meetings held by senior managers who were tasked with implementing the rectifications. We noted the agency had also utilised the "three lines of defence model" to provide regular updates to their senior management group responsible for GCHQ's overall legal compliance. During 2022, GCHQ continued to dip sample the systems to verify the effectiveness of compliance controls in the file storage area.

Internal audit capabilities

10.39 Random audit checks of the justifications for selection are conducted retrospectively by, or under the direction of, GCHQ's Internal Compliance Team; in addition, the IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use. The results of these retrospective audits were provided to us during our inspections, and we were satisfied that these were comprehensive and robust.

10.40 The audit checks of analysts' justifications to examine bulk material have been in place since 2016 and are referenced in a number of our previous reports. We noted considerable improvement in the justifications made by analysts to examine bulk data, and in the steps taken by those auditing the justifications to improve standards via a compliance network that spans each of GCHQ's operational departments. The team collates statistics to identify areas of concern, so that it can focus future audits on missions or individuals who need to improve their justifications when examining bulk data.

Compliance Investigations

10.41 The Compliance Incident Investigation Team (CIIT) investigates errors and, if necessary, prepares error reports for the IPC. On a monthly basis, the Deputy Director Mission Policy

reviews errors and, as detailed previously, they can escalate any matter of concern to the Compliance Board. The team also aims to identify any error trends and to develop mitigations to enhance the compliance picture. Following the 2022 BCD inspection, the CIIT changed its guidance on how mistakes should be reported to encompass a wider set of potential instances and improve the data received by the team. The changes mean that the guidance now encapsulates all matters that relate to compliance and not just errors. Mission areas and the Compliance Network have now been asked to report all compliance matters to the CIIT.

Handling Arrangements

10.42 When considering the complex nature of IPA/RIPA safeguards and Handling Arrangements within GCHQ, and the breadth of our inspection, our report's conclusions were a positive reflection on what are, overall, compliant processes and systems. No actions or recommendations were made and the majority of observations were administrative or were included to fine tune current procedures.

Implementing the "three lines of defence" model for compliance

10.43 GCHQ has commenced its development and implementation of the three lines of defence model and we were given an in-depth briefing and had discussions concerning:

- introducing Data Safeguarding Teams and projects;
- applying a "three lines" mindset to safeguarding data;
- surfacing issues and making improvements using the three lines of defence model; and
- future developments.

10.44 We were also provided with documentation setting out in detail GCHQ's internal governance, and how oversight functions will fit within the three lines model. The maturing development and implementation of a three lines of defence model is a positive move towards identifying issues early before they escalate into risks, as well as bringing the advantage of delivering improved horizon scanning of potential future issues.

11. The Ministry of Defence

Overview

11.1 During 2022, we undertook inspections of the Ministry of Defence's (MoD) use of investigatory powers in the UK that are provided for under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA).

11.2 At the request of the MoD, we also continue to oversee the MoD's use of covert human intelligence sources (CHIS) overseas where there is no UK connection on a non-statutory basis. It has now been agreed with the MoD that this oversight should have a statutory basis; we will work through the options to achieve this with the Government over the coming months.

Covert human intelligence sources (CHIS) and directed surveillance

11.3 The MoD continues to achieve high levels of compliance, with excellent and detailed applications alongside what are usually well considered inputs from Authorising Officers (AO). However, this was not always consistent, with some AOs failing to evidence their considerations regarding necessity and proportionality and specify with precision what conduct they were authorising.

11.4 Following our 2021 inspection, we flagged the importance of the MoD properly understanding when its activity conducted physically outside of UK territory should still be subject to a RIPA authorisation due to the presence of a UK connection, such as the subject of interest being a UK national or likely to be subject to legal proceedings in the UK. As made clear in the Code of Practice, where such a "UK nexus" exists, the MoD should apply RIPA, especially as it does not have recourse to another means of authorising the activity (e.g., the Intelligence Services Act 1994 (ISA)). It should not rely on the non-statutory regime and only reserve this for activity which is both outside of UK territory and where no other UK nexus exists.

11.5 In 2021, we also highlighted that a Criminal Conduct Authorisation (CCA) granted under section 29B of RIPA is only valid if an authorisation for the use and conduct of a CHIS has been made under section 29A. The effect of this is that statutory CCAs are not available for CHIS authorised under the MoD's non-statutory process. These points were reiterated in our 2022 inspection.

11.6 In response to these two issues, the MoD has undertaken a major review of its RIPA policy and processes. At the time of our 2022 inspection, this policy was in the late stages of preparation but had not yet been implemented. We have been consulted on aspects of the new policy, which aims to address the substantive issues we have raised, as well as more generally improve and rationalise the MoD's use of RIPA.

Targeted interception (TI) and targeted equipment interference (TEI)

11.7 The Armed Forces conduct activities on land and in UK territorial waters and airspace which are covered by TI/TEI warrants. Each application to conduct activity goes into the detail of what equipment will be used, the location where it will be used, the duration of the activity, and the risk of collateral intrusion.

11.8 The warrants are also used by the Defence Science and Technology Laboratory (Dstl) to test new equipment. In limited circumstances, collected data may be kept for longer periods to allow analysis of the results. Testing and training is an essential part of the MoD's mission and the authorised activity allows the MoD to keep pace with new technical developments. We were satisfied that the MoD and its various units have a good level of compliance with the IPA and the Codes of Practice.

12. The Principles

Overview

12.1 This is the third year that we have overseen the "The Principles relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence relating to Detainees" (The Principles), which came into force on 1 January 2020.

Findings

12.2 Generally, we found there to be a high level of compliance from the six public authorities subject to The Principles (the Principles Partners), with a great deal of care being taken by them to assess accurately the risks and to follow both the letter and spirit of The Principles.

12.3 While we were satisfied that the National Crime Agency (NCA) was generally compliant with The Principles and was making appropriate risk assessments in the majority of cases, we were concerned about its use of thematic authorisations in certain circumstances, in particular where there was an unmitigated real risk of torture to certain categories of detainees. Paragraph 12.27 sets out further details on this, including our recommendations, which were all accepted and have all subsequently been discharged.

12.4 Given the high level of activity, the number of errors (two) or potential errors reported was low. MI5 reported a Principles error, but this was in a case where it was clear that there was no real risk of unacceptable conduct arising from the sharing of intelligence.[29] GCHQ reported a potential Principles error which we have subsequently assessed not to be an error.

Statistics

12.5 Table 12.1 sets out details on the number of cases reviewed under The Principles since they came into effect in January 2020.

12.6 The table below sets out the total number of cases in which the Principles Partners have referred to Ministers for a decision because there was a real risk of one or more of the categories of unacceptable conduct as set out in The Principles. They also include the number of cases which the Partners have proactively brought to our attention because they raised particular legal or policy issues – some of which have informed the findings presented in this report.

12.7 There are important caveats to the data presented here:

- first, an increase in cases which cross the threshold of real risk does not, necessarily, indicate that the Principles Partners have taken additional risks in their engagement

29 See: paragraph 12.10.

with overseas authorities. A single operation (such as, in response to a major terrorist plot) may generate a "spike" in referrals to Ministers, for example. As such, it will not be possible to conduct a straightforward year on year analysis of these figures to determine whether or not the overall level of risk associated with the application of The Principles has increased. Similarly, a reduction in the number of cases does not necessarily suggest a lower risk appetite has been adopted; and

- second, as The Principles makes clear, consulting Ministers does not imply that action will or will not be authorised, and the UK Government's clear stated policy is that the UK does not participate in, solicit, encourage or condone unlawful killing, the use of torture or cruel, inhumane or degrading treatment (CIDT), or extraordinary rendition.

Table 12.1: Cases reviewed under The Principles, 2020 to 2022

Number of cases reviewed		2020	2021	2022
Cases reviewed on inspection		93	68	104
Cases reviewed proactively due to contentious legal or policy issues		8	7	7
Triggers: Total number of all cases (not limited to those reviewed on inspection)	Personnel knew or believed torture, unlawful killing or extraordinary rendition would occur	0	0	0
	Personnel identified a real risk of torture, unlawful killing or extraordinary rendition and submitted for approval despite the presumption not to proceed in such cases (this may include cases where engagement is intended to reduce the risks of unacceptable conduct or where there is an imminent threat of serious harm to individuals including children)	2	3	8
	Personnel identified a real risk of cruel, inhumane or degrading treatment (CIDT) and submitted for approval	15	17	17
	Personnel identified a real risk of rendition and submitted for approval	3	0	0
	Personnel identified a real risk of unacceptable standards of arrest and/or detention and submitted for approval	28	34	54

MI5

12.8 Overall, we found MI5 to be highly compliant with both the letter and the spirit of The Principles. The forms used by MI5 to articulate Principles risk assessments were clear, easy to follow and completed to a high standard.

12.9 MI5 reported one Principles error during the year. This case involved sharing intelligence with a foreign partner organisation in circumstances where The Principles should have been considered but were, uncharacteristically, overlooked during a time-sensitive operation. This case engaged the passing of intelligence to a foreign authority concerning an individual detained by that authority. MI5 retrospectively assessed that its personnel did not "know or believe" that unacceptable conduct would occur, nor that there was a "real risk" of unacceptable conduct. There was therefore a "lower than real risk" under The Principles. Appropriate remedial action was taken in response to this error. A Principles risk assessment form was subsequently produced to cover further intelligence exchange in relation to that case.

12.10 We noted that MI5 was making greater use of thematic authorisations in circumstances where there was a "lower than real risk" and was making use of intelligence exchange logs to record information passed under these authorisations. We consider this to be an appropriate mechanism for dealing with lower than real risk activities.

12.11 We also noted that MI5 was beginning to increase the review period for thematic authorisations for sharing with countries where there is a "lower than real risk" from six to 12 months. We consider that this was appropriate.

Secret Intelligence Service (SIS)

12.12 During our June 2022 inspection, we reviewed the framework that we had recommended previously for gathering and assessing information about the end-to-end "pathway" for detention operations overseas conducted by foreign partners. We concluded that the framework provided a comprehensive set of questions to help gather all of the relevant information and recommended SIS incorporated it into its decision-making process. These questions are listed in the text box below:

Questions set out in the end-to-end pathway framework

Point of capture

1) Which services or agencies in the country have formal powers of arrest under domestic law?
2) Is there a real risk of unacceptable conduct at the point of arrest?
3) Is the detainee told of the reason for their detention at the point of capture? When are they told?

Initial detention

4) Where will the detainee be detained?
5) Is there a real risk of unacceptable conduct during this period?
6) Does the detainee have the ability to challenge the detention? If so, after how many days?
7) Who are they able to challenge it in front of? Is there a power to release them?

Safeguards against incommunicado detention

8) Is the detainee able to contact their family? If so, after how long?
9) Is the detainee able to consult a lawyer?

Subsequent detention

10) Are there any changes to the detaining authority before charge? If so, who is the new detaining authority?
11) Is the detainee moved to a different facility prior to charge?
12) Is there a real risk of unacceptable conduct during this period of detention?

12.13 We reviewed instances in which SIS had been made aware of allegations of mistreatment. In general, we were satisfied that these allegations had thoroughly been investigated and the conclusions accurately recorded. In one case, while we agreed with SIS's conclusion that the allegation lacked credibility, we considered it should have been recorded in a more structured way. We recommended that SIS introduces a list of structured questions for officers to use when assessing allegations of mistreatment.

12.14 SIS achieved good progress against previous actions and its overall compliance with The Principles continued to be of a high standard. We will continue to maintain close scrutiny of intelligence sharing with high-risk partners. We were concerned by the potential for caveats relating to assurances from one international partner to undermine those assurances with respect to due process and detention conditions that could amount to CIDT. We placed an action on SIS to clarify the situation with regard to these assurances at renewal of the relevant Ministerial submission. We will revisit this matter at inspection in 2023.

12.15 We noted the good use of scarce resources and effective triage by the UKIC Principles compliance team, including the introduction of a data visualisation tool and the use of low risk open source Principles country assessment documents. These documents can help case officers to reach well informed decisions as to the Principles risks associated with such countries. We endorsed efforts to share these country assessments across all six Principles Partners, where appropriate.

Government Communications Headquarters (GCHQ)

12.16 GCHQ had acted upon all the recommendations made following our last inspection and has continued to demonstrate a high standard of compliance with the requirements of The Principles. We found that overall GCHQ was applying careful consideration to cases where intelligence was being shared and The Principles were engaged.

12.17 We saw evidence of staff seeking clarification and, where necessary, additional information from requesting parties before agreeing to requests for sharing. We were also pleased to see that GCHQ was now providing cross references to relevant Ministerial submissions in its Principles considerations.

12.18 In one urgent threat to life case, GCHQ had not properly documented its consideration of The Principles at the time of the decision to share intelligence. GCHQ brought this to our attention following its own "after the event" review of the decision. There were clearly mitigating factors in the circumstances and we agree with GCHQ that there was no risk that mistreatment would have occurred as a result of the intelligence sharing and therefore this did not constitute an error.

12.19 GCHQ has developed a data visualisation tool to help staff understand The Principles risks associated with different countries. We were given a demonstration of this valuable tool and we hope that this can be made available to all Principles Partners in the coming year. Overall, this will contribute to even stronger compliance.

12.20 Last year, we were told that GCHQ was working on a policy which would govern the process where a UK government department that was not subject to The Principles was seeking permission to release intelligence owned by a Principles Partner. However, we were told that there had been no instances in the last 12 months where Principles Partners had to rely on Principles risks assessments made by non-Principles Partners. We agreed that, in these circumstances, a memorandum of understanding was not currently required.

The Ministry of Defence (MoD)

12.21 Overall, our 2022 inspection concluded that the MoD continues to secure a good level of compliance with the requirements of The Principles. As we reported in our 2021 report, the Government has agreed a policy which applies where there is no causal link between the actions of UK personnel and any risk of mistreatment. The MoD's internal policy had not been updated to take account of this policy as of the date of our inspection. We recommended the MoD circulates a note to all relevant personnel making clear the actions they must take to comply with that policy pending a full update to the internal guidance itself. Immediately following the inspection, the MoD did so and a full update to the internal guidance was in train as at the time of writing. Additionally, we identified a small number of other actions, some of which had been identified and proposed by the MoD itself, which focused on small changes which could usefully be made to the MoD's internal record-keeping.

Metropolitan Police Counter Terrorism Command (SO15)

12.22 SO15 continued to develop and improve in the last 12 months in relation to its application of The Principles. The central team overseeing compliance continues to improve knowledge and communications among its colleagues based overseas, as well as in the wider UK Counter Terrorism Police Units. SO15 has set up robust processes to manage and inform staff who are involved in decision making around The Principles. We were impressed by the internal guidance which, with a few recommended minor amendments, should lead applicants and senior personnel through all the necessary considerations when sharing information relating to detainees held overseas.

12.23 We recommended that SO15 makes some minor changes to records of decision making in Principles-related matters. Generally, SO15 takes a cautious approach when considering cases that might engage The Principles.

The National Crime Agency (NCA)

12.24 We conducted one inspection of the NCA in 2022. We are satisfied the NCA was compliant with The Principles and were making appropriate risk assessments in the majority of cases.

12.25 The NCA has put considerable effort into providing additional training for staff who are engaged in The Principles. It has developed e-learning packages and was close to completing a central knowledge repository which will be accessible to all NCA officers and provide a one-stop shop for guidance.

12.26 Last year, we recommended that the NCA move away from assessing all operations on a case-by-case basis, towards a model where "thematic" or "framework" assessments are developed. These would set out the risks associated with a particular set of activities in a particular country. This ensures that the risks are assessed comprehensively, having regard to all of the relevant evidence, reducing the risk of individual officers overseas making errors when producing their own ad hoc risk assessments at short notice.

12.27 However, we were concerned that the NCA had submitted a "thematic" application when it had assessed a particular country to have had a real risk of torture in relation to certain detainees that could not be mitigated. The Principles state that, where there is a real risk of torture, there is a presumption that Principles Partners will not proceed with the intended activity. Such facts need carefully to be considered by a Minister before a decision is made. The NCA highlighted to the Minister the presumption not to proceed, but stated

its view was that it could rely on an overarching Ministerial authorisation to rebut that presumption. However, our opinion was that sharing in such circumstances needs to be considered on a case-by-case basis by a Minister, who is given advice on why, exceptionally, it is appropriate and lawful to proceed in any given instance. The Minister had approved this application for 12 months of sharing but we recommended that sharing under this thematic authorisation was stopped. The NCA agreed there will not now be any sharing under this authorisation where there is an unmitigated real risk of torture and any such cases will now be put before the Minister for individual consideration.

12.28 We also recommended to the NCA that, in circumstances where it relies on assurances by an in-country partner agency to mitigate real risks, it needs to be satisfied that those assurances can provide the mitigation to reduce the risk. The NCA has complied with all the recommendations we made and all have been discharged.

13. Law Enforcement Agencies and Police

Overview

13.1 Law enforcement agencies (LEAs) are usually inspected on an annual basis with inspections completed in relation to all of the powers they use. In 2022, we conducted 115 inspections of LEAs with a mix of in-person and remote engagements.

Findings

13.2 2022 saw the first full year of authorisations under the Covert Human Intelligence Sources (Criminal Conduct) Act 2021. While there were some initial teething issues, the new provisions are now well embedded, helped by feedback from inspections, commentary by Judicial Commissioners and training by national police working groups. Applicants and Authorising Officers (AOs) are now showing an improved explanation of proportionality in this context and explaining better the criminality permitted.

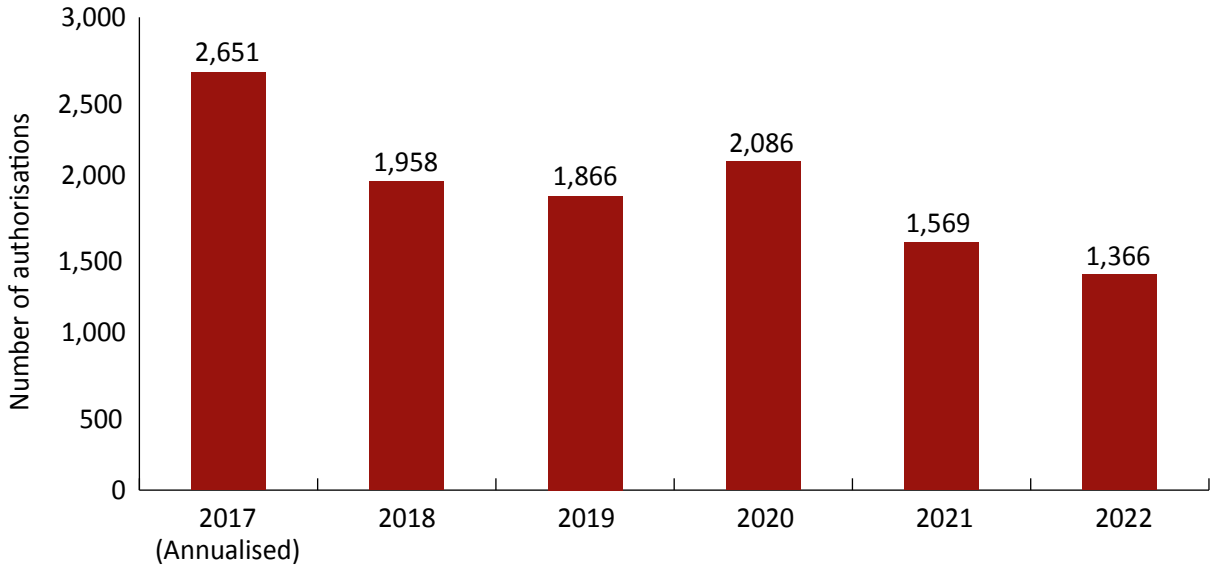
13.3 For 2022, we have taken a different approach to our inspections of the use of targeted equipment interference (TEI) by police forces and LEAs. We produced individual reports at the end of each inspection but have drawn the findings together into a thematic report which was issued in 2023. Some of the initial findings are set out from paragraphs 13.26 and we will update further in our 2023 report. This approach is of particular value as it helps us determine the structure of forthcoming inspections and our findings can help inform the Home Office and LEAs of how to improve consistency in approach, inform future policy or legislative change and assist with training and capability development.

13.4 For a number of years, we have been flagging concerns about the performance and compliance issues in the system used by LEAs to manage intercept material. The project to develop a replacement system is underway by the Home Office and we urge that this should be given the highest priority. The shortcomings of this system came to the fore at the end of 2022 when it was identified that again some collected data could not be deleted. Further details on the bespoke investigations on this issue will be set out in our 2023 report.

Covert human intelligence sources (CHIS)

13.5 Our inspections have continued to identify a high degree of compliance with the statutory framework, with necessity and proportionality considerations for the use of this covert tactic generally well-articulated. At inspections, we are looking for CHIS authorisations and risk assessments which provide sufficient detail but are not formulaic or overly bureaucratic. As we set out in our 2021 report, there is still room for improvement in how collateral intrusion should be addressed when there is interference with the private or family life of persons who are not subject to criminal investigations. This matter was a focus for us during 2022 and will continue to be so during our 2023 inspections.

Figure 13.1: Covert human intelligence source authorisations for LEAs, 2017 to 2022



13.6 The welfare of those authorised as CHIS will always be a priority for our Inspectors. With Covid-19 restrictions fully removed, we are pleased to see the return of more in-person meetings between CHIS and CHIS handlers. Significant efforts have been made by most LEAs to identify CHIS welfare issues, whether this be ongoing drug and/or alcohol addictions or when, in some instances, specific welfare matters arise due to coercive behaviour by a partner or criminal associate. We have seen several examples of good risk management measures being put in place by the AO and CHIS management team, with advice and guidance for CHIS including signposting appropriate social or voluntary services. In addition, several LEAs have taken a proactive approach by bringing in qualified professionals to train or advise CHIS management teams in how to identify such welfare matters at an early stage.

13.7 We continue to share the good practice we have encountered during our inspections through the National Source Working Group (NSWG). Additionally, Inspectors have attended AO courses, delivered by the College of Policing and others.

Juvenile CHIS

13.8 As highlighted in last year's report, the Investigatory Powers Commissioner (IPC) wrote to all relevant authorities in August 2021 asking to be informed within seven days of the authorisation of a juvenile or vulnerable adult CHIS. This requirement has now been incorporated into the 2022 CHIS Code of Practice. We will visit and review the case as soon as possible following such a notification, underlining our commitment to ensuring that oversight of any juvenile or vulnerable CHIS is sufficiently dynamic to enable early identification of any concerns. We thoroughly review the relevant authorisation paperwork, including risk assessments, and will meet with those responsible for the authorisation and ongoing management of the individual. Any matters of concern are fed back to the officers concerned.

13.9 In 2022, four new CHIS authorisations were granted which related to a juvenile. It was disappointing that despite the requirement for juvenile CHIS authorisations to be notified to the IPC within seven days, two of the four authorised during 2022 were not reported to us within that timescale and could not therefore be inspected until 2023. We will report further on these cases in the 2023 Annual Report.

13.10 The low number of cases shows that this tactic is only considered in exceptional circumstances and when other potential sources of information have been exhausted. While it would be inappropriate to give specific details, we can report that juveniles were assisting with investigations tackling the supply of class A drugs and firearms. We were reassured that the duty of care was being taken extremely seriously and that the need to safeguard and promote the best interests of the juveniles was a primary consideration in the decision to authorise. In neither of the cases we examined was the juvenile authorised to participate in crime; in fact, the decision to authorise was viewed as a means of helping to break the cycle of crime and danger for each individual.

13.11 As part of our reviews, we provided advice on clarifying the parameters of the authorisation so that the juvenile fully understands their role as a source. We also provided guidance as to the appropriate handling of confidential personal information.

13.12 One of these juvenile CHIS authorisations has been used by one of the supervising officers as a sanitised case study shared with the wider law enforcement community through a NSWG Continuous Professional Development (CPD) event. We also provide regular support to practitioners as LEAs consider using such tactics themselves.

13.13 While there have been no vulnerable CHIS authorisations in 2022, we identified a very small number of cases when a CHIS had either been mischaracterised as vulnerable despite not meeting the criteria outlined in the Code of Practice or, alternatively, one case where their vulnerability went unrecognised and the source was not subject to the enhanced authorisation level. The latter case was reported as a relevant error to the IPC, who was satisfied that appropriate measures were taken to reduce the likelihood of recurrence.

CHIS Criminal Conduct Authorisations (CCAs)

13.14 Following the commencement of the Covert Human Intelligence Source (Criminal Conduct) Act 2021 for LEAs in September 2021, we carried out quarterly reviews of Criminal Conduct Authorisations (CCAs) during the first year of operation. The feedback for AOs and Judicial Commissioners from these reviews generally focused on the need for clearer descriptions of the actual conduct authorised and a better articulation of the proportionality for that conduct. Although we do not see the continuing need for these specific reviews, we continue to look at those CHIS cases where a CCA has been granted in the annual inspections of all those public authorities empowered to use the provisions.

13.15 We also continue our regular discussions with the NSWG and National Undercover Working Group (NUWG) in relation to any areas of concern or learning arising from our oversight and inspections. In particular, the NUWG has held a series of regional presentations to raise awareness and improve consistency in the management of CCAs. Inspectors have attended these events.

13.16 Given the Parliamentary and public interest in this regime, it is important that our oversight has been extensive and constructive, ensuring that the new powers have been implemented in a compliant and informed manner.

Relevant sources

13.17 In 2022, we conducted over 90 bespoke reviews of operatives in addition to the examination of operations using relevant sources as part of our annual inspections of LEAs. Table 13.1 sets out the authorisations and applications for relevant sources since 2020.

Table 13.1: Relevant source authorisations and applications, 2020 to 2022[1]

	Total Applications (incl. renewals)[2]	Total Authorisations (incl. renewals)	Urgent	Renewals (long term authorisations)	Judicial Commissioner refusals[3]
2020	301	293	2	75	0
2021	495	434	4	74	0
2022	526	433	1	103	0

Notes:

[1] *Prior to 2020, IPCO reported data on "notifications" and cancellations of relevant sources. IPCO no longer collects or reports this data from public authorities.*

[2] *Applications include notifications to IPCO of authorisations and applications to renew authorisations after 12 months.*

[3] *Refusals relate to applications to renew only.*

13.18 In general, the oversight, governance and management regimes have continued to ensure good levels of compliance with the legislation and Code of Practice. Working closely with us, the NUWG will regularly circulate good practice matters we have noted during inspections, as well as assisting with implementing improvements. This year, this has included the IPC's concern at the increasing tendency for thematic type authorisations to be formed. These could address many different types of criminality across a wide geographical area, mostly relating to the investigation of county lines criminal activity. The IPC considered the parameters of some of these types of authorisations to have been set too broadly, with the significant potential for "mission creep" to occur or for operational deployments to stray far from the initially authorised covert activity.

13.19 The IPC wrote to the Chair of the NUWG expressing his concerns and was pleased to see the matter immediately addressed. We will continue to review this on future inspections.

Surveillance and property interference

13.20 We continue to see a good overall standard of covert surveillance and property interference authorisations, with the necessity and proportionality requirements, generally speaking, clearly understood.

Figure 13.2: Intrusive surveillance authorisations and directed surveillance authorisations for LEAs, 2017 to 2022

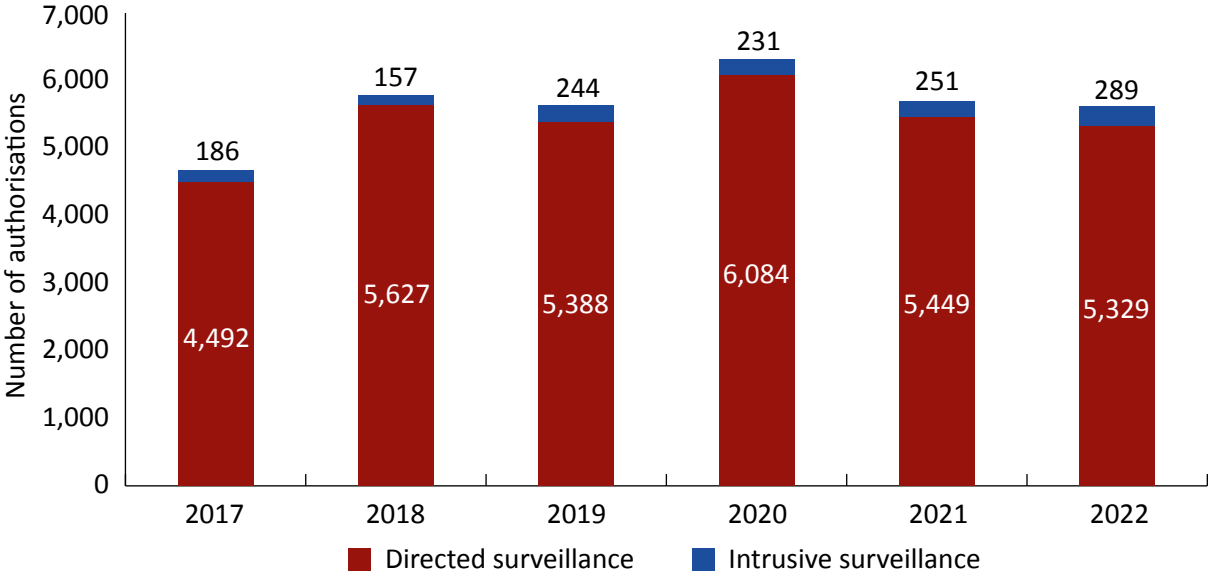
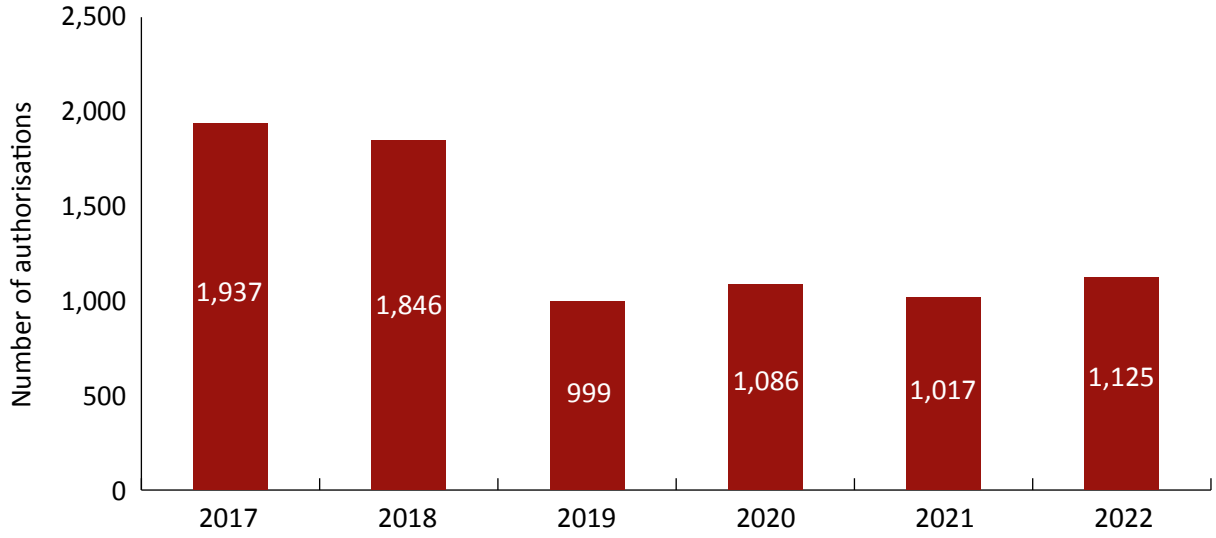


Figure 13.3: Property interference authorisations for LEAs, 2017 to 2022



13.21 One of our few issues of concern related to directed surveillance where there had been insufficient justification for each tactic requested and authorised. By way of an example, an area of non-compliance was issued to a force for adopting a "standard regional wording", namely a list of tactics applied to almost all directed surveillance authorisations. All public authorities are strongly advised to adopt an incremental approach, adding or removing tactics at reviews and renewals based on the emerging intelligence picture and the expected value to the investigation from each tactic. Such an approach ensures that all the actions authorised are necessary and proportionate.

13.22 We continue to see overly lengthy applications and authorisations. There is a real risk that, if too much information is provided, AOs could overlook the most salient and important elements in their considerations. It is equally unnecessary for AO comments in support of the more intrusive tactics, which require the Chief Constable's authorisation, to repeat

information already provided by the applicant. We will continue to make observations when we identify opportunities for reducing unnecessary bureaucracy.

13.23 Turning to cancellations, we see regularly a failure by AOs to ensure arrangements are in place for the ongoing management of any covertly acquired material. We expect to see specific instructions on review and destruction dates with an assigned individual responsible for the ongoing management of the material and ensuring the Code of Practice requirements will be complied with. Reassuringly, we have found fewer instances of late cancellations when the criteria for continued surveillance or property interference are no longer met. If it is impracticable to secure a prompt written cancellation from the AO, we have advised that the cancellation can be given verbally but must then be followed by confirmation in writing.

Legal professional privilege (LPP) material

13.24 As highlighted in last year's report, the likelihood of acquiring material subject to legal professional privilege (LPP) is a continuing focus for us, particularly in relation to intrusive surveillance. Following a meeting in January 2022 with the IPC, Chief Constable Mark Roberts, the National Police Chiefs' Council (NPCC) Lead for Covert Legislation and Guidance, wrote to all Chief Constables, Covert Authorities Bureau (CAB) Managers and Senior Responsible Officers about the handling of LPP material. This letter set out that LPP material was not exclusively limited to first-hand conversations between subjects and their professional legal advisors and that, in certain contexts where information has been provided or made available in confidence, such as when an individual discusses legal advice with immediate family or close friends, privilege may not be considered to have been waived generally.

13.25 Our increased focus on this topic has led to an overall improvement in the considerations of acquiring LPP material. Despite this, we continue to receive late notifications from LEAs that LPP has been retained other than for the purpose of its destruction. All cases should be reported to the IPC as soon as practicable and Judicial Commissioners will then consider whether to order destruction of the item or impose conditions on its use or retention.

Targeted equipment interference (TEI)

13.26 During 2022, we took a thematic approach to our TEI oversight. We examined records and interviewed key staff involved in the application and process of TEI warrants through a number of inspections which cut across LEAs. We also interviewed those involved in the management and deployment of TEI capabilities. Several Judicial Commissioners joined these inspections, as did members of the Technology Advisory Panel (TAP), particularly for those involving more complex casework such as at the National Crime Agency (NCA).

13.27 Although all UK police forces are empowered to use TEI independently, most equipment interference capability is being developed and managed through regional collaborations. Larger organisations such as the NCA and the Metropolitan Police Service (MPS) have an independent capability but also offer support to other organisations.

13.28 While our findings overall identified reasonable levels of legislative compliance, we observed significant inconsistencies in the way TEI warrants were processed and managed across LEAs. Inconsistency was evident in the application process, the description of the conduct being authorised and the review, retention and deletion of material obtained in consequence of the warrant.

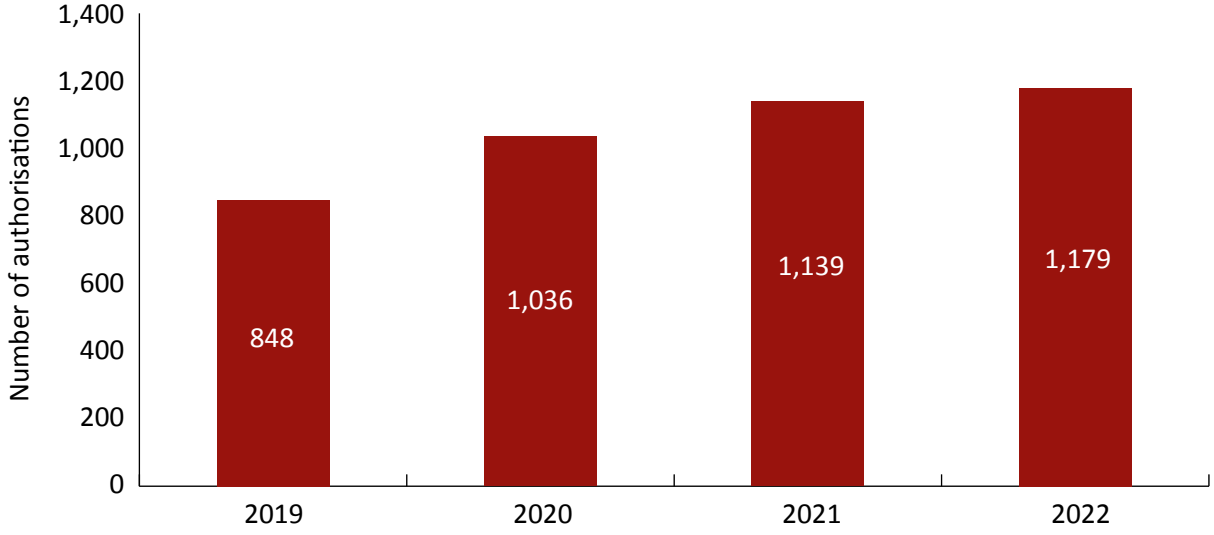
13.29 We observed that the mandatory training requirement set out in paragraph 1.7 of the Code of Practice was not being met and, as a result, we encountered frequently a lack of knowledge and understanding of the differences in procedure required for the Investigatory Powers Act 2016 (IPA) as compared to those used historically by LEAs under the Police Act 1997. This was most prevalent in the selection of the subject matter, as set out in sections 101 and 115 of the IPA.

13.30 A common observation was an excess of unnecessary material included in support of a TEI warrant rather than a focussed approach to the requirements of the legislation. This was undoubtedly a result of the lack of knowledge and understanding of the IPA, as referenced above, and suggests an erroneous assumption that if an application includes "everything" it must surely hit the essential elements.

13.31 We saw an increase in warrants being issued to access intelligence/evidence held as remotely stored electronic data, particularly during the post arrest, overt stage of an investigation where communications devices had been seized or usernames and passwords to online accounts recovered. We believe this has been triggered by the fact that reliance on Police and Criminal Evidence Act powers for this purpose is seen by many as increasingly vulnerable in the light of comments in the 2020 Law Commission on Search Warrants.[30]

13.32 A growing concern for us is the lack of a formal accreditation process for organisations and staff engaged in the deployment of TEI capabilities, particularly those involving computer network exploitation, and a lack of national agreement on the method of operation and verification of those capabilities. We have expressed our concerns to LEAs and the Home Office and will expect to see some steps taken to address these issues during 2023.

Figure 13.4: Targeted equipment interference authorisations for LEAs, 2019 to 2022



Targeted interception

13.33 Five LEAs are permitted to carry out interception of communications under the IPA for the purpose of preventing or detecting serious crime: the NCA, His Majesty's Revenue and Customs (HMRC), the MPS, Police Scotland and the Police Service of Northern Ireland (PSNI).

30 See: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/10/Search-warrants-report-grayscale-web-1.pdf

The National Crime Agency (NCA)

13.34 The NCA operates at a national level providing targeted interception (TI) to meet intelligence requirements for NPCC police forces in England and Wales and for NCA operations. The NCA has an internal compliance regime which arranges assurance visits to NCA offices and Police Regional Organised Crime units (ROCUs) to check that its interception material is being handled correctly in accordance with the IPA. Overall, the NCA demonstrated a good level of compliance with Part 2 of the IPA and the Code of Practice.

13.35 We raised concerns last year that there was insufficient explanation for the management and dissemination of intercept material within the NCA Handling Arrangements. These Handling Arrangements, which have to be approved by the Home Secretary, are a statutory requirement and referred to in warrant applications considered by the Secretary of State and Judicial Commissioners. As taskings for NCA warrants can originate from the NCA, NPCC regional forces in England and Wales or the MPS, we were looking for parity in how material was being handled across all operations. In fact, we were concerned at the different approaches and, particularly, that the NCA had not addressed our previous concerns regarding the MPS dissemination model. We understand that this has now been addressed and a new version of the Handling Arrangements has been sent to the Home Office for consideration. We will inspect against this in 2023 and report back on compliance next year.

HM Revenue and Customs (HMRC)

13.36 We inspected HMRC during February 2022, finding a continuing good track record of compliance with the requirements of the Act and Code of Practice for TI. The inspection was focused on modifications, renewals and cancellations following the approval of a warrant by a Judicial Commissioner and the arrangements in place to safeguard intercept product. The necessity and proportionality of any modification was well justified, although in a couple of instances the Inspectors questioned whether new subject matter details fell outside the approved scope of the warrant, albeit this targeted activity was criminal in nature and clearly within the remit of HMRC. Individual warrants, including thematic warrants, were well managed to ensure that the interception being undertaken remained proportionate, and (with exception of the subsequent issues identified in paragraphs 13.40-13.41) good arrangements were in place to ensure adherence with the interception safeguards. The Inspectors have mandated the temporary retention of intelligence logs to aid our future oversight.

Metropolitan Police Counter Terrorism Command (SO15)

13.37 The inspection of the MPS in October 2022 found continued good compliance with requirements of the Act and Code of Practice for TI. Where warrants had been modified, they were within the foreseeable scope of what had been authorised and approved. Like the NCA, the MPS supports ROCU operations and conduct assurance visits to ensure intercept material is being handled correctly. However, Inspectors raised concerns that the differing Handling Arrangements (such as the dissemination format) in place for TI material at ROCUs, whether it is provided by the NCA or the MPS, may be a source of confusion which could impact on the effective application of the safeguards without additional controls. Further assurance will be sought in 2023 that sufficient controls are in place to ensure compliance with those Handling Arrangements.

Police Scotland

13.38 Police Scotland has demonstrated a good level of compliance with Part 2 of the IPA and the Code of Practice. We were satisfied that Police Scotland's Handling Arrangements for intercept material were robust and there was a good awareness among staff of their responsibilities around the handling of confidential or privileged information.

Police Service of Northern Ireland (PSNI)

13.39 An inspection during June 2022 found that PSNI continues to demonstrate good compliance with the requirements of the Act and Code of Practice for TI. The inspection was focused on modifications, renewals and cancellations following the approval of a warrant by a Judicial Commissioner and the arrangements in place to safeguard intercept product. The necessity and proportionality of any modification was justified to a good standard. Intercept material is secured well, although PSNI will have to review the retention period of some types of material acquired and, in a small number of instances, particular records which are exceptionally sensitive.

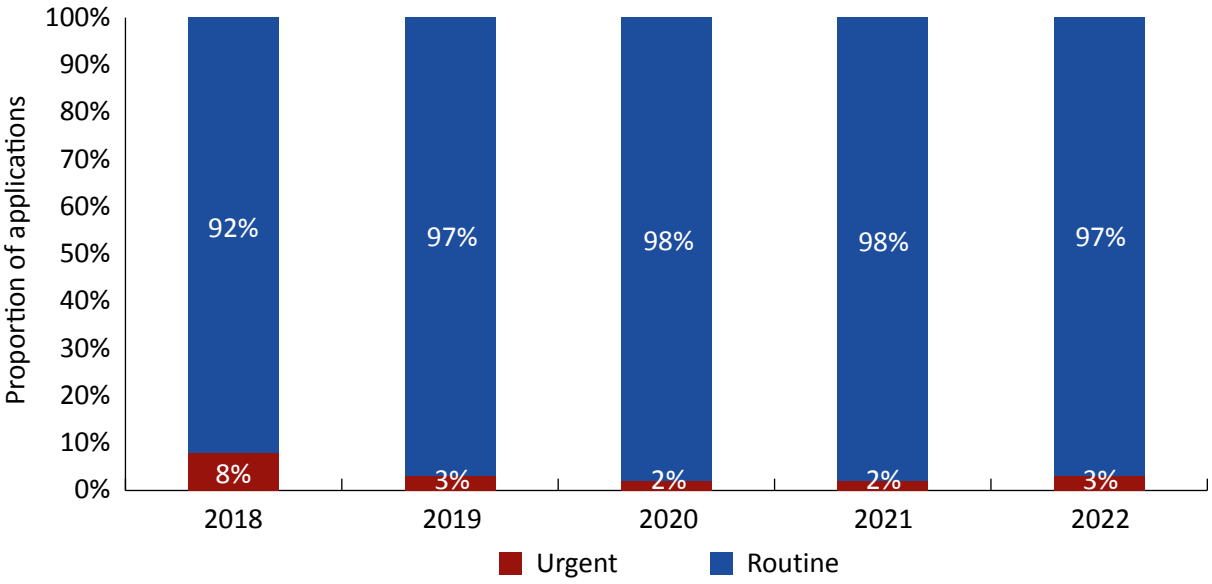
Management of intercept material

13.40 As we have indicated in previous years, the replacement of the IT system used by LEAs to manage and disseminate intercept product internally and to ROCUs is well overdue. New issues regularly are identified, with particular concerns emerging at the end of this year in relation to the inability to delete some data at the end of operations. This system is distinct from other agency and police systems which are used to listen to and analyse intercept product.

13.41 HMRC was the first agency to report this to us as an error in December 2022. At the same time, it informed other LEAs who use the same system. In January 2023, the MPS, PSNI, Police Scotland and, to some extent, the NCA all confirmed that they had the same issue. We will include this error for the other LEAs in our 2023 annual report statistics. At the time of writing, we are conducting bespoke investigations of the remaining LEAs to clarify the extent of the problem. The Home Office is also looking at short-term options to fix the issue.

13.42 Although we understand that this is a complicated system and the development of a new solution, while ensuring that ongoing investigations are not affected, is a substantial undertaking, there is no doubt that the project should be given the highest priority by the Home Office.

Figure 13.5: Proportion of urgent and routine applications by LEAs for targeted interception, 2018 to 2022



Communications data (CD)

13.43 Overall, our inspections during 2022 provided reassurance that the level of compliance with the IPA remains good. The role of the Single Point of Contact (SPoC) ensured that, in general, the quality of applications submitted to the Office for Communications Data Authorisations (OCDA) was high and that the subsequent acquisition of CD from a telecommunications operator (TO) was in accordance with the authorisation granted.

Figure 13.6: Communications data applications and authorisations for LEAs, 2020 to 2022

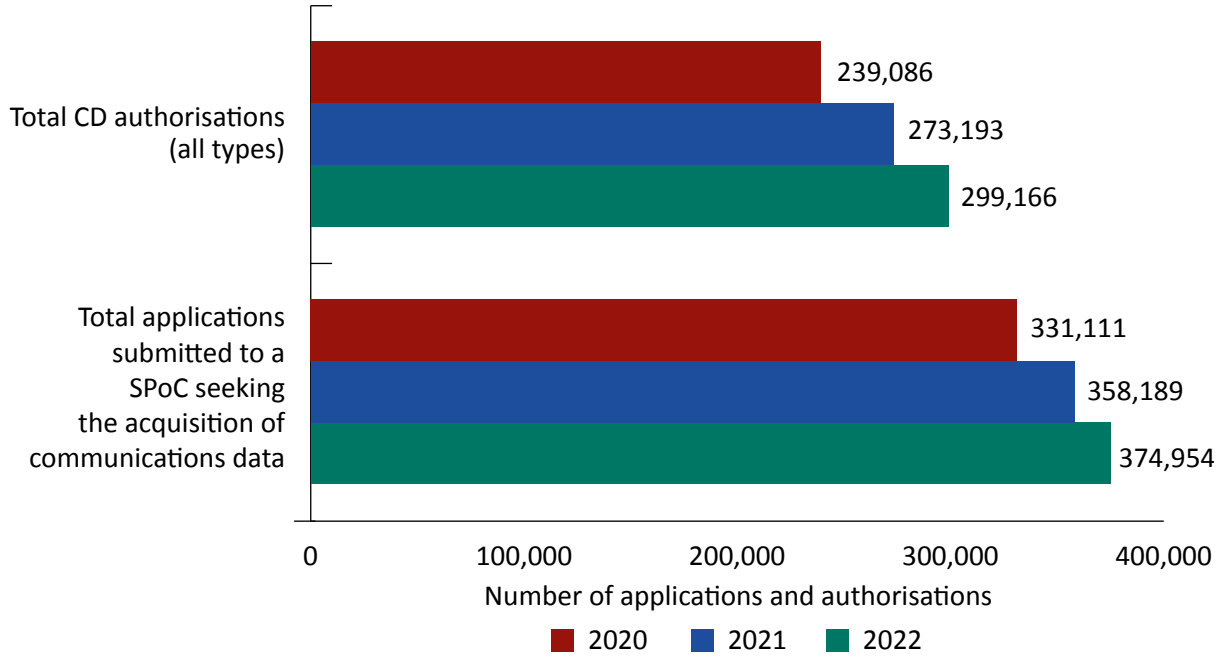
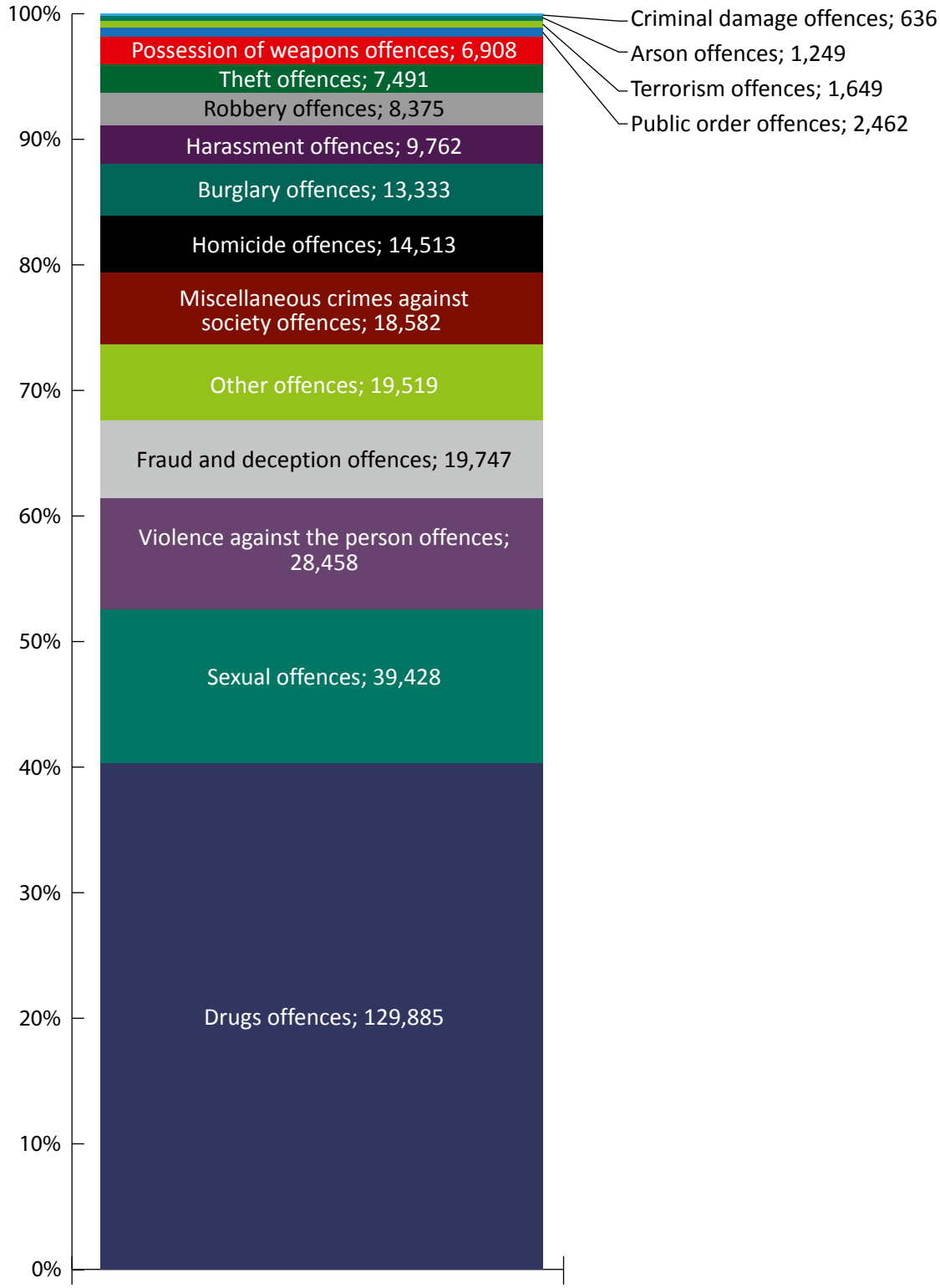


Figure 13.7: Communications data authorisations by offence, 2022



13.44 We have seen a significant improvement in the standard of applications submitted by police professional standards departments in the light of the minimum expectations for such applications set out by the IPC and imposed by OCDA. The additional obligation imposed for 2022, namely that such applications must have been reviewed by a legal advisor to the public authority before submission to OCDA, is also having a significant effect.

13.45 We continued to see a willingness from LEAs to report mistakes and vulnerabilities, together with a positive attitude towards the reduction and elimination of errors. In 2021, we reported a recurring area of concern in relation to cases of malicious communications, harassment or minor offences under the Public Order Act 1986. While there has been some improvement, this has not been consistent across all LEAs and the issue remains a focus of our attention. We understand that, with so many people living their lives across a myriad of social media platforms, the number of complaints and allegations being dealt with by police about what is said and posted on those platforms has increased. However, our message is clear: while material posted may be unpleasant, rude or offensive, or targeted towards high profile celebrities or politicians, the circumstances must be sufficient to reach the criminal threshold before an authorisation to acquire CD can be considered. This is a further area that we believe LEAs should, in many cases, be seeking advice from their legal advisors on before submitting an application to OCDA.

13.46 While our inspections will continue to report on the efficiency of individual SPoC units to the respective Senior Responsible Officers, our attention is increasingly focussed on the percentage of applications returned by OCDA to each LEA due to a deficiency or a need for clarity of information.[31] Where we identified that an LEA was significantly above the average return for rework rate, we probed deeper to identify the cause; this could often identify a training requirement for applicants or a need to update processes or workflow systems. Where we identified significantly lower rates of return, we sought to draw out areas of good practice that could be shared across other public authorities.

13.47 Throughout 2022, we have worked with the Home Office and OCDA to implement the agreed additional CD guidance highlighted in our 2021 report.[32] At times this has been challenging, particularly in respect of banking and financial services as they, for example, try to determine whether data held by a bank is held in connection with its provision as a telecommunications operator of online services or as a means of contacting or verifying their customer for general financial services. This work will continue during 2023.[33]

Communications data relating to journalists or seeking to confirm or identify a journalist's source

13.48 Journalistic freedom is protected under Article 10 (freedom of expression) of the European Convention on Human Rights (ECHR) and we would expect all relevant applications to consider the necessity and proportionality of any request in that context.

13.49 Some applications relating to journalists fall into the sensitive profession category where a journalist has been a victim of crime. During our inspections, we scrutinise all applications and authorisations relating to journalists for compliance with the requirements set out in paragraphs 8.12 to 8.44 of the Code of Practice. Under section 77 of the IPA, authorisations for CD seeking to identify a journalistic source require the prior approval of a Judicial Commissioner who must be satisfied that there is an overriding requirement in the public interest to approve an application to identify a source of journalistic information.

13.50 In 2022, LEAs made 30 such applications, all of which were investigated further as part of IPCO's *ex post facto* oversight. A summary is set out below.

---

31 See: from paragraph 7.12.

32 See: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice/additional-guidance-to-the-communications-data-codes-of-practice-definition-of-communications-data-accessible

33 See: from paragraph 2.9.

13.51 Almost half of the total 2022 applications relating to journalists were in support of a counter-corruption investigation into police officers suspected of providing journalists, for a financial gain, with timely information about serious investigations. The applications presented a sound intelligence case for suspecting the corruption offences and sought to establish contact and co-location between the officers and the journalist. Judicial Commissioner approval was obtained in each case as the objective of the applications was to confirm the role of identified police officers as journalistic sources, with the ancillary purpose of identifying any other suspects who may have conspired in the alleged criminality. The likelihood of identifying other journalistic sources not subject of the investigation was also a factor considered by the Judicial Commissioners for the submissions where data was sought on a device known to be used by the journalist.

13.52 One application which was granted involved three individuals suspected of leaking very sensitive government information related to national security. Through the acquisition of CD on the suspects' mobile phones, the application sought to identify contact between them before and after the leaks rather than to identify the source. Owing to the possibility that the data would identify contact between one or more of the suspects and a journalist therefore confirming their role as a source, Judicial Commissioner advice was sought as required by paragraph 8.41 of the Code of Practice. This requires all applications which involve leaking of information or documents to the media to be referred to a Judicial Commissioner due to the unusual degree of sensitivity involved.

13.53 Two applications related to separate investigations into hoax bomb calls. Incoming call data on the landline phones of the two newspapers concerned was sought covering a limited and specific timeframe to identify the callers. The calls were made in furtherance of a crime and therefore the unidentified suspects were not acting as a source of journalistic information for the purposes of the IPA. One application was referred to a Judicial Commissioner, which is appropriate when it is deemed likely that the data returned will result in the incidental and unintended identification or confirmation of a journalistic source (see paragraph 8.41 of the Code of Practice). The second application justified this as unlikely to occur and was appropriately authorised by OCDA without Judicial Commissioner referral.

13.54 Several applications required careful assessment by the public authorities and OCDA of whether section 77 of the IPA was engaged. Among these included two applications concerning a long-running investigation into fraud and corruption offences. It appeared feasible, although unlikely, that they may have led to the identification of a journalist's source. Following consultation with and review by OCDA, the applications were referred to a Judicial Commissioner who approved them.

13.55 Seven applications related to an investigation into online sexual exploitation of children. The initial submission, having identified the suspect was a journalist, outlined the potential to acquire CD that could identify journalistic sources. The application was referred by OCDA to a Judicial Commissioner who approved the acquisition. The next application was approved by a second Judicial Commissioner who questioned whether section 77 of the IPA was, in fact, relevant. The CD requested was solely linked to the crime under investigation with no intention to use the data to identify any journalistic sources, nor was it likely that the data would cause them to be identified or confirmed unintentionally. Based on these comments the remaining five applications were all approved by OCDA.

13.56 One case where two authorisations were granted concerned an investigation into money laundering and the breach of financial sanctions involving a freelance journalist. The applications did not relate to the subject's role as a journalist, nor were they for

the purposes of identifying a journalistic source. Judicial Commissioner approval was nonetheless obtained on both occasions owing to the likelihood of the CD resulting in the incidental and unintended identification or confirmation of a journalistic source. A cautious approach was adopted in consultation with OCDA where it was uncertain whether the activities of the subject constituted journalism. When assessing whether an individual is a journalist for the purposes of the Act, the CD Code of Practice (8.15) instructs that consideration is given to the frequency of an individual's relevant activities, the level of professional rigour applied to their work, how the information is disseminated and whether payment is received for their work.

Internet connection records

13.57 An Internet Connection Record (ICR) is a record of an event held by a TO about a service to which a customer connected on the internet. ICRs do not provide content and are classed as CD. To acquire an ICR, a TO must firstly collect and retain them. This is done via a retention notice served on the TO by the Secretary of State with Judicial Commissioner approval.

13.58 To date, the collection of ICRs for investigative purposes has been to support small scale trials. The technology to collect, retain and filter results has been the mainstay of a second trial that took place in 2022. Where applications have been made in support of the trials, we have examined all approved requests during our annual inspection programme. It remains too early to report on the results of these trials.

14. Wider Public Authorities

Overview

14.1 As set out in Annex A, a number of other organisations, referred to as wider public authorities (WPAs), have the statutory power to use certain covert tactics. The nature and extent of the powers used across the WPAs varies depending on their specific functions. Several are empowered to authorise the use of directed surveillance and the acquisition of communications data (CD), whereas property interference and intrusive surveillance powers, which require a higher level of authorisation, are limited to a smaller number of organisations.

14.2 The regularity of our inspections of these organisations depends on the range of powers available to the authority, their level of usage and previous performance. When inspecting wider public authorities, we will consider how they comply with legislation, their own internal policies and the adequacy of their staff training.

Findings

14.3 During 2022, we conducted 23 inspections of WPAs. Of the 15 inspections relating to directed surveillance and covert human intelligence sources (CHIS), only seven organisations utilised the powers available to them.

14.4 Following the inaugural inspection of the UK National Authority for Counter-Eavesdropping (UK NACE) in late 2021 and the identification of a number of errors, including some relating to authorisations to identify a journalist's source, the Investigatory Powers Commissioner (IPC) concluded that the authority was not competent lawfully to exercise its powers lawfully. A number of measures were put in place while these serious issues were addressed, including a suspension of UK NACE's internal authorisation powers. Considerable efforts have been made to address these issues and, following an inspection in December 2022, the IPC was content that UK NACE now has the processes and understanding to operate compliantly.

Covert human intelligence sources (CHIS) and directed surveillance

14.5 The use of CHIS powers among WPAs remains relatively low. Errors reported by WPAs during 2022 predominantly related to witnesses or persons providing intelligence being subject to prolonged contact, or tasked in a manner which required an assessment and, where applicable, authorisation as a CHIS but such authorisation had not been put in place. Areas for improvement around CHIS structures included reviewing CHIS referral processes within the Department for Work and Pensions (DWP) to ensure that the risks to the source arising from their provision of information are suitably identified. It is important that even where WPAs seek not to use the covert power, such as the Environment Agency, or use any Regulation of Investigatory Powers Act 2000 (RIPA) powers, such as the Charity

Commission, there must still be appropriate organisational structures in place to be able to deal with such eventualities until such time as these powers are removed by legislative amendment, should Parliament consider this appropriate.

14.6 Figures 14.1 and 14.2 set out the use of CHIS and directed surveillance among WPAs.

Figure 14.1: Covert human intelligence source authorisations for WPAs, 2017 to 2022

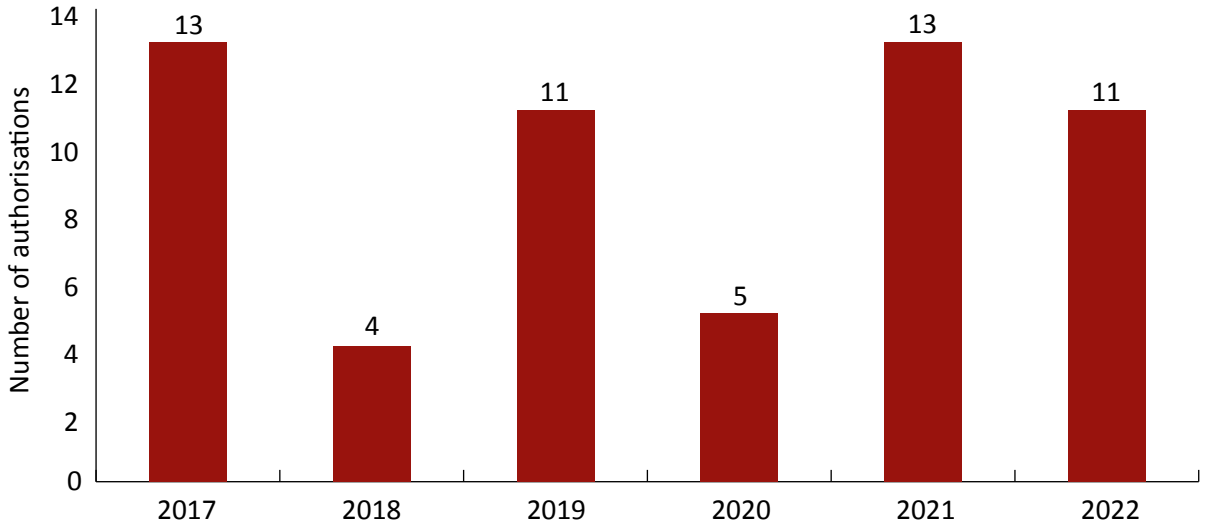
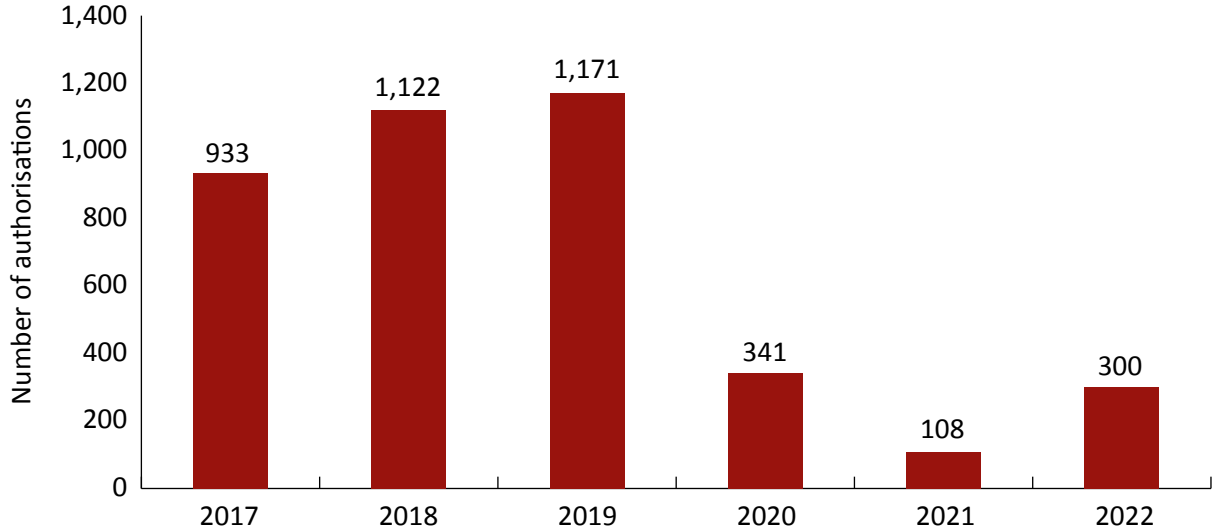


Figure 14.2: Directed surveillance authorisations for WPAs, 2017 to 2022



14.7 During our inspections, we identified some good practice and continued efforts by organisations to ensure compliance with legislation. Examples include:

- the Information Commissioner's Office (ICO) and the DWP had built robust processes to retain, review and dispose of material obtained using covert surveillance. It is commendable that they have achieved the requirements set out in the Code of Practice for Records and Product Management;
- the Environment Agency and Natural Resources Wales were able to demonstrate good quality and current training for Authorising Officers (AOs) and applicants on all relevant

aspects of RIPA legislation, despite being moderate to low users of directed surveillance activity only;

- Natural Resources Wales and Social Security Scotland have developed effective governance structures to ensure that, if needed, operations can be planned and delivered with appropriate checks and balances ensuring legitimate use of tactics;
- we noted consistently good and improving standards of directed surveillance authorisation compliance at the Financial Conduct Authority (FCA), relatively frequent users of covert surveillance powers with practiced applicants and AOs; and
- the Competition and Markets Authority demonstrated excellent oversight and processes for online and social media investigation, using a small cadre of trained analysts to assist investigations teams. This was supported by a controlled, auditable and well understood process.

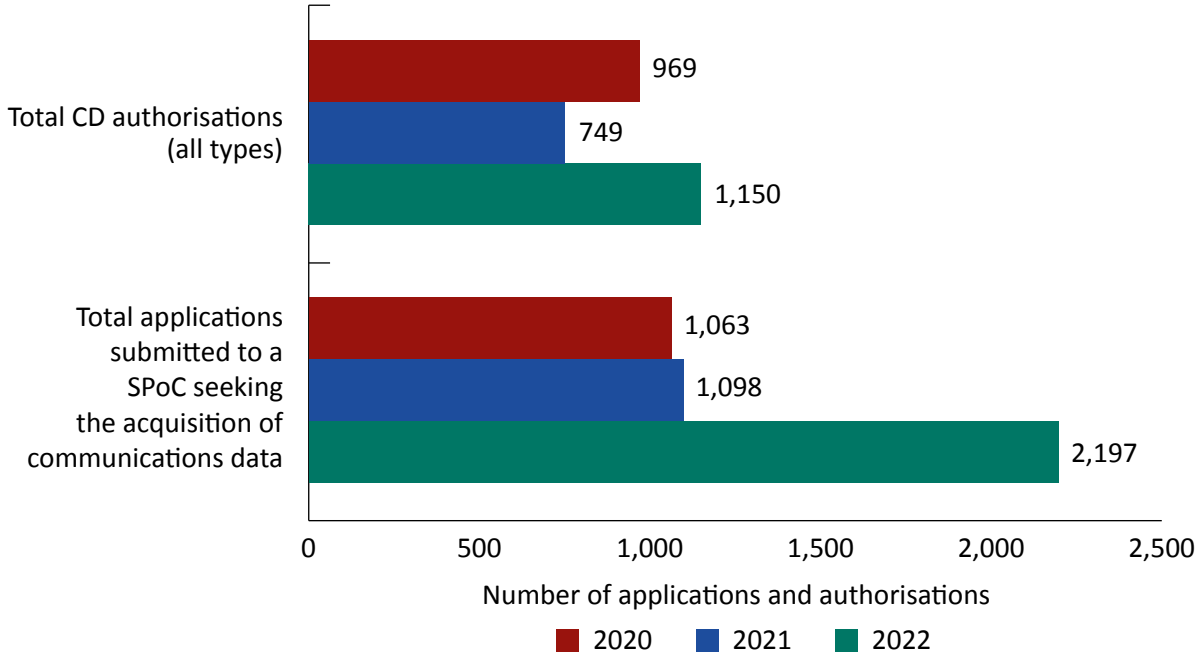
14.8 It is critical that WPAs maintain knowledge and skills in order that staff recognise where activity would require consideration for authorisation. This is especially relevant with the prevalence of online activity. Lapses in acceptable training provision post-Covid-19 were noted specifically for Transport Scotland and the ICO, while several WPAs also required guidance on statutory compliance requirements in relation to necessity, proportionality and collateral intrusion considerations.

14.9 In 2022, none of the WPAs who are authorised to use property interference or intrusive surveillance powers made any applications to use them.

Communications data

14.10 The volume of CD acquired by WPAs remains low. Despite the infrequent use, our inspections of WPAs during 2022 identified a generally good standard of compliance. That said, while it is not our role to encourage or dissuade use of powers to acquire CD, it does appear that some WPAs have failed to recognise the investigative opportunities available from CD and as such, we question whether those with minimal or no use should remain on the Schedule to the Investigatory Powers Act 2016 (IPA).

Figure 14.3: Communications data applications and authorisations for WPAs, 2020 to 2022



14.11 Some WPAs, while not compelled to do so, have chosen to partner with the National Anti-Fraud Network (NAFN) to provide Single Point of Contact (SPoC) services on CD applications. Where this is the case, the process works well with good standards of compliance and efficiency.

14.12 Where WPAs manage their own SPoC arrangements, compliance is still generally good, but we often identify minor failings in administration processes or record keeping. This is largely a result of those SPoCs only occasionally being called on to perform the function; as a result, they can find it hard to develop and retain experience and knowledge.

14.13 Many of the cases we examined involve quite complex investigations relating to unusual or unique criminal offences. We were satisfied overall that the documentation justified the principles of necessity, proportionality and collateral intrusion and provided sufficient explanation that the threshold for the relevant statutory purpose had been reached.

14.14 While a small number of WPAs can call on internal authorisation in cases of life at risk urgency (for example the Maritime and Coastguard Agency), we rarely see this option being exercised. All routine applications must be submitted to the Office for Communications Data Authorisations (ODCA) for independent consideration.

UK National Authority for Counter-Eavesdropping (UK NACE)

14.15 UK NACE plays a critical role in protecting the UK's most sensitive information and sites (including the intelligence agencies, Armed Forces and Critical National Infrastructure) from compromise by technical espionage. UK NACE is part of FCDO Services, a trading fund of the Foreign, Commonwealth and Development Office (FCDO), and the Foreign Secretary is accountable to Parliament for its conduct.

14.16 In October 2021, following UK NACE being vested with new powers to authorise the acquisition of CD in the interests of national security, we undertook our first inspection of

the organisation. While UK NACE had not used these powers extensively, the inspection and follow up enquiries (which continued into 2022) found there was a high incidence of errors and certain forms of CD were routinely being acquired without the appropriate authorisations in place. Of most concern, we identified five authorisations (resulting from one single tasking) to identify a journalistic source in respect of which UK NACE had failed to seek the requisite approval from a Judicial Commissioner under section 77 of the IPA.

14.17 The failure to seek Judicial Commissioner approval meant the authorisations had no legal effect and, therefore, could not be relied upon by UK NACE to render lawful the acquisition of CD from the relevant telecommunications operators (TOs). Although CD was obtained, it is important to note that none of the purported authorisations were successful in their objective to identify a journalistic source. Accordingly, although the non-compliance was serious in failing to seek the requisite approval from a Judicial Commissioner, no serious error had occurred within the meaning of the IPA and there was no affected person for us to notify.

14.18 While the IPC was satisfied that the issues that arose were due to a lack of awareness, training and support structures, rather than any bad faith, he was so concerned by the inspection findings that he concluded that UK NACE, at that point, was not competent lawfully to exercise its powers without close supervision. The IPC informed UK NACE and the FCDO that, in his view, an extraordinary measure was required, namely that UK NACE's internal authorisation powers should, in effect, be suspended until he could have confidence that UK NACE was capable of operating compliantly. Arrangements were put in place for the IPC personally to consider any application to acquire CD from UK NACE and progress was tracked by Inspectors against the range of actions we requested to improve the controls and governance in place.

14.19 UK NACE was re-inspected in December 2022. Considerable effort had been expended by both UK NACE and FCDO Services to address the failings identified in 2021. We have identified that further action was still needed to ensure that UK NACE had access to dedicated legal advice to enable it to operate compliantly and confidently in its specialist area of operations. We were, however, satisfied that UK NACE had made sufficient improvement to processes, controls and governance, as well as its understanding of the requirements of the IPA, to restore the IPC's confidence that it will operate compliantly. In January 2023, with the agreement of the IPC, UK NACE resumed its internal authorisation of the acquisition of CD. We will continue to monitor UK NACE's compliance through our annual inspections.

15. Local Authorities

Overview

15.1 Local authorities can make use of a limited range of investigatory powers: covert human intelligence sources (CHIS); directed surveillance; and the acquisition of communications data (CD).

Findings

15.2 In 2022, we conducted many of our inspections of local authorities through video or telephone meetings. In 2022, almost 100 Councils were inspected in relation to their use of covert powers in accordance with the current three-year cycle of oversight.

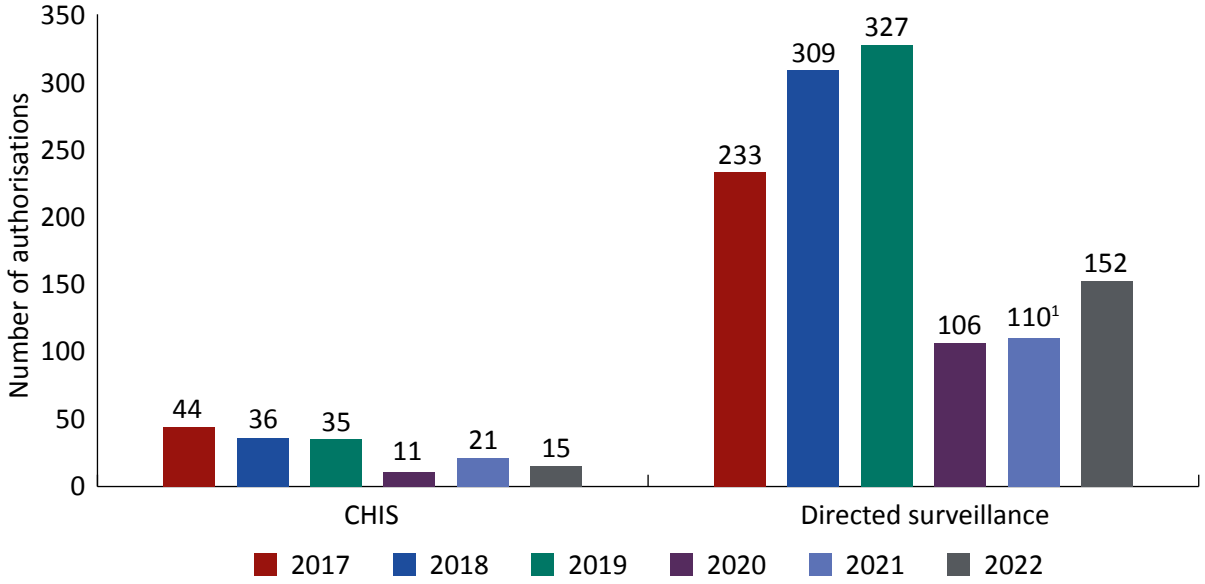
15.3 Overall, the use of directed surveillance and CHIS is lower compared to pre-pandemic levels, with local authorities finding other means either to prevent criminality or detect it through overt measures. The resources and funding needed to run covert investigations are often simply unavailable with the current demands on local authority services.

15.4 As detailed below, some Councils have continued to provide good levels of internal governance and awareness training, even if the powers have not been used. Others, however, appear to have put this area of business on the back burner, whether by design or through changes to key personnel. Such an approach is not sustainable while a public authority remains on the Regulation of Investigatory Powers Act 2000 (RIPA) schedule.

Covert human intelligence sources (CHIS) and directed surveillance

15.5 Figure 15.1 sets out the use of CHIS authorisations and directed surveillance authorisations for local authorities.

Figure 15.1: Covert human intelligence source and directed surveillance authorisations for local authorities, 2017 to 2022



Note:

[1] This figure was incorrectly reported as 159 in 2021.

15.6 In 2022, we identified some good practices by a number of Councils. Examples include:

- Fareham Borough Council had used its powers and demonstrated good levels of compliance, maintaining the finding from 2018 that its standards were "an example to all";
- Wolverhampton City Council had used the powers, and its policies and training provision reflected an engaged Senior Responsible Officer (SRO);
- Stockton on Tees Borough Council again showed its continuing high standards overall, with internal governance maintained through its SRO and a RIPA Steering Group;
- Dundee City Council had included training on the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) training for its Elected Members and used the powers on several occasions;
- Blackburn with Darwen Council ran regular training, including a forum by its SRO twice a year and had a clearly written policy. We reviewed one use of the "non-RIPA" process[34] that was well executed;
- Eastleigh Borough Council, while not having used the powers during the latest inspection period, nonetheless had thorough internal governance, guidance and oversight mechanisms in place. Its training provision was comprehensive and the Investigatory Powers Commissioner (IPC) noted the findings as exceptional;
- Leicester City Council had a conscientious SRO, good training inputs and staff conducting checks on the use of social media by staff as part of investigations;

34 This refers to situations whereby the key considerations in relation to privacy and human rights are documented by an Authorising Officer where an authorisation under the powers is not available (for example, if the matter under investigation does not relate to one of the statutory grounds available to that authority).

- Leicestershire County Council presented very well on inspection and was clearly on top of its records and product management; and
- Wiltshire Council showed good evidence of collaboration with another agency (the Food Standards Agency) when it ran a prolonged directed surveillance operation during an investigation of an individual selling meat without any hygienic practices.

15.7 Over the same period, however, we also recommended a number of actions towards raising compliance standards. Most often, this was to resume or repeat RIPA training for Council staff after a prolonged period (in some cases as a result of the Covid-19 pandemic), or to ensure their policy documents were updated following legislative changes. In some, the internal governance had lapsed, running the risk that no-one was scrutinising whether staff were thinking about the potential covert nature of their activities on social media, for example, or were ignorant of the need to authorise certain activities. In others, the requirement to update Elected Members annually on the Council's policy and use, or not, of the powers, had fallen by the wayside.

15.8 While the following is not an exhaustive list, some examples of our recommendations were:

- Powys County Council demonstrated a need for better training, as it presented very poor authorisations and had purported to use the urgent powers which were removed from local authorities in 2012. In addition, its recommendations in relation to policy and training had remained extant since its two previous inspections and internal governance was lacking;
- Stroud District Council had provided no training on RIPA since 2015;
- Conwy County Council had not addressed its recommendations from 2019, but a change in key personnel was hoped to bring about the necessary improvements; and
- Maldon District Council's compliance had been allowed to wither and a senior manager from another council was brought in towards the end of 2022 to address this. The IPC has asked for an update from Maldon by the end of April 2023.

15.9 In November 2021, we conducted our routine inspection of East Cambridgeshire District Council. Disappointingly, there still remained compliance issues dating from a 2014 inspection carried out by the Office for Surveillance Commissioners and our 2018 inspection. Despite an initial response from the Chief Executive in January 2022 and an update in August, these matters were still unresolved at the end of 2022. The Council's RIPA Policy document had not been updated since 2015 (thereby failing to account for the changes brought about by the Investigatory Powers Act 2016 (IPA) and was not due to be placed before the Council's Members for approval until the end of March 2023. The outdated 2015 RIPA Policy remained (at the start of 2023) the latest version on the Council's public website. The provision of RIPA awareness training, noted as a compliance failing in both 2014 and 2018, was unlikely to take place until several months into 2023. We will provide a further update in our 2023 report.

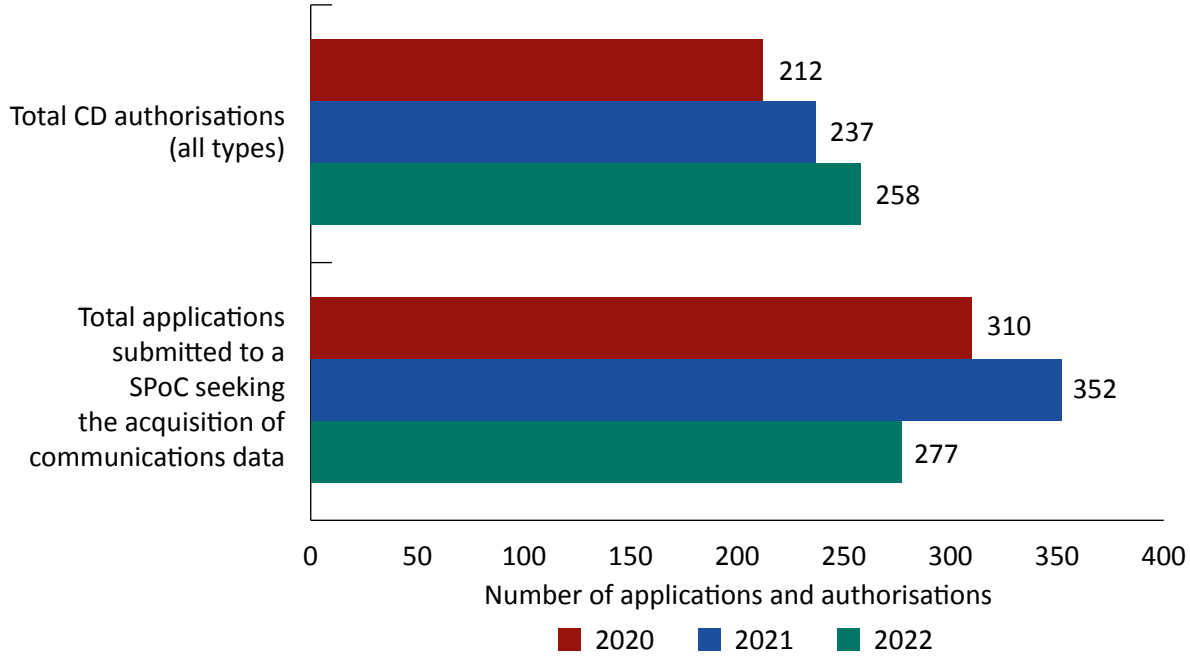
Communications data (CD)

15.10 Local authorities can only acquire CD by means of independent authorisation through the Office for Communications Data Authorisations (OCDA). In order to do so, they must use the centralised services of the National Anti-Fraud Network (NAFN) which acts as the Single Point of Contact (SPoC) to quality assure applications and, should an application be granted, will then acquire the CD from the telecommunications operator (TO) on behalf of the

requesting local authority. As a member of the NAFN, local authorities also have access to excellent CD and IPA training packages for their investigators and senior managers.

15.11 Most local authorities are now members of the NAFN but not all. Those that have decided not to join the collaboration cannot acquire CD. While it is not our role to encourage or dissuade use of powers to acquire CD, it does strike us as odd that some local authorities have failed to recognise the investigative opportunities available from CD. Overall, the use of CD by public authorities remains low. A handful may see applications into double figures, but it remains the case that many submit just one or two a year or in some cases, none at all. We monitor the pattern of acquisition by each authority and any sudden increase or decrease would trigger a review of that individual organisation.

Figure 15.2: Communications data applications and authorisations for local authorities, 2020 to 2022



15.12 Our 2022 inspection of the NAFN identified a continuing regime of good compliance. An area of concern arose around applications which sought to acquire extended periods of CD in relation to some types of fraud offences. A recommendation was made to reduce the interference with Article 8 of the European Convention on Human Rights (ECHR) by advising that the NAFN should apply an incremental approach to the acquisition of CD across all investigations. Where a larger dataset is necessary, it is our firm position that any requests must be commensurate and wholly justified.

16. Prisons

Overview

16.1 We inspect His Majesty's Prison and Probation Service (HMPPS), the Northern Ireland Prison Service (NIPS) and the Scottish Prison Service (SPS), along with a selection of prisons across England and Wales, Northern Ireland and Scotland.

16.2 We carry out inspections of prisons to ensure that communications monitoring is conducted adequately and that any use of surveillance techniques or covert human intelligence sources (CHIS) is compliant with legislation and the Codes of Practice. On our inspections of the use of the interception of communications, we also assess compliance against the relevant guidance in England and Wales, Northern Ireland and Scotland.

16.3 We conducted 78 prison inspections in 2022.

Findings

16.4 Our last report highlighted our concerns about the underlying arrangements for the interception of communications and we have been working with HMPPS to resolve those issues. We were particularly concerned that the Prison Service Instruction (PSI), which regulates such activity was overly complex and often contradictory. We are therefore pleased to note that the PSI was replaced in September 2022 by the Authorised Communications Controls and Interception Policy Framework (ACCIPF). The new guidance provides clearer guidance on the authorised interception and monitoring of prisoner communications. We are grateful for the engagement we have had with HMPPS and are pleased with how some of the issues we had identified have been addressed. It was apparent, though, from inspections carried out towards the end of 2022 that various issues and inconsistencies with legacy directives remain in the new framework and supporting material which HMPPS is working to address.

16.5 In our 2021 report, we set out the findings from our thematic investigation into the safeguards in place to protect intercept material on the PIN phone system. A number of the recommendations made in the report related to the operation of the PIN phone system where opportunities were identified to embed "compliance by design". We remain engaged with HMPPS on work to address our findings and have been informed that a new PIN phone system will be piloted in 2023. We will monitor this development and report further in due course.

16.6 This year, we have reflected on our prison inspection model and considered whether a more thematic approach would provide a more effective way to improve compliance. Since our inception, we have inspected each prison independently with a report issued to the prison governor. While some issues can be addressed locally, we assess that many areas of non-compliance can be attributed to a combination of underlying factors beyond the control of the individual establishment. As such, to coincide with the implementation of

the new policy framework, we will adopt a revised inspection model from 2023. Individual prison inspections will continue but will be conducted in smaller batches focussing on specific themes. Each prison will receive a compliance assessment, with the collective findings reported to the HMPPS Senior Responsible Officer (SRO) for prison interception in a detailed report; these will then be responsible for addressing areas of non-compliance across the prison estate and reporting their progress of the actions to us. We will update on our thematic inspection findings and the operation of this new model in our 2023 report.

Covert human intelligence sources (CHIS) and surveillance

16.7 HMPPS continues to make progress in its management of CHIS and surveillance activity and compliance with the legislation and the Codes of Practice. Our engagement with HMPPS leads is overseen by a Judicial Commissioner who leads on prisons for the IPC. Since our last report, HMPPS has developed its IT management system, which is now utilised fully across the estate. Early teething problems with the system have been addressed and, while some minor issues still exist, the system is seen by Inspectors as straightforward, fit for purpose and easy to use.

16.8 Increased resourcing in the Covert Authorities Bureau (CAB) and an increased focus on quality assurance, has clearly contributed to improved compliance standards.

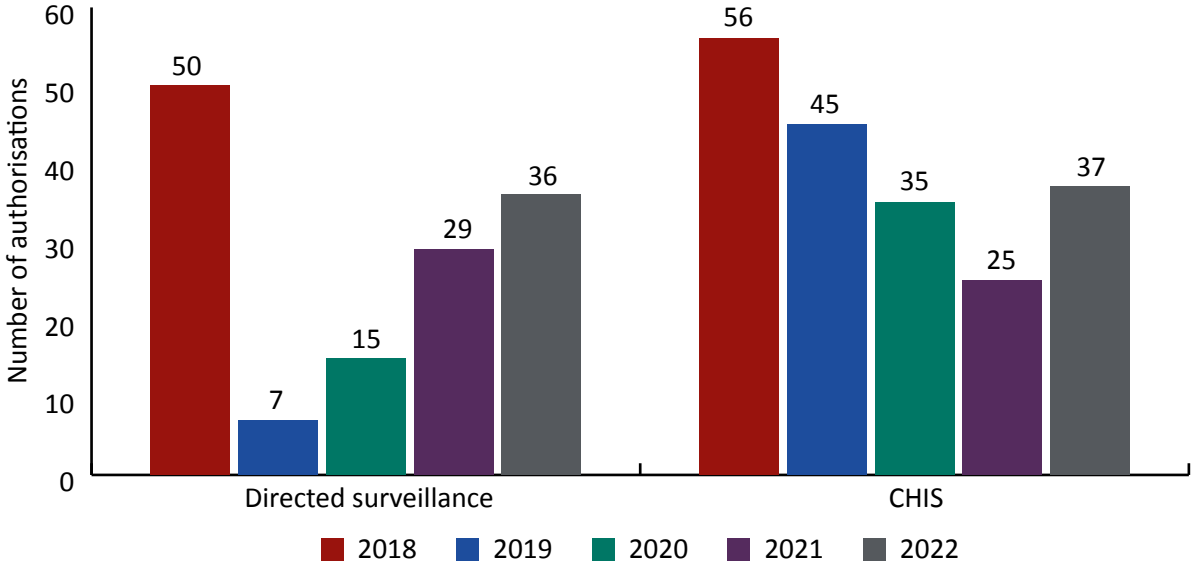
16.9 Our 2022 work incorporated individual inspections of each Regional Intelligence Unit (RIU) and a further visit to a Long-Term High Security Estate (LTHSE) prison. This provided a chance for us to assess the progress of the regional operating model and the status of the LTHSE. The RIUs were seen as progressing well with applicants, handlers, controllers and Authorising Officers (AOs) growing in confidence and achieving in general a high level of compliance. HMPPS is developing a strong cadre of regional and national AOs with an ongoing focus on their continued professional development.

16.10 Concerns remain with regard to the status of the LTHSE and, while standards have been raised, LTHSE prisons remain outside of the regional operating model. This creates an unnecessary vulnerability and potential compliance challenges. Our concerns were shared directly with the Executive Director for Security and the SRO responsible for Regulation of Investigatory Powers Act 2000 (RIPA) matters, who acknowledged the issue and committed to seek the appropriate resolution while managing the obvious risk.

16.11 HMPPS is now well placed nationally with a seat on many of the covert powers national working groups. It is at the forefront of a number of joint initiatives, working with partner agencies in a number of key areas of risk. The Prison Source Working Group has also been reviewed; the new group has a much clearer agenda with HMPPS in a joint chairing role. This partnership role continues to provide a clearer understanding of the management of CHIS across the prison estate by partner agencies.

16.12 HMPPS has also made significant progress with regard to the management of surveillance records and product. An interim inspection demonstrated a good level of understanding of requirements and some progress towards compliance with the data safeguard measures outlined in the Code of Practice. Further progress was noted during the annual inspection, with HMPPS very close to full compliance in this area.

Figure 16.1: Covert human intelligence source and directed surveillance activity at His Majesty's Prison and Probation Service, the Scottish Prison Service and the Northern Ireland Prison Service, 2018 to 2022



Interception

England and Wales

16.13 Section 49 of the Investigatory Powers Act 2016 (IPA) provides for the lawful interception of communications in prisons if carried out in the exercise of any power conferred by or under the Prison Rules. The arrangements for the interception of communications in prisons exist to prevent inappropriate use of telephones and letters, for example, to harass victims or witnesses or facilitate criminal conduct.

16.14 Our findings from inspections carried out in 2022, in common with those described in previous reports, show ongoing inconsistencies in compliance levels and the need repeatedly to highlight the same areas of vulnerability or failure. Common findings have included: a failure of AOs to provide sufficient reasoning of necessity and proportionality; a lack of justification when an authorisation is reviewed or extended; the absence of regular reviews; incomplete authorised monitoring, therefore undermining any grounds of necessity and proportionality given at the outset; and an inconsistent approach to record keeping. Likewise, we continue to identify training issues and emphasise the importance of embedding awareness and understanding of the relevant policies when individuals are appointed to roles involved in the monitoring of intercepted prisoner communications. We hope to see improvements in these areas as the ACCIPF is embedded and through the implementation of our new inspection model.

16.15 Prisoners' communications with their lawyers, Members of Parliament (MPs) and several other organisations are privileged, or confidential, and should not be read or listened to other than in the most exceptional circumstances. We have reported previously that there is a lack of safeguards for the handling of the inadvertent interception of such material and we continue to work with HMPPS, the Ministry of Justice and the Home Office to explore how this vulnerability can be addressed.

16.16 For a number of years, we have considered it unsatisfactory to rely upon the prisoner to inform the recipient of a telephone call that their discussion is being recorded and may be monitored. Taking these concerns on board, HMPPS ran a pilot during 2021 across a number of prisons using an overt announcement at the start of a call. We are pleased to report that the introduction of the audible warning to call recipients was implemented across the entire prison estate in June 2022. This brings England and Wales into line with the approach in Scotland, Northern Ireland and in many other foreign jurisdictions.

Scotland and Northern Ireland

16.17 Inspections of all three prisons in Northern Ireland and six prisons in Scotland were carried out in 2022.

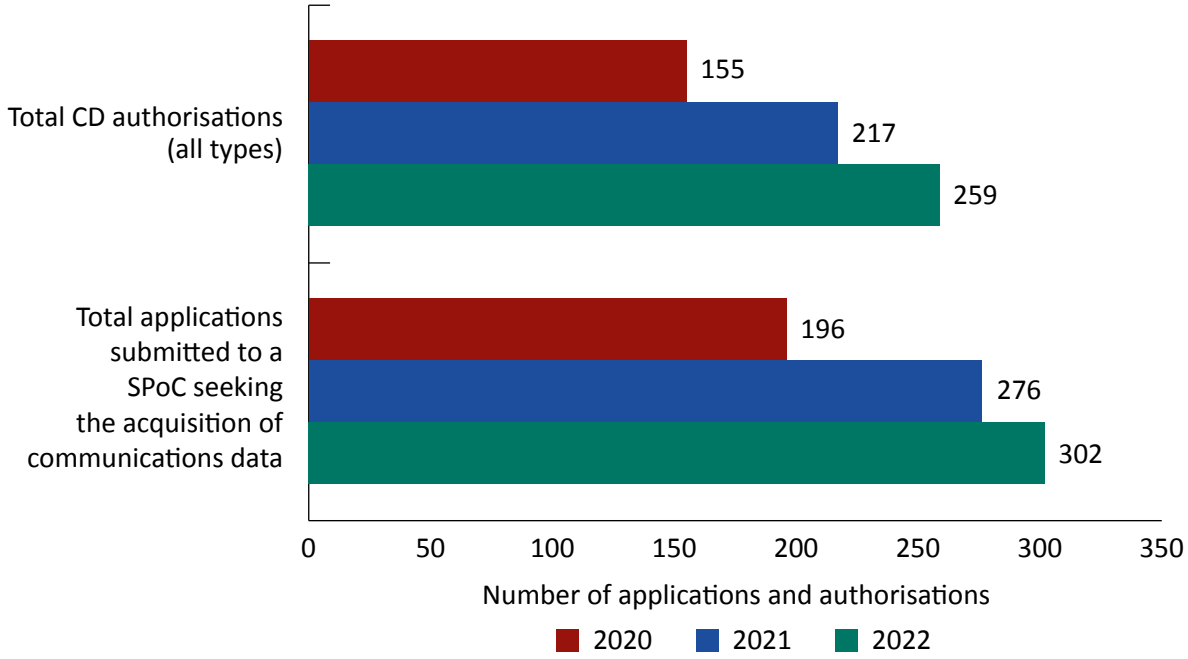
16.18 In Northern Ireland, our inspections found high levels of compliance with the rules governing interception in prisons made under the Prison Act (Northern Ireland) 1953. All three prisons were fully discharging their legal obligations to inform prisoners that their communications were subject to interception and staff demonstrated a thorough understanding of the requirements of the legislation. Initial discussions on the retention of records relating to interception activities were held with Northern Ireland Prison HQ. This will be an area of focus in 2023.

16.19 Our inspections of Scottish prisons assessed compliance with the rules and directions governing interception in prisons made under the Prisons (Scotland) Act 1989. Of the compliance issues identified, many were associated with gaps in policy and procedures which impacted all the prisons inspected. There were, for example, no arrangements in place requiring prison staff to justify the necessity and proportionality for monitoring intercepted communications. A representative from the SPS attended several of the inspections with a view to drawing upon our findings to inform the creation of a national policy. Further inspections will be scheduled in 2023 to assess progress.

Communications data (CD)

16.20 The acquisition and disclosure of CD is undertaken by the HMPPS Digital Media Investigation Unit and, unless a case meets the urgency criteria, all applications for CD are considered independently by the Office for Communications Data Authorisations (OCDA). While our 2022 inspection acknowledged good overall standards, two areas of non-compliance were identified. These both related to the procedures in place to store and handle CD acquired under the IPA. As a result of these findings we conducted a follow up inspection six months later and were satisfied with the progress made to remedy the deficiencies.

Figure 16.2: Communications data applications and authorisations in prisons, 2020 to 2022



Records and Product Management

16.21 The safeguarding of records and material derived from prison interception is governed by the ACCIPF and PSI, rather than the IPA Codes of Practice. Our inspections nonetheless adopt the same process of audit that we apply to material obtained through the use of other covert powers. This is to ensure that such material is held securely and then reviewed and deleted in line with those requirements.

16.22 The findings from our 2022 inspections remain mixed. In some prisons, staff are aware fully of the requirements to ensure that the content of intercepted communications (mail, email, telephone or video calls) is deleted after 90 days and that, in general, authorisation records should be retained for six years. In other prisons we have found a lack of consistency and understanding. The lack of accountability for managing the retention, review and disposal of records persists across many establishments. On occasions, we have identified material that has been held beyond the 90-day limit and have required its immediate destruction.

16.23 The ACCIPF includes some additional direction on safeguarding requirements, although it was too early to judge from our inspections what, if any, impact this will have on compliance levels. Safeguarding procedures will be the subject of a dedicated round of inspections in 2023 and the findings reported to HMPPS.

17. Warrant Granting Departments

Overview

17.1 Warrant granting departments are responsible for reviewing all applications submitted by the intelligence agencies or law enforcement agencies (LEAs) which require their approval. For new warrant applications and renewals, this will involve submitting such applications to Ministers for their personal approval once they are satisfied all the paperwork is in order.[35] We conduct annual inspections at each department, reviewing casework across the powers they authorise.

Findings

Home Office

17.2 In 2022, the Home Office exercised both its scrutiny of applications and its advisory role to a high standard. We were pleased to see continued engagement by Home Office teams and a more proactive questioning of agencies to understand the implications that new technical innovations may have on privacy and collateral intrusion. The level of advice being given to the Secretary of State was to a high standard.

17.3 The Home Office has worked hard to rectify and improve out-of-hours processes as a result of the error from last year. We were satisfied those processes have been revised to mitigate the risk of the error recurring. The Home Office continues to deal with large volumes of warrants and the introduction of a new management of information system in the coming year will help to maintain a good level of compliance.

Foreign, Commonwealth and Development Office (FCDO)

17.4 As in previous years, we saw clear evidence that the FCDO was providing valuable advice to the Foreign Secretary to assist in their consideration of submissions relating to warrants under the Investigatory Powers Act 2016 (IPA) and authorisations under the Intelligence Services Act 1994 (ISA) for the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ).

17.5 We saw one instance where the Foreign Secretary had signed a thematic warrant but with a caveat, the effect of which was to exercise greater control over who could be added to the warrant. While this was perfectly justified in narrowing the scope of the warrant, it left some room for confusion with the unauthorised general descriptor remaining on the application submission and the signed warrant instrument. While recognising that the warrant should be read alongside the caveat, we observed that for clarity the general descriptor should have been removed by modification at the earliest opportunity.

35 With the exception of applications for targeted equipment interference warrants by law enforcement which do not require ministerial approval.

17.6 In circumstances where the Foreign Secretary chooses not to follow FCDO advice (as they are entitled to do), we continue to recommend that there should be a written account setting out why the advice was not followed.

17.7 The submissions handled by the FCDO often deal with complex and evolving issues and risks and it is important that they are presented in the clearest and most informative way. We are therefore supportive of efforts continually to improve and update submissions and we saw clear evidence of this from discussions with FCDO officials and in the papers we scrutinised.

17.8 The complexities and risks around this work were clearly demonstrated when applying The Principles to engagement with countries with questionable human rights records. In one case we examined, we felt that the legal risks under international humanitarian law were probably understated but that, on balance, the decision to authorise was defensible.

Northern Ireland Office (NIO)

17.9 We were satisfied that the NIO was discharging its function as a "gateway" and provider of advice to the Secretary of State to a very high standard. Officials carefully examine submissions, the vast majority of which are from MI5 and the Police Service of Northern Ireland (PSNI), challenging them where appropriate and producing objective and balanced advice for the Secretary of State. The NIO has developed an interim policy and made good progress on last year's Action to review and set a policy for its own retention of IPA warrant documents.

Scottish Government

17.10 The Scottish Government adopts a proactive approach with agencies. It provided good quality control of warrant applications and advice to the Minister for Justice and Veterans.

17.11 There was a good level of compliance with the IPA and the Code of Practice. Collateral intrusion and the potential for the collection of any legally professional privilege (LPP) or confidential material was considered carefully by the WGD.

18. Errors and breaches

Overview

18.1 The investigation of errors and breaches, either reported to us or discovered during our inspections, continue to be a critical part of our work. We investigate all reported matters, considering both the impact the error has had on the human rights of any individual affected and whether the report reveals any failings in the processes and safeguards in place at that authority.

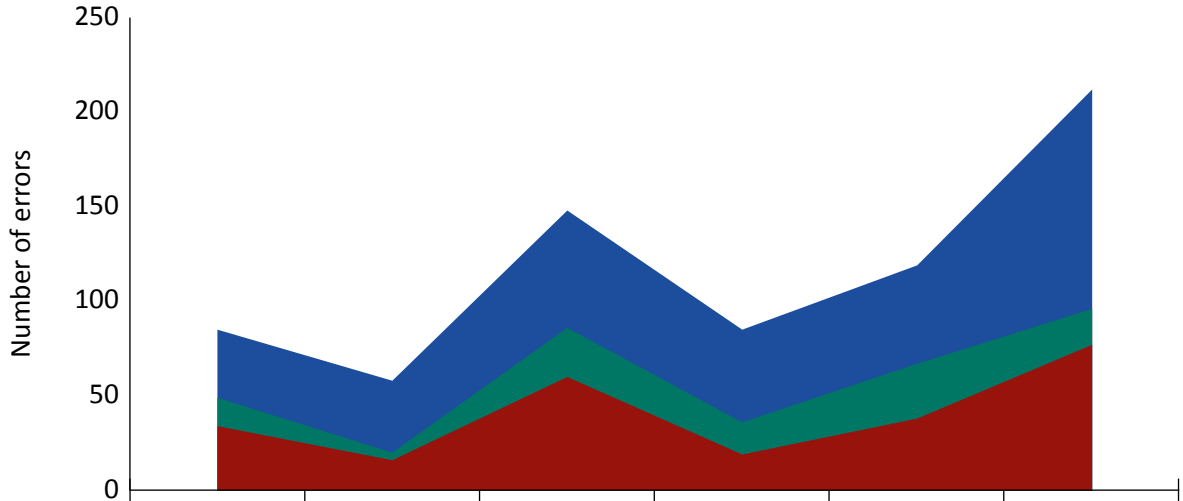
UK intelligence community (UKIC) errors

18.2 For 2022, the errors reported did not suggest systematic failures of safeguards or an attempt to act unlawfully or circumvent safeguards. The tables and graphs below show the relevant errors reported to the Investigatory Powers Commissioner (IPC) by UKIC.

Table 18.1: UK intelligence community (UKIC) errors, 2022

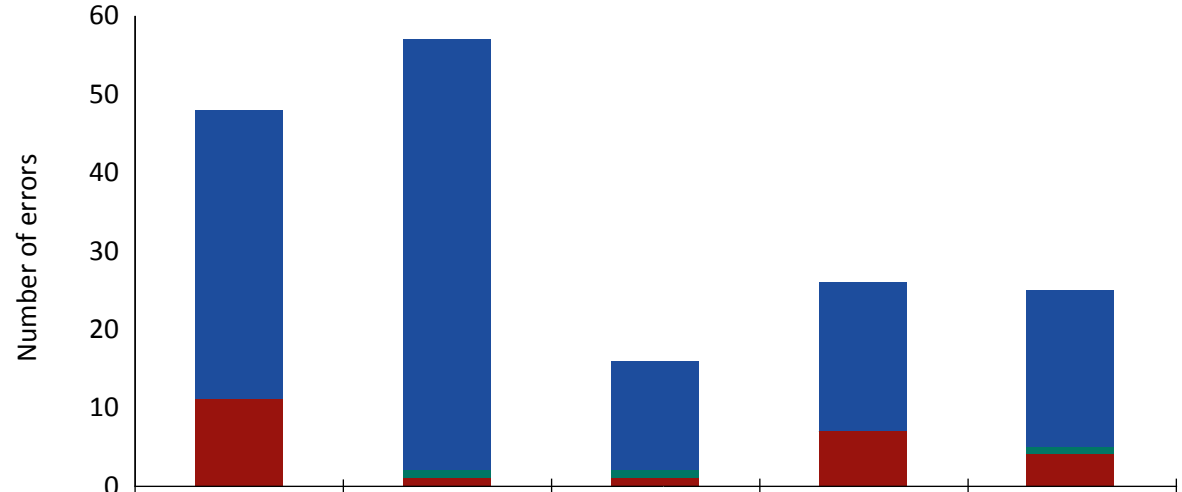
	Agency			
	MI5	SIS	GCHQ	Total
Covert human intelligence sources (CHIS)	9	4	1	**14**
Directed surveillance (DSA)	23	0	0	**23**
Property interference and intrusive surveillance (PI/IS)	10	0	0	**10**
Bulk personal data (BPD)	20	13	0	**33**
Section 7 Intelligence Services Act 1994 (s7 ISA)	0	0	0	**0**
Interception (interception)	47	0	71	**118**
Systems	0	0	1	**1**
Bulk/targeted equipment interference (EI)	6	1	5	**12**
Communications data (reportable) (CD)	20	1	4	**25**
The Principles	1	1	0	**2**
Total	**136**	**20**	**82**	**238**

Figure 18.1: UKIC errors (excluding systems and communications data), 2017 to 2022



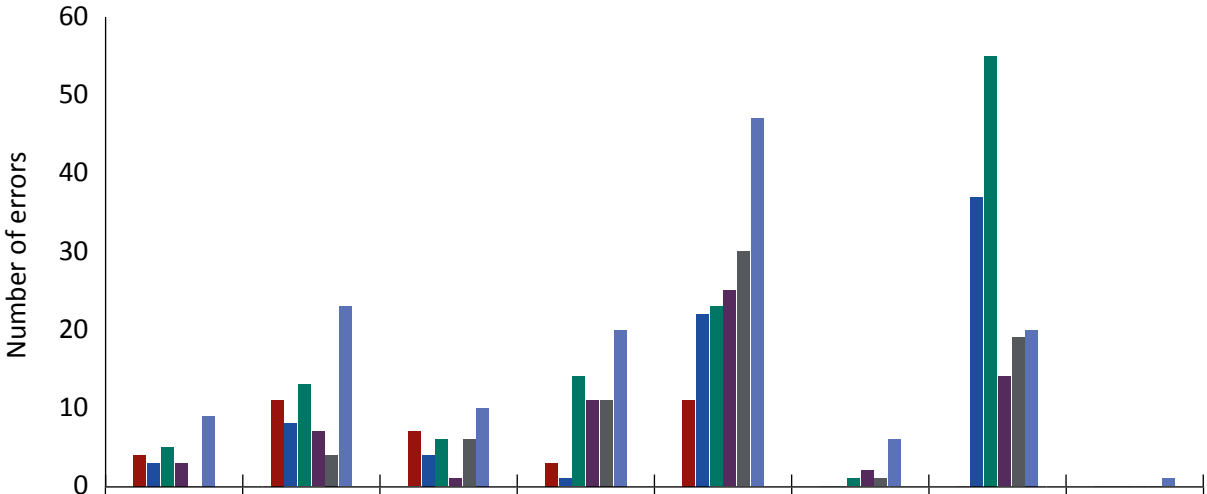
	2017	2018	2019	2020	2021	2022
MI5	36	38	62	49	52	116
SIS	15	4	26	17	29	19
GCHQ	34	16	60	19	38	77

Figure 18.2: Reportable UKIC communications data errors, 2018 to 2022



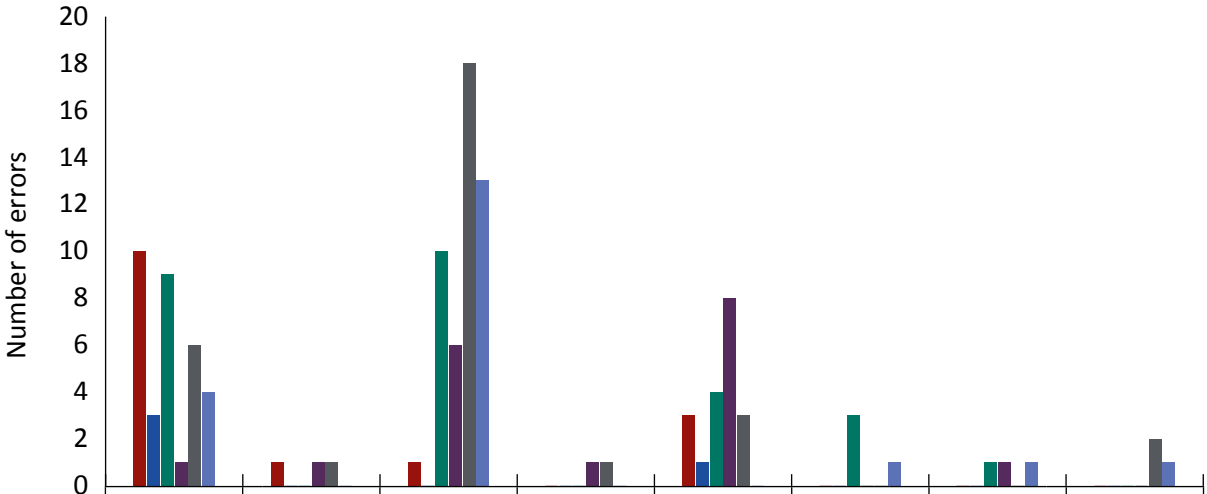
	2018	2019	2020	2021	2022
MI5	37	55	14	19	20
SIS	0	1	1	0	1
GCHQ	11	1	1	7	4

Figure 18.3: MI5 errors (excluding systems), 2017 to 2022



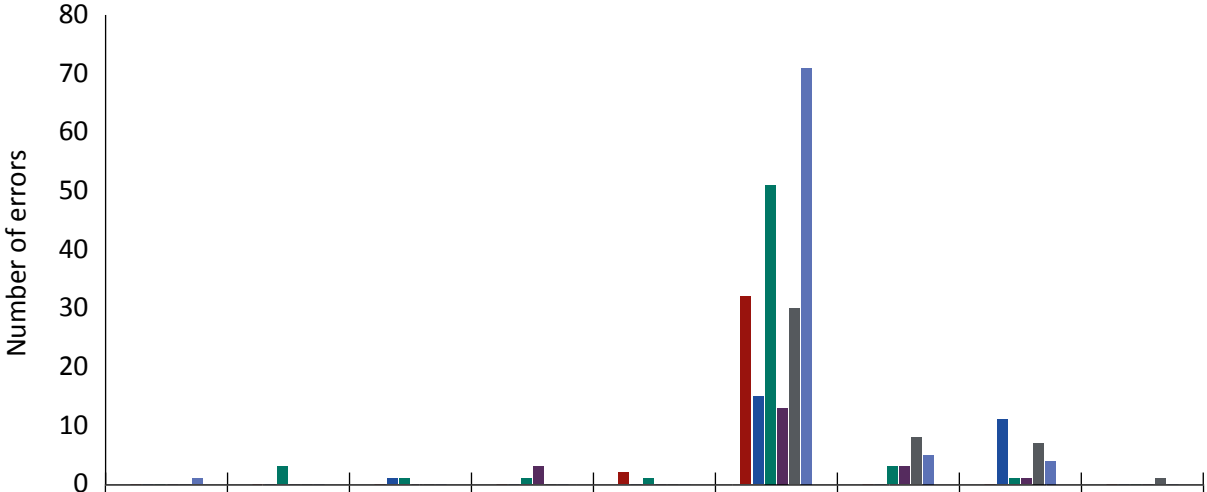
	CHIS	DSA	PI/IS	BPD	Interception	EI	CD (reportable)	The Principles
2017	4	11	7	3	11	0	0	0
2018	3	8	4	1	22	0	37	0
2019	5	13	6	14	23	1	55	0
2020	3	7	1	11	25	2	14	0
2021	0	4	6	11	30	1	19	0
2022	9	23	10	20	47	6	20	1

Figure 18.4: Secret Intelligence Service (SIS) errors (excluding systems), 2017 to 2022



	CHIS	DSA	BPD	s7 ISA	Interception	EI	CD (reportable)	The Principles
2017	10	1	1	0	3	0	0	0
2018	3	0	0	0	1	0	0	0
2019	9	0	10	0	4	3	1	0
2020	1	1	6	1	8	0	1	0
2021	6	1	18	1	3	0	0	2
2022	4	0	13	0	0	1	1	1

Figure 18.5: Government Communications Headquarters (GCHQ) errors (excluding systems), 2017 to 2022



	CHIS	DSA	PI/IS	BPD	s7 ISA	Interception	EI	CD (reportable)	The Principles
2017	0	0	0	0	2	32	0	0	0
2018	0	0	1	0	0	15	0	11	0
2019	0	3	1	1	1	51	3	1	0
2020	0	0	0	3	0	13	3	1	0
2021	0	0	0	0	0	30	8	7	1
2022	1	0	0	0	0	71	5	4	0

18.3 In 2022, UKIC reported 238 relevant errors compared to the 158 reported in 2021. This is a significant increase; however, analysis conducted on these errors indicates that a substantial number of them were historical and related to activity that had taken place before 2022. It is clear that a backlog of potential error reports had built up during Covid and it has taken some time for the agencies' own internal compliance units to investigate and reach decisions as to whether they were relevant errors and then report them to the IPC. It is anticipated that it will take further time for the agencies to address fully this backlog.

18.4 In 2022, MI5 reported 136 errors, an increase from the 71 reported in 2021. This was mainly due to an increase in directed surveillance, covert human intelligence sources (CHIS), bulk personal datasets (BPD) and interception errors. Most of these errors related to human error or to systems or processes not working as they should have done.

18.5 In 2022, SIS reported 20 errors, a decrease from the 32 reported in 2021.

18.6 In 2022, GCHQ reported 82 errors which was an increase from the 55 reported in 2021. This was mainly due to an increase in interception errors. The figure also includes 14 interception errors by the National Technical Assistance Centre (NTAC),[36] which is administratively part of GCHQ. While NTAC does not apply for warrants in its own right, it plays a key role in the delivery of lawfully intercepted communications to all interception agencies. The majority of the NTAC errors involved the routing of lawfully intercepted

36 NTAC errors have been included within the GCHQ total in previous years and the distinction is being made from 2022 onwards to provide increased transparency around the cause of interception errors.

product to the wrong intercept agency, or to errors in de-tasking of interception. These errors were discovered quickly and appropriate action was taken to rectify each case.

Interception and The Principles: law enforcement

18.7 There has been an overall reduction in the number of errors reported by LEAs with a decrease from 24 in 2021 to 22 in 2022. The breakdown of the 2022 errors is as follows:

- the National Crime Agency (NCA) reported 10 errors in 2022 compared to 16 errors in 2021. There was no particular theme to these errors and some of them had been found as a result of inspections undertaken by the NCA's own compliance team;
- the Metropolitan Police Service (MPS) reported three errors in 2022, compared to six reported in 2021. Of these, two related to interception and one related to The Principles;
- Police Scotland reported no errors in 2022;
- Police Service of Northern Ireland (PSNI) reported one error in 2022; and
- His Majesty's Revenue and Customs (HMRC) reported five errors compared to one error in 2021.

IT Systems

18.8 As we have discussed at paragraph 13.40, in late 2022 HMRC notified us of an error that it had discovered in relation to the IT system used by LEAs to manage and disseminate intercept product, specifically in relation to the system being unable to delete some of the data collected. Early in 2023, it became clear that the other LEAs that utilise the same system were experiencing similar issues. We have already commenced a series of bespoke inspections of the LEA intercepting agencies to explore this issue and will report on our findings in our 2023 report.

Warrant granting departments

18.9 In our last Annual Report, we noted that the Home Office had reported an error to us in the autumn of 2021 in relation to the signing of out-of-hours Investigatory Powers Act 2016 (IPA) warrants and that the full extent of this error was still being investigated. The investigation was completed during 2022 and we are satisfied that the Home Office has addressed and rectified the issue. Following our inspections of LEA intercepting agencies during the course of 2022, we are also satisfied that all agencies are now signing modification instruments at the time that authorisation is given.

Surveillance, property interference and covert human intelligence sources (CHIS): LEAs, public and local authorities and prisons

18.10 As set out in table 18.2, 60 errors relating to surveillance, property interference and CHIS (including relevant sources) were reported during 2022. This is an improvement compared to 2021 when 80 errors were recorded. While each error is regrettable, none of the errors constituted a serious error as defined under section 231 of the IPA; this means that no significant prejudice or serious harm was suffered by any individual as a result of any activity.

Table 18.2: Surveillance, property interference and CHIS errors for LEAs, public and local authorities and prisons, 2022

Investigatory Power	Number of errors
Directed surveillance	30
Property interference	15
Intrusive surveillance	0
Covert human intelligence sources (including relevant sources)	15
Total	60

18.11 The largest proportion of errors was in relation to surveillance. Considering the total number of authorisations, this remains reassuringly small. In line with previous years, the most common of surveillance errors were starting the surveillance before the authorisation had come into effect, or failing to obtain an authorisation or exceeding the parameters of the authorised activity.

18.12 Surveillance errors are often caused by a lack of awareness of the law or an overly narrow interpretation of what constitutes private information. Inspectors continue to encourage Covert Authorities Bureau (CAB) managers to provide regular refresher training to those officers who are most likely to engage the powers.

18.13 Property interference errors were predominantly in relation to the targeting of unauthorised vehicles. Restrictive terminology on authorisations, where it is anticipated that subjects are likely to have access to multiple vehicles for criminal purposes accounted for several errors. It remains key to reducing the frequency of these types of error that communication of the exact details of the authorisation is provided to Technical Surveillance Units (TSUs) and Surveillance Teams who are charged with installing and monitoring the equipment.

18.14 Most CHIS errors arose from the need for an authorisation either not being identified or being unnecessarily delayed while the source was assessed for their suitability for recruitment. On two occasions, the vulnerabilities associated with the CHIS were not appropriately accounted for; this should have resulted in the authorisation being provided by a more senior officer or member of staff. Relevant source errors were specifically in relation to the requirement to notify a Judicial Commissioner within seven days of granting an authorisation.[37]

18.15 A very small number of errors related to failures to comply with the requirements set out in Chapter 9 of the Codes of Practice relating to safeguarding material acquired through the use of covert investigative powers. One of these errors involved insufficient IT security measures being in place for the protection of highly sensitive material, namely sources' true identities. While the risk of compromise was assessed as very low in this particular case, such incidents highlight the importance of maintaining the highest standards of operational security and why the inspection of each public authority's records and product management procedures remains an important part of our inspections.

37 See: Covert Human Intelligence Sources Revised Code of Practice 2022 (Chapter 5.11)

Equipment interference errors: LEAs, public authorities and prisons

18.16 Four errors were notified or identified during inspection in relation to targeted equipment interference (TEI). These errors related to erroneous acquisition due to incorrect details being obtained and acted upon, conducting activity without the appropriate authorisation being in place, and exceeding the parameters of the authorisation. On each occasion, satisfactory arrangements were made to deal with the data acquired, no serious errors occurred and matters were appropriately reported in accordance with section 235(6) of the IPA.

18.17 In addition to these, we identified a TEI error during an inspection in late 2021 which was investigated as a serious error. This resulted in a determination being made by the IPC in 2022 that the error had resulted in significant prejudice and harm. In accordance with section 231 of the IPA, the IPC wrote to the affected party to inform them of their rights to apply to the Investigatory Powers Tribunal (IPT) if they wished to do so. The details are included in error investigation 12 in Annex C.

Communications data (CD) errors: LEAs, public authorities and prisons

18.18 There are two categories of error for CD: recordable, where the mistake has not resulted in the acquisition of CD; and reportable, where the mistake did result in the disclosure of CD and there is a duty on the public authority to notify the IPC.

18.19 The breakdown of errors for 2022 is shown in table 18.3. The data displays a pattern that mirrors previous years and does not cause us any specific concern or highlight any increasing trend or systemic failures. It is encouraging there has been a drop in the number of errors we have classed as potentially serious.

Table 18.3: Reportable communications errors, 2018 to 2022

Cause	Number of errors				
	2018	2019	2020	2021	2022
LEAs	758	755	741	899	835
Telecommunications operators	127	230	253	332	184
Postal	0	0	0	6	0
Other public authorities	13	14	10	15	13
Workflow	5	12	1	7	0
Total	**903**	**1,011**	**1,005**	**1,259**	**1,026**

18.20 As shown in table 18.4, it remains the case that most errors are the result of human fault where there has been a simple transposition of a number or letter in a communications identifier. These errors are usually noticed at a very early stage before any harm or prejudice has occurred. Of those errors we investigated, the biggest single cause was established to be the provision of an incorrect identifier by a third party to the public authority. This is most often the result of a miscommunication during dynamic life at risk situations where an incorrect telephone number has been provided to the police by a witness or a family member. In such circumstances, the Single Point of Contact (SPoC) has little or no opportunity to verify the data before submission and the mistake is only realised when the result is returned from the telecommunications operator (TO).

Table 18.4: Breakdown of communications errors by type and responsibility, 2022

	Applicant	SPoC	Telecoms/postal operator
Incorrect Identifier	377	67	50
Time/Date	23	205	16
Excess/No Data	0	0	104
System Error	0	0	5
No IPA authority	10	160	9
Total	**410**	**432**	**184**

18.21 Errors resulting from failures in TO systems are low and we maintain good liaison with those TOs who co-operate fully with us to identify and rectify the cause as soon as possible after detection.

18.22 The Error Reduction Strategy (ERS) designed to reduce the potential for errors occurring has been revised to provide further safeguards and the new version will be published in 2023. The new version includes recognition of the role performed by the Office for Communications Data Authorisations (OCDA) to ensure that source data has been verified through review by a second SPoC, prior to any authorisation being granted.

Serious error investigations

18.23 Section 231(1) of the IPA requires the IPC to inform a person of any relevant error if deemed serious, that is having caused them significant harm or prejudice, and it is in the public interest to inform them. A relevant error is defined as an error made by a public authority rather than a TO. Once a relevant error has been established, the IPC must then consider the seriousness. The circumstances in which we would investigate as potentially serious include:

- technical errors relating to the systems used by TOs to disclose CD to public authorities that have resulted in a significant number of erroneous disclosures;
- where a public authority has, as a result of a relevant error, made an arrest, searched a person's home, or made an improper disclosure of information; and
- errors which result in the wrongful disclosure of a large volume of CD or a particularly sensitive dataset.

18.24 None of our serious error investigations in 2022 involved an incorrect interpretation of a time zone conversion. While such errors did occur, adherence to the ERS by SPoCs ensured that the error was identified before any enforcement action had been taken.

18.25 In 2022, we investigated 11 relevant errors in relation to CD that may have resulted in serious harm or prejudice. None these cases were determined to reached the seriousness threshold required for the IPC to notify the person concerned.

18.26 Table 18.5 sets out the breakdown of the cause of each error. A summary of these investigations is set out in Annex C.

Table 18.5: Serious error investigations by cause, 2022

Error Type	Relevant public authorities	Telecoms operator/postal operator
Incorrect Data (Human)	5	1
Incorrect Data (System)	0	3
Hacking	0	1
Breach of Code	1	0
Total	**6**	**5**

19. Statistics

Overview

19.1 Each year, the Investigatory Powers Commissioner's Office (IPCO) gathers data on how investigatory powers are being used across the country. We have revised this process over the past two years and introduced some changes to ensure that the information being collated is, firstly, accurate and reliable and, secondly, a less time-consuming and complex undertaking for the organisations we oversee. This has seen the introduction of a standardised template and streamlined approach which we hope will ensure we collect the information we need in a proportionate way.

19.2 IPCO is required to publish statistics on the use of investigatory powers in line with section 234 of the Investigatory Powers Act 2016 (IPA). In addition to what we are obliged to publish, we aim to be as transparent as possible while balancing the need not to jeopardise the operational activities of the authorities we oversee or compromise national security. We also remain committed to not providing statistics which are partial or misleading in any way. This means our statistical publication is limited in areas where we would not be able to provide sufficient detail to contextualise that information or paint an accurate analytical picture for our readers. This is particularly pertinent for the functions of the intelligence agencies. However, as we have flagged in previous reports, we do not take a structured or statistically driven approach to oversight but rather believe a compliance risk-based approach and a focus on areas of clear public interest is more beneficial. As such, throughout this report, statistics have been included alongside our findings to provide the context in which they are being used.

19.3 We believe our selections for publication will give an accurate account of the categories of authority and the extent to which the powers we oversee are being used. Where possible, we have sought to present statistics in the same format used in previous years to enable comparisons to be made. We welcome feedback on the value of the statistics we publish and the level of transparency we offer through our report.[38]

Warrants and authorisations

19.4 In 2022, 332,442 warrants and authorisations were issued across all powers. Table 19.1 provides a further break down of this number. Law enforcement agencies (LEAs) continue to have larger numbers of authorisations due to their use of communications data (CD) powers.

38 Reference to statistics from the UK intelligence community (UKIC) refer to the three Security and Intelligence Agencies (MI5, Secret Intelligence Service and the Government Communications Headquarters) plus the Ministry of Defence. NB: some powers are only available to the three agencies.

Table 19.1: Investigative and other powers authorised by public authority sector, 2020 to 2022

	UKIC	LEA	WPA	Local authorities	Prison services	Total
2020	18,119	251,674	1,130	588	181	271,692
2021	17,458	284,815	870	368	271	303,782
2022	19,632	310,592	1,461	425	332	332,442

Notes:

[1] *This figure was incorrectly reported as 417 in our 2021 report.*

[2] *his figure was incorrectly reported as 303,831 in our 2021 report.*

19.5 Table 19.2 sets out the total number of warrants and authorisations issued, considered and approved in 2022. We have also included in this table some information on certain notifications to IPCO as well as the total number of submissions refused by Judicial Commissioners. A total of six applications were refused in 2022.

19.6 Judicial Commissioners also have the option to request further information on an application before making a decision. This would often involve internal discussions with the IPCO Legal Team, or, in many cases, the applicant would be required to provide additional information to clarify aspects of their application. There were 88 cases in 2022 where Judicial Commissioners sought clarification and for most of these, sufficient information was provided, or the application was revised by the applicant to enable it to be approved. Twelve applications were withdrawn (or no decision required) and, of those withdrawn, seven were as a result of enquiries by Judicial Commissioners.

Table 19.2: Breakdown of authorisations, notifications and refusals, including those considered by a Judicial Commissioner, 2022

	Considered by a Judicial Commissioner	Approved, issued or given	Refused by a Judicial Commissioner
Covert human intelligence sources (CHIS) including juveniles and relevant sources	N/A	2,226	N/A
CHIS criminal conduct authorisation	N/A	326	N/A
Directed surveillance	N/A	6,892	N/A
Intrusive surveillance	N/A	644	N/A
Property interference under section 5 of the Intelligence Services Act 1994	N/A	631	N/A
Property interference under the Police Act 1997	N/A	1,742	0
Bulk personal datasets – class warrant	111	111	0
Bulk personal datasets – specific warrant	77	77	0
Directions under section 219 of the Investigatory Powers Act 2016	0	0	0
Directions under section 225 of the Investigatory Powers Act 2016	5	5	0
Bulk communications data acquisition warrant	24	24	0
Communications data authorisation	N/A	310,033	N/A
Bulk interception warrant	30	30	0
Targeted examination of interception warrant	74	74	0
Targeted interception warrant	4,574	4,574	0
Bulk equipment interference warrant	16	16	0
Targeted examination of equipment interference warrant	73	73	0
Targeted equipment interference warrant	5,327	5,323	4
Mutual assistance warrant	0	0	0
Relevant source notification[1]	n/a	696	n/a
Request to retain legal professional privileged material	102	100	2
Notification under section 77 of the Investigatory Powers Act 2016	30	30	0

Note:

[1] *These notifications relate to a new undercover operative deployment and an operative may be deployed on multiple operations.*

Statutory purpose of applications

19.7 Table 19.3 provides the total number of authorisations by statutory purpose across the different investigatory powers. It is worth noting that a single application could employ more than one statutory purpose.

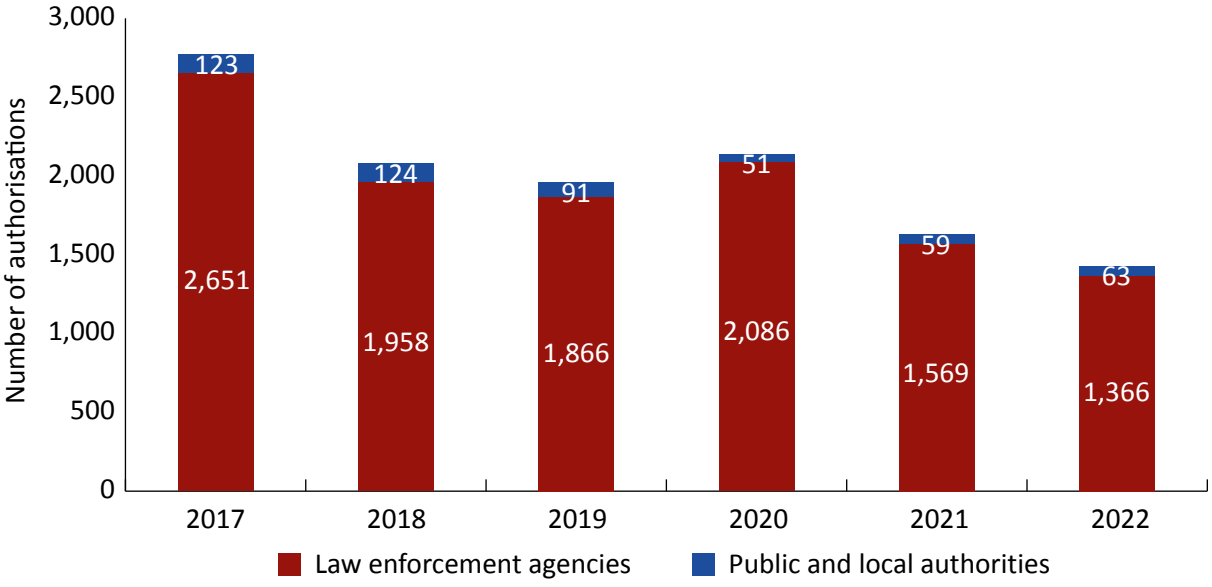
Table 19.3: Authorisations by statutory purpose, 2021 to 2022

	Number of authorisations	
Statutory purpose	2021	2022
Prevent/detect crime	268,697	271,374
Preventing death or injury	36,663	47,853
National security	13,772	16,374
Identify person	814	979
Interests of public safety	418	537
Economic well-being	360	223
Other	142	116

Covert human intelligence sources (CHIS)

19.8 Figure 19.1 shows the total number of covert human intelligence sources (CHIS) authorisations made in 2022 across LEAs, the wider public authorities (WPAs), local authorities and prisons. 1,429 authorisations were made in 2022 across all sectors. Of the 1,366 authorisations to LEAs, seven of these were urgent.

Figure 19.1: Covert human intelligence sources across law enforcement agencies, public and local authorities, 2017 to 2022



Juvenile CHIS

19.9 Of the 1,429 CHIS authorisations granted, only four related to juveniles. None of these were under the age of 16 at the time the authorisation was granted.

Criminal Conduct Authorisations

19.10 Provisions under the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 were commenced from June 2021, with authorisations being made from August 2021. In 2022, Judicial Commissioners were notified of 868 operatives being authorised under this legislation. The number of CHIS Criminal Conduct Authorisations (CCAs) made under section 29B of the Regulation of Investigatory Powers Act 2000 (RIPA) where a CCA was obtained totalled 326. It is worth noting that a single authorisation for criminal conduct may involve multiple operatives and a single operative might be authorised on a number of operations throughout the year.

Relevant sources

19.11 Renewals for authorisations for relevant sources (or LEA undercover police operatives) must be approved by a Judicial Commissioner at the 12-month stage. Table 19.4 sets out the number of relevant source authorisations and applications since 2020.

Table 19.4: Relevant sources authorisations and applications, 2020 to 2022[1]

	Total Applications (incl. renewals)[2]	Total Authorisations (incl. renewals)	Urgent	Renewals (long term authorisations)	Judicial Commissioner refusals[3]
2020	301	293	2	75	0
2021	495	434	4	74	0
2022	526	433	1	103	0

Notes:

[1] *Prior to 2020, IPCO reported data on "notifications" and cancellations of relevant sources. IPCO no longer collects or reports this data from public authorities.*

[2] *Applications include notifications to IPCO of authorisations and applications to renew authorisations after 12 months.*

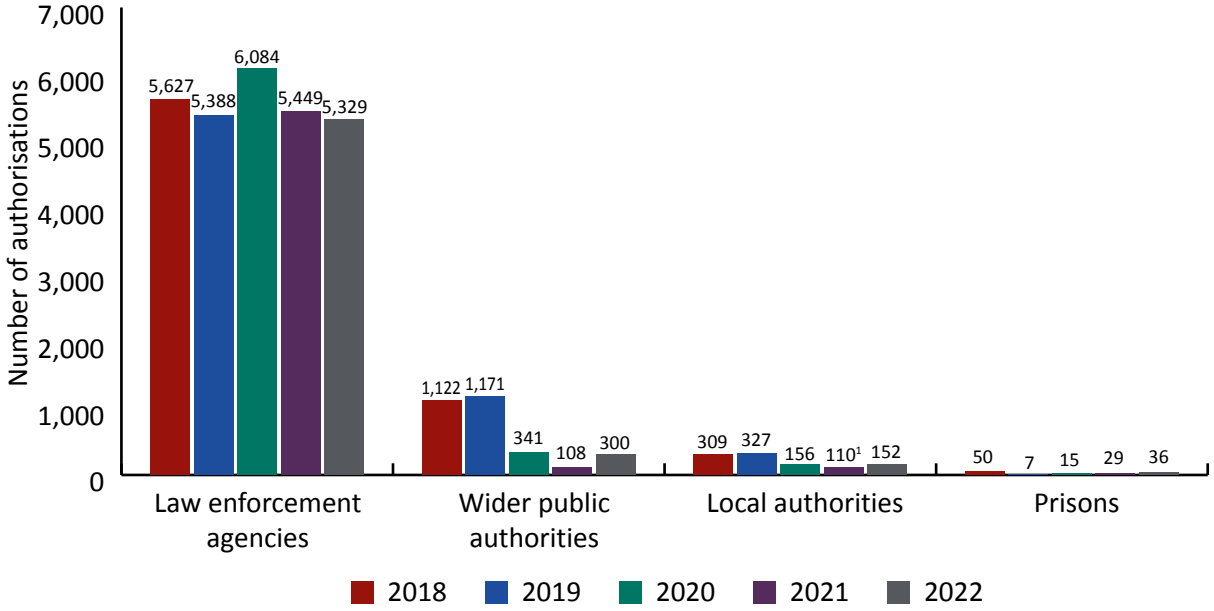
[3] *Refusals relate to applications to renew only.*

Directed surveillance

19.12 Figure 19.2 shows that a total of 5,817 directed surveillance authorisations were made in 2022 across LEAs, WPAs, local authorities and prisons. Of these authorisations, 564 authorisations were made under urgent provisions.

19.13 Thirty six applications were granted where legal professional privilege (LPP) was either sought or likely to be obtained. No authorisations were granted that either sought or were likely to obtain other confidential or privileged material.

Figure 19.2: Directed surveillance authorisations across law enforcement agencies, wider public authorities, local authorities and prisons, 2018 to 2022



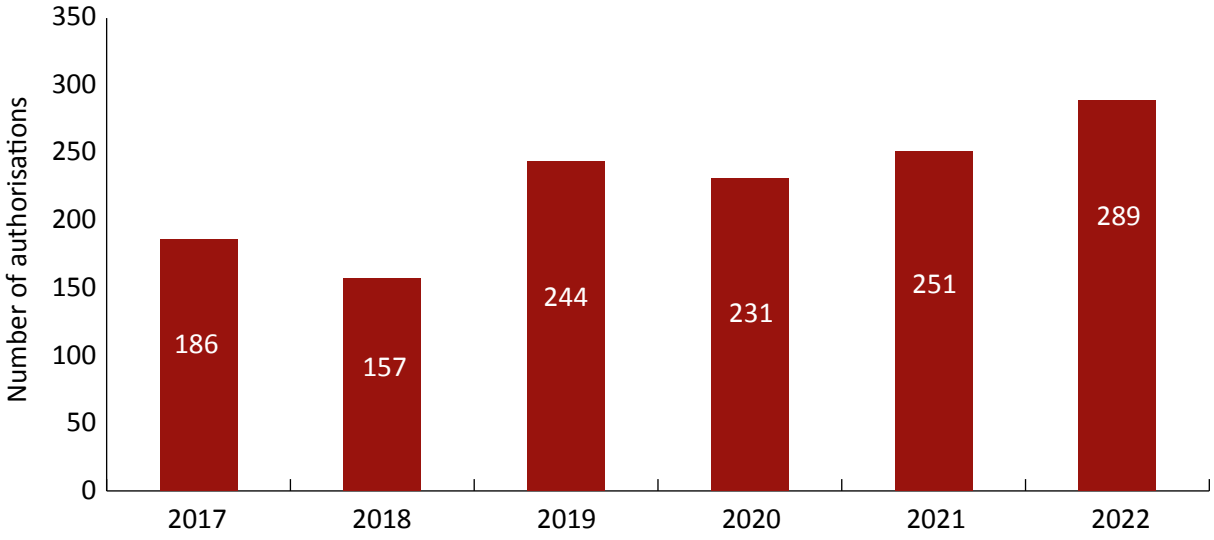
Note:

[1] *This figure was incorrectly reported as 159 in our 2021 report.*

Intrusive surveillance

19.14 In 2022, 289 authorisations were granted to LEAs. Of these, 26 were urgent authorisations. Of these, 17 authorisations either sought or were likely to obtain confidential of privileged material which was other than LPP. A further 24 were granted where LPP was either sought or likely to be obtained.

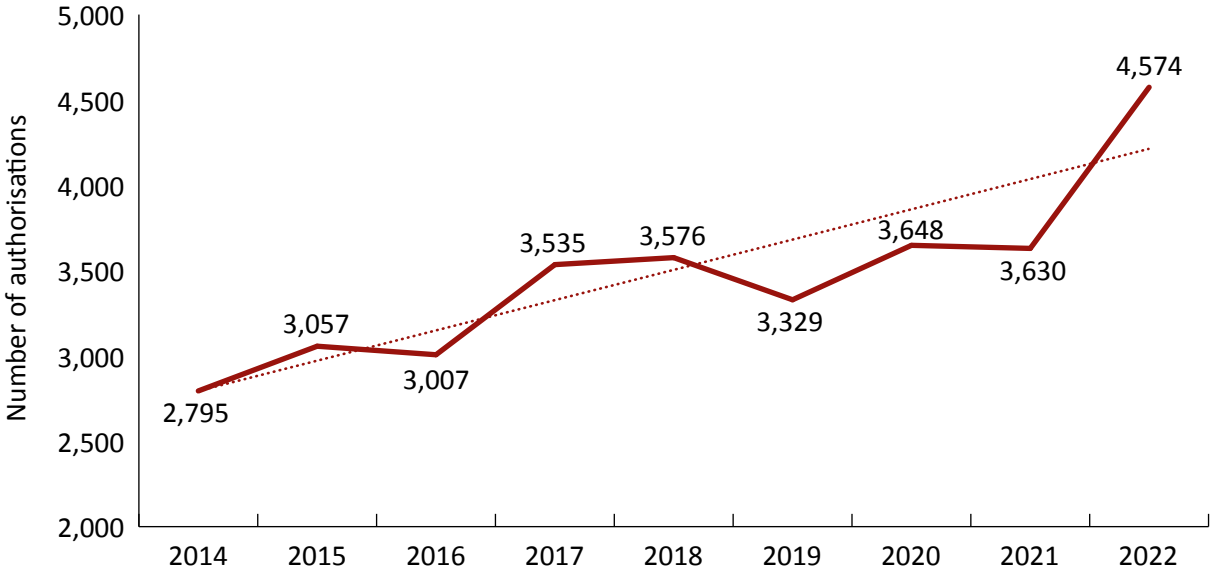
Figure 19.3: Intrusive surveillance authorisations for law enforcement agencies, 2017 to 2022



Targeted interception

19.15 Figure 19.4 shows the number of targeted interception (TI) warrants authorised in 2022. A total of 4,574 authorisations was made, an increase on previous years. Of the 4,574 authorisations made in 2022, 70 were urgent.

Figure 19.4: Targeted interception authorisations for the UK intelligence community and law enforcement agencies, 2014 to 2022



19.16 Table 19.5 sets out the number of TI warrants granted that involved either deliberate attempts to obtain legally privileged material (LPP – sought) as part of the purpose of the intercept warrant, warrants where it was likely or possible that LPP would be obtained (LPP – possible) or warrants relating to sensitive professions. As set out in the Code of Practice, all warrants which involved such confidential material are subject to additional scrutiny at inspection. The material produced by such warrants is also subject to additional safeguards in accordance with the Code of Practice.

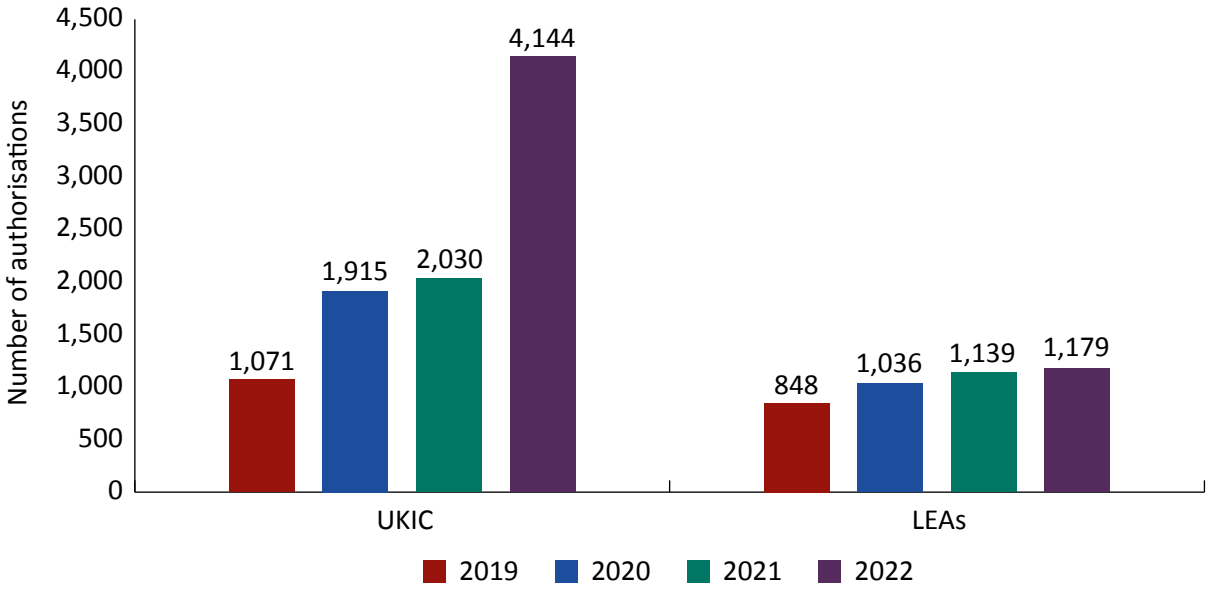
Table 19.5: Targeted intercept warrants involving confidential material, 2020 to 2022

	LPP – sought	LPP – possible	Sensitive professions
2020	12	359	35
2021	11	187	11
2022	29	211	20

Targeted equipment interference

19.17 In 2022, 5,323 authorisations were granted to use targeted equipment interference (TEI) powers, of which 351 were urgent. As was the case over the past two years, the three WPAs with access to TEI powers made no use of them in 2022.

Figure 19.5: Targeted equipment interference authorisations for the UK intelligence community and law enforcement agencies, 2019 to 2022



19.18 Table 19.6 shows that confidential material was only sought or likely to be obtained in a small number of TEI warrants.

Table 19.6: Targeted equipment interference warrants involving confidential material, 2020 to 2022

	LPP – sought	LPP – possible	Sensitive professions
2020	14	207	66
2021	15	64	14
2022	29	499	63

Communications data

19.19 In total, 310,033 CD authorisations of all kinds were made in 2022. These include applications made under section 60A, as authorised by the Office for Communications Data Authorisations (OCDA); warrants authorised under section 61 in the interest of national security (which were not authorised through OCDA); and those made under the urgent provisions. Table 19.7 shows the totals by sector and, as was the case in previous years, LEAs remain the greatest user of the power, responsible for over 96% of all authorisations made.

Table 19.7: Communications data authorisations, 2020 to 2022

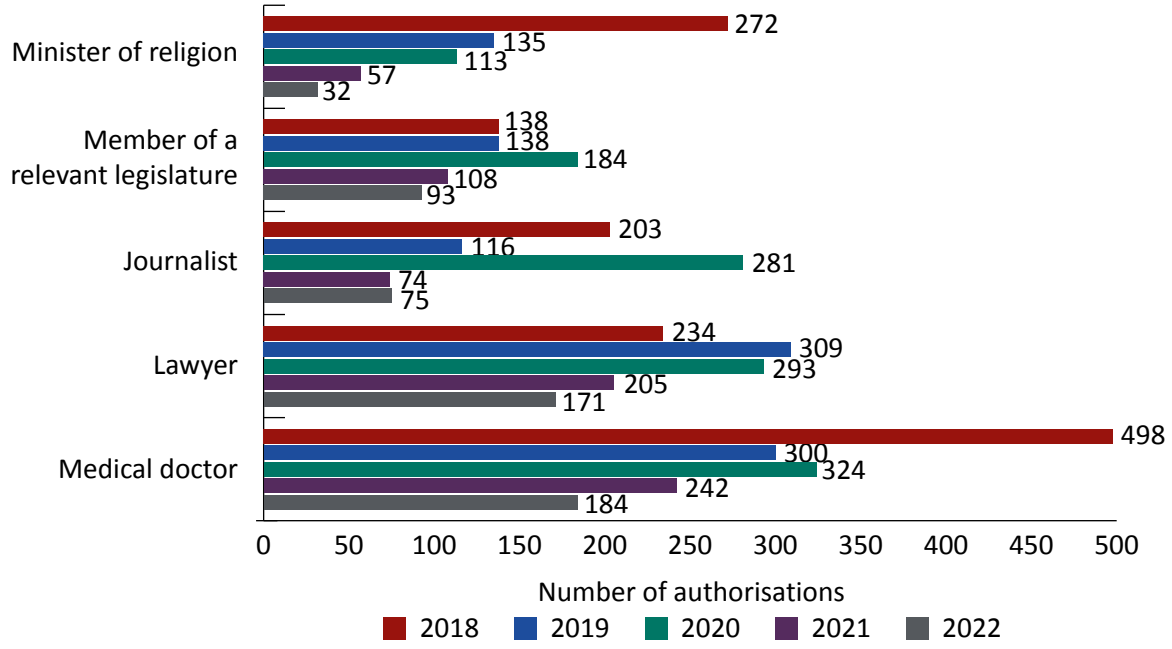
	UKIC	LEAs	WPAs	Local authorities	Prison services	Total
2020	11,444	239,086	969	212	155	251,866
2021	10,531	273,193	749	237	217	284,927
2022	9,200	299,166	1,150	258	259	310,033

19.20 CD applications are used to request one or more data items. Unfortunately, the systems used to process that data are not able to provide precise statistics and we believe there is a margin of error of around 10% on the number of data items obtained. That said, the nature of our oversight means that this does not reduce the level of confidence we have in those authorities. In 2022, just over 1.1 million data items were obtained.

19.21 Figure 19.6 sets out the number of authorisations obtained in relation to sensitive professions. CD acquired and disclosed under the IPA does not include content. Nonetheless, it must be considered whether there is a risk that acquiring the data could create an unwarranted risk that sensitive professional contacts will be revealed, or that there could be other substantive adverse consequences which are against the public interest. The Communications Code of Practice (from paragraph 8.8) requires applicants to give special consideration to requests for CD that relate to persons who are members of professions which handle privileged or otherwise confidential information. This can include, for example, lawyers, journalists, members of parliament, ministers of religion or doctors.

19.22 Public authorities must record the number of such applications and report to the IPC annually. Most applications relating to sensitive professionals were submitted because the individual had been a victim of crime. For example, it might be the case that a member of parliament or a lawyer received threatening or malicious calls and CD requests were made in an attempt to attribute phone numbers or email addresses to perpetrators.

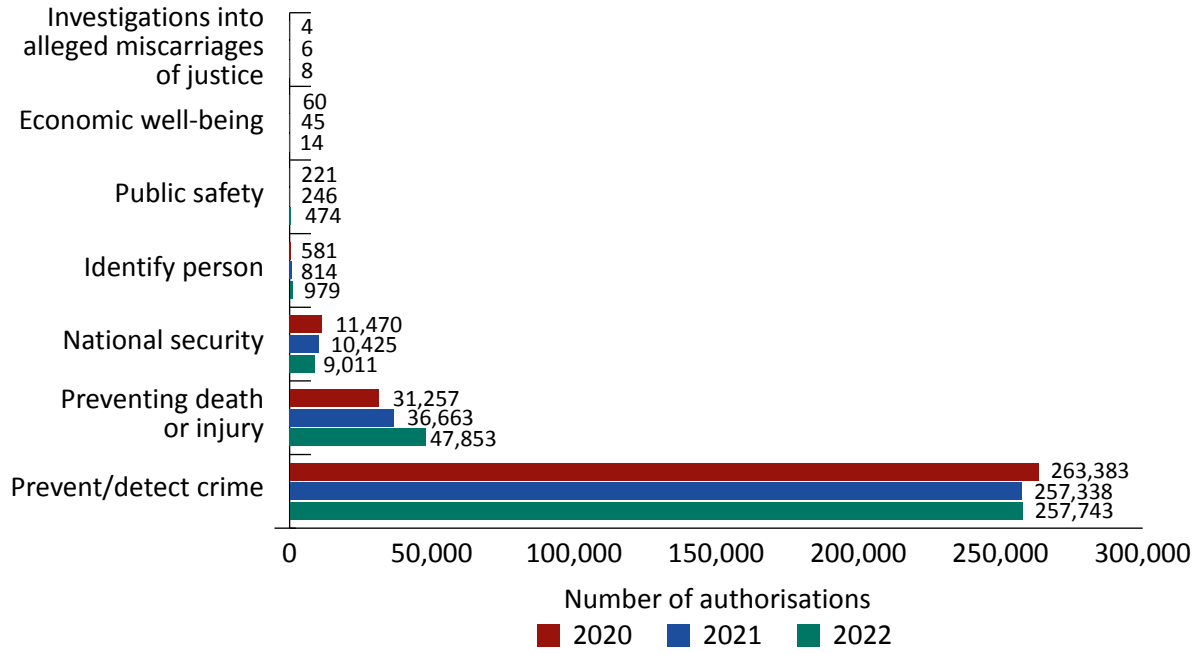
Figure 19.6: Communications data authorisations involving members of a sensitive profession, 2018 to 2022



19.23 A total of 31 applications for CD were made to confirm or identify a journalist's source, four of which were urgent. There were no Judicial Commissioner refusals in relation to these applications. A further 30 applications were made across all powers to identify a journalist's source.

19.24 Figure 19.7 shows the number of CD authorisations for each of the seven statutory purposes. Prevention and detection of crime remains the principal purpose, representing 81.5% of the total authorisations.

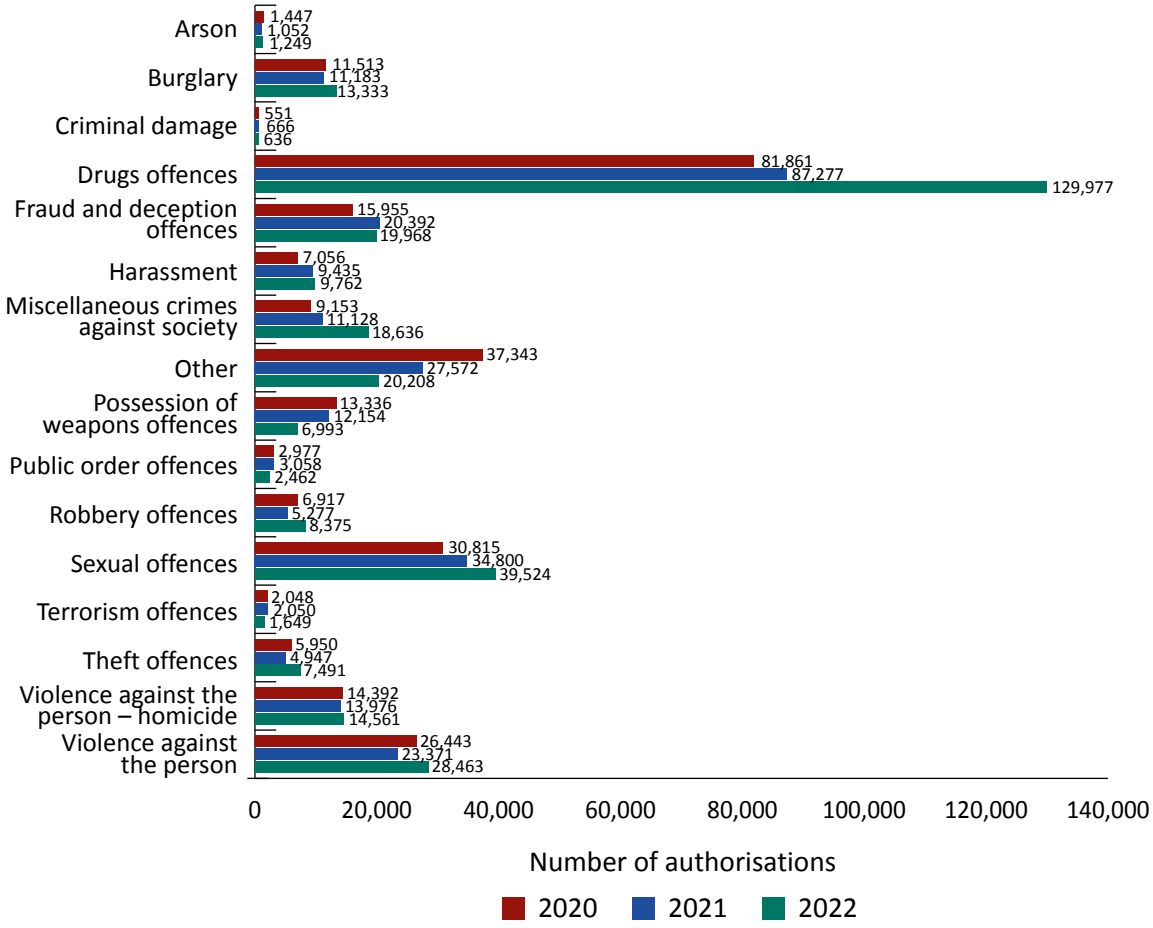
Figure 19.7: Communications data authorisations by statutory purpose, 2020 to 2022



19.25 For each CD authorisation where the statutory purpose is "prevention and detection of crime", public authorities who can use this purpose are required to keep a record of what types of crime the authorisation relates to. One authorisation may relate to more than one of the crime categories (as shown in detail in figure 19.8), which is why the total number of crime types exceeds the number of authorisations shown in table 19.7 above.

19.26 Figure 19.8 shows the number of authorisations where CD is being sought for an "applicable" crime as set out in section 60A(7), 61(7) or 61A(7) of the IPA. Drug offences make up the largest number of authorisations (40.2%), followed by sexual offences (12.2%).

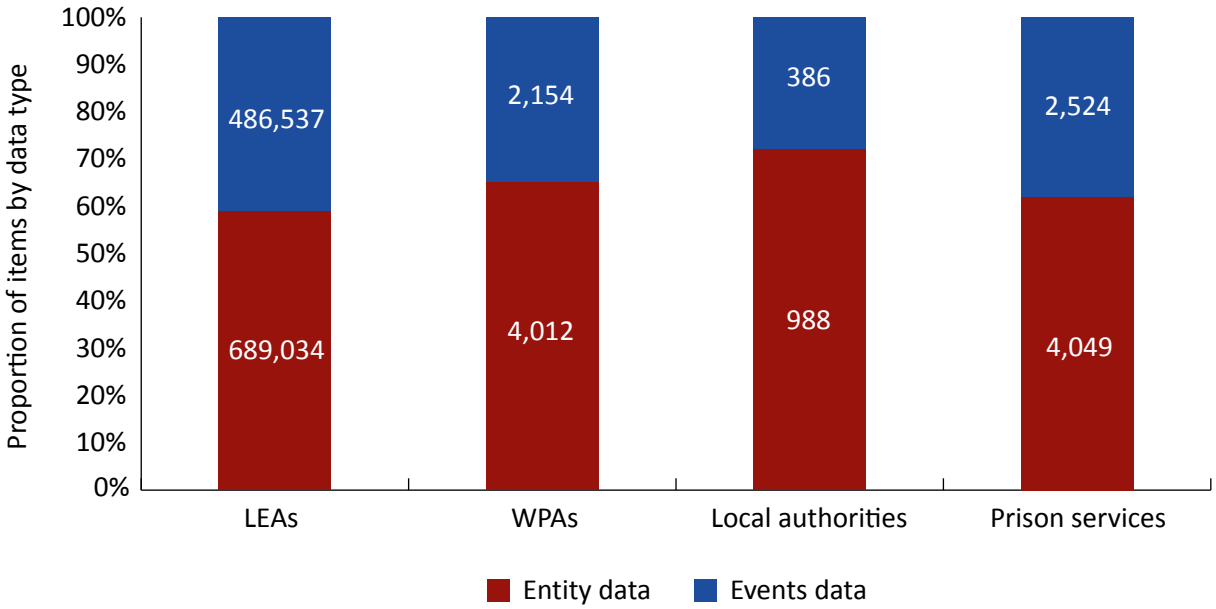
Figure 19.8: Communications data authorisations by crime type under the "prevent and detect crime" statutory purpose, 2020 to 2022



19.27 Figure 19.9 shows the total number of CD items sought in authorised applications by whether the items of data were categorised as either events or entity data. [39]

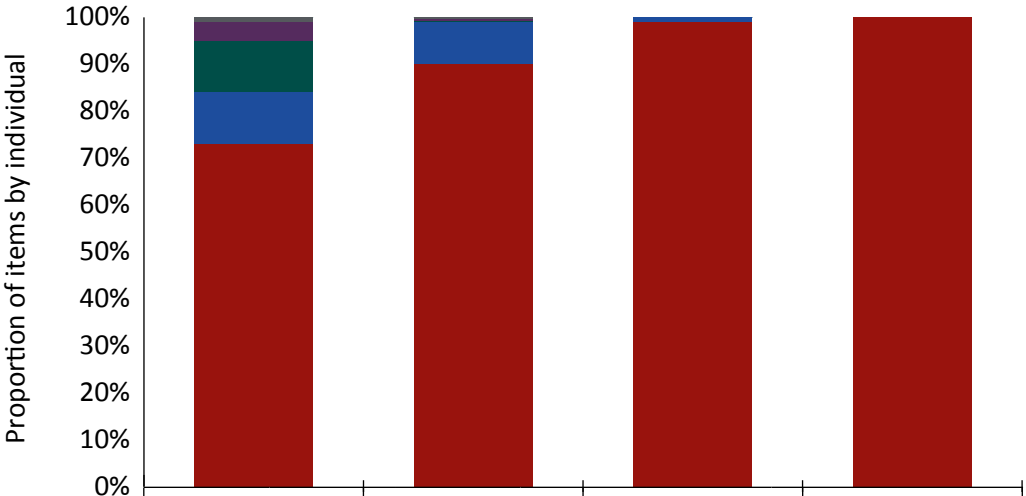
39 All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories:
- entity data: this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices); and
- events data: events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

Figure 19.9: Communications data items by data type, 2022



19.28 Figure 19.10 sets out the number of items of CD sought by the subjects of the authorisations. One authorisation may relate to more than one category of subject.

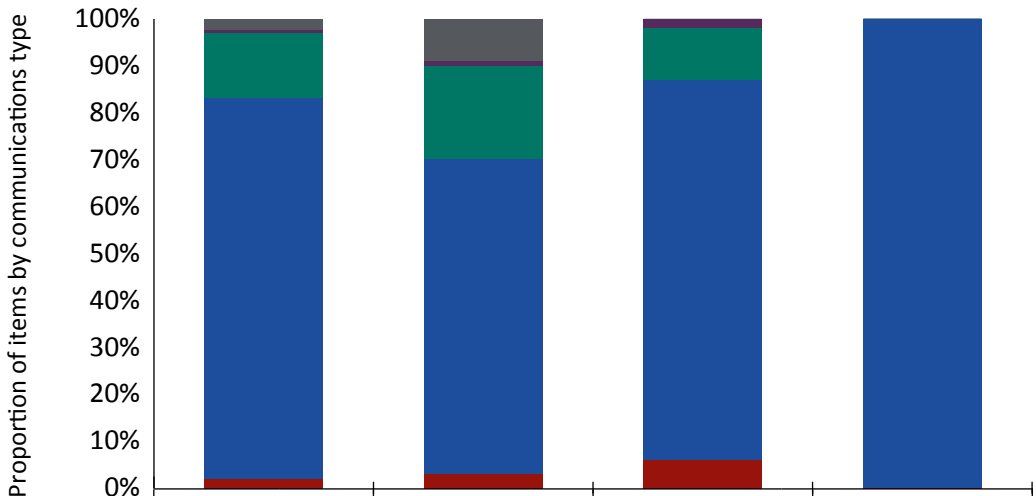
Figure 19.10: Communications data items by individual (subject), 2022



	LEAs	WPAs	Local authorities	Prison services
Next-of-kin	2,610	0	0	0
Witness	6,768	24	1	0
Victim and/or complainant	47,915	14	0	0
Vulnerable person	115,717	0	0	0
Other relevant person	123,260	512	13	0
Suspect	784,444	5,204	1,360	6,573

19.29 Figure 19.11 shows the total number of items of CD sought by the types of data that is being sought. An authorisation may involve several different data types and multiple items. It should be noted that, just because the items of CD were sought, it does not mean they were subsequently obtained.

Figure 19.11: Communications data items by communications type, 2022



	LEAs	WPAs	Local authorities	Prison services
Other	25,250	563	1	0
Postal	5,843	37	24	0
Internet	151,697	1,173	150	19
Mobile telephony	886,048	4,012	1,113	6,547
Fixed line telephony	21,937	176	86	7

Office for Communications Data Authorisations (OCDA)

19.30 Table 19.8 sets out the volume of applications received by OCDA between 2020 and 2022.

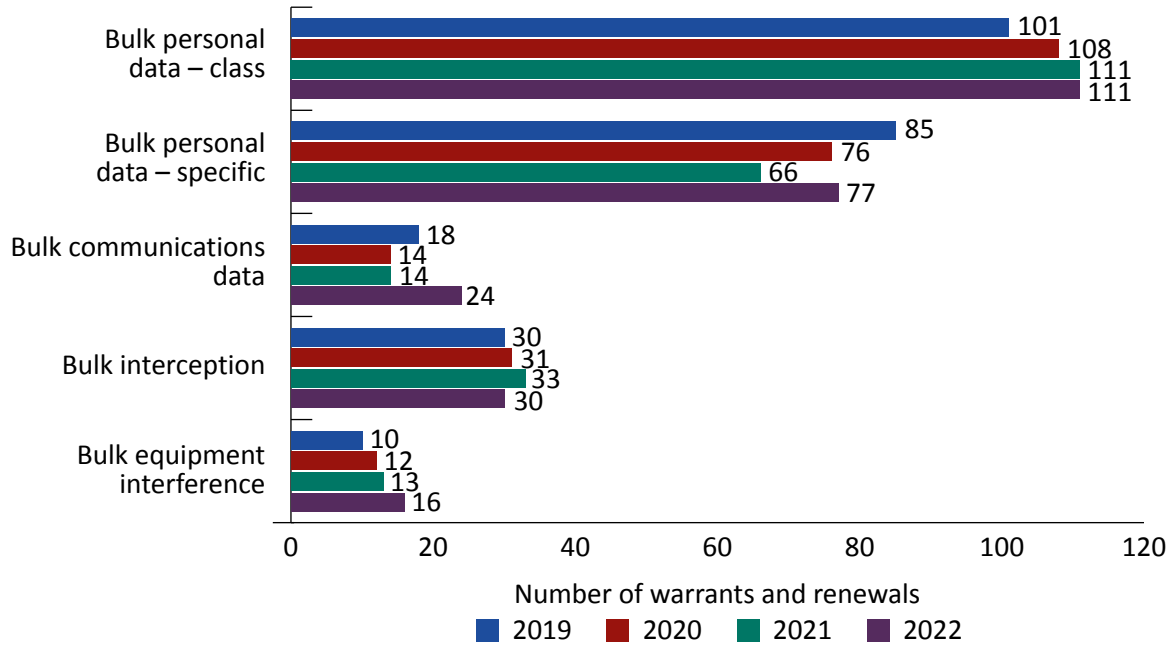
Table 19.8: Applications submitted to OCDA, 2020 to 2022

		2020		2021		2022	
Total applications		226,383		245,272		270,842	
Decisions made		223,322	98.6%	242,535	98.9%	266,755	98.5%
Of which	Authorised	199,482	88.1%	222,009	90.5%	245,125	90.5%
	Returned	23,596	10.4%	20,244	8.3%	21,529	7.9%
	Rejected	244	0.1%	282	0.1%	100	0.0%
Withdrawn		3,051	1.3%	2,736	1.1%	4,087	1.5%
Applications with no decision at year end (31 December)		10	0.0%	1	0.0%	0	0.0%

Bulk powers

19.31 Figure 19.12 shows the number of authorisations (including renewals) for each class of bulk warrant since 2019.

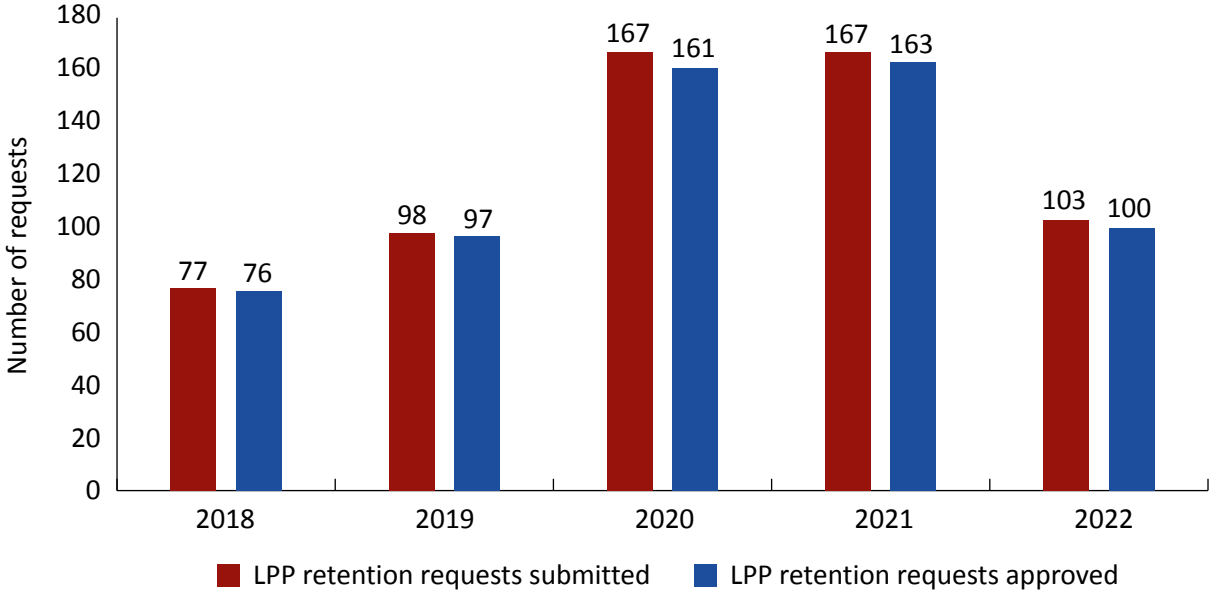
Figure 19.12: Bulk warrants and renewals by type, 2019 to 2022



Legal professional privilege (LPP) material

19.32 Public authorities must inform us if they think it is necessary to retain LPP material and apply to a Judicial Commissioner for permission to do so. In 2022, 100 approvals from 103 applications were made.

Figure 19.13: Number of requests submitted and approved for LPP material, 2018 to 2022



Intelligence Services Act 1994

19.33 Section 5 of the Intelligence Services Act 1994 (ISA) relates to interference with property or wireless telegraphy by the intelligence agencies. In 2022, 631 warrants were granted.

19.34 Section 7 of the ISA applies to acts done outside the UK and which are necessary for the proper discharge of a function of SIS and GCHQ only. In 2022, 75 warrants were issued.

The Principles

19.35 The Principles relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees (The Principles) is a published government policy relating to how the intelligence agencies, the Ministry of Defence (MoD), the National Crime Agency (NCA) and SO15 of the Metropolitan Police Service (MPS) must deal with detainees and intelligence relating to detainees overseas, outside UK jurisdiction. The Principles came into effect on 1 January 2020 and replaced the Consolidated Guidance. The Principles provide guidance in support of the UK Government's position that it does not participate in, solicit, encourage or condone unlawful killing, the use of torture or cruel, inhuman or degrading treatment (CIDT) or extraordinary rendition.

19.36 The table below sets out the total number of cases in which the Principles Partners have referred to Ministers for a decision because there was a real risk of one or more of the categories of unacceptable conduct as set out in The Principles. They also include the number of cases which the Partners have proactively brought to our attention because they raised particular legal or policy issues – some of which have informed the findings presented in this report.

19.37 There are important caveats to the data presented here:

- first, an increase in cases which cross the threshold of real risk does not necessarily indicate that the Principles Partners have taken additional risks in their engagement with overseas authorities. A single operation (in response to a major terrorist plot, for example) may generate a spike in referrals to Ministers. As such, it will not be possible to conduct a straightforward year-on-year analysis of these figures to determine whether or not the overall level of risk associated with the application of The Principles has increased. Similarly, a reduction in the number of cases does not necessarily suggest a lower risk appetite has been adopted; and
- secondly, as The Principles makes clear, consulting Ministers does not imply that action will or will not be authorised.

Table 19.9: Cases reviewed under The Principles, 2020 to 2022

Number of cases reviewed		2020	2021	2022
Cases reviewed on inspection		93	68	104
Cases reviewed proactively due to contentious legal or policy issues		8	7	7
Triggers: Total number of all cases (not limited to those reviewed on inspection)	Personnel knew or believed torture, unlawful killing or extraordinary rendition would occur	0	0	0
	Personnel identified a real risk of torture, unlawful killing or extraordinary rendition and submitted for approval despite the presumption not to proceed in such cases (this may include cases where engagement is intended to reduce the risks of unacceptable conduct or where there is an imminent threat of serious harm to individuals including children)	2	3	8
	Personnel identified a real risk of cruel, inhumane or degrading treatment (CIDT) and submitted for approval	15	17	17
	Personnel identified a real risk of rendition and submitted for approval	3	0	0
	Personnel identified a real risk of unacceptable standards of arrest and/or detention and submitted for approval	28	34	54

Annex A. Definitions and glossary

Annex A is divided into three parts:

- definitions of terms about the use and oversight of investigatory powers;
- a glossary of the authorities we oversee; and
- a summary of the abbreviations used throughout the report.

Definitions

Term	Definition
Bearer	A communication link carrying data e.g., Internet Protocol data.
Bulk communications data	This is communications data relating to a large number of individuals; communications data is the information about a communication but not the content. It includes the "who", "where", "when", "how" and "with whom" of a communication. This could be a list of subscribers to a telephone or internet service, for example.
Bulk interception	Bulk interception allows for the collection of communications of persons who are outside the UK. This enables authorities to discover threats that may otherwise be unidentified.
Bulk personal data	Bulk personal datasets are sets of personal information about a large number of individuals, for example, an electoral roll or telephone directory. Although the data held is on a large group of people, analysts will only actually look at data relating to a minority who are of interest for intelligence purposes.
Code of Practice	A Code of Practice provides guidance to public authorities on the procedures to be followed when they use investigatory powers. The advice offered in any Code of Practice takes precedence over any public authority's own internal advice or guidance. In general, there are separate Codes of Practice available for each power. These are available on the GOV.UK website

Term	Definition
Collateral Intrusion	Collateral intrusion is the interference with the privacy of individuals who are neither the targets of the operation nor of intelligence interest. An example of this would be the unintentional recording of background conversation of passers-by alongside the speech of the target. Additional intrusion to the privacy of the passers-by would have taken place – this is collateral intrusion. We expect public authorities proactively to assess the possible extent of collateral intrusion in any proposed activity and, where possible, take reasonable steps to prevent this.
Communications data	Communications data is the "who", "where", "when" and "how" of a communication but not its content. It enables the identification of the caller, user, sender or recipient of a phone call, text message, internet application or email (together with other metadata), but not what was said or written. In addition to electronic communications, it also covers postal services, enabling the identification of a sender or recipient of a letter or parcel.
Covert human intelligence sources	A covert human intelligence source (informally referred to as a "CHIS") is an informant or an undercover officer. They support the functions of certain public authorities by providing intelligence covertly. A CHIS under the age of 18 is referred to as a juvenile CHIS. Another type of CHIS is known as a "relevant source". This is the term used to describe staff from a designated law enforcement agency that are trained to act as undercover operatives and are subject to an enhanced authorisation and oversight regime. A CHIS may be authorised to participate in criminal conduct in specific circumstances, namely in the interests of national security; for the purpose of preventing of detecting economic crime or of preventing disorder; or in the interests of the economic well-being of the United Kingdom.
Covert surveillance	Surveillance is covert if it is carried out in a manner that ensures the subject of the surveillance is unaware that it is or may be taking place. Surveillance includes monitoring, observing or listening to people, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.
Directed surveillance	This is surveillance that is covert but not carried out in a residence or private vehicle. It could include the covert monitoring of a person's movements, conversations and other activities.

Term	Definition
Double lock	Public authorities must have authorisation to use the most intrusive investigatory powers. Authorities will therefore submit applications for the use of investigatory powers to a Secretary of State or a senior officer; this decision is then reviewed and authorised by one of our Judicial Commissioners – only with authorisation from one of our Commissioners can a warrant be issued. This is the double lock process. It ensures a two-stage approval for the use of investigatory powers.
Equipment interference	Equipment interference is the process by which an individual's electronic equipment may be interfered with to obtain information or communications. Activity could include remote access to a computer or covertly downloading a mobile phone's contents.
Interception	Interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.
Intrusive surveillance	This is surveillance which is carried out, for example, using eavesdropping devices in residential premises or in private vehicles. It may involve the covert presence of a listening device to capture conversations and ensure that the individual being observed is unaware that surveillance is taking place.
Modification	A modification is a change to a warrant authorising the use of investigatory powers. It is requested after the warrant has been issued. A modification to a warrant could be, for example, adding an additional individual so that their communications can be lawfully intercepted.
National Security Notice	Under section 252 of the Investigatory Powers Act 2016, a Secretary of State, with approval from a Judicial Commissioner, can issue a National Security Notice to direct a UK telecommunications operator to act in the interests of national security. This covers actions to assist the security and intelligence agencies, which may additionally be authorised under a warrant. National Security Notices could, for example, ask a company to provide access to a particular facility.
Operational purpose	The IPA establishes defined operational purposes for the use of BPD. An agency may only use bulk data for an operational purpose listed on the warrant under which the BPD is being retained and examined. Under the Act, the full list of operational purposes is approved by the Prime Minister.

Term	Definition
Promotion rules	These determine what intercepted data is forwarded to storage in order to make it available for selection for examination by analysts.
Property interference	Property interference is the covert interference with physical property, but also covers wireless telegraphy. This may be for the purpose of conducting a covert search or trespassing on land. For example, police may trespass to covertly install a listening device in a person's house.
Relevant Error	A relevant error is an error made by a public authority when carrying out activity overseen by IPCO. A relevant error is defined in section 231(9) of the Investigatory Powers Act 2016.
Section 7 of the Intelligence Services Act 1994	Section 7 of the Intelligence Services Act 1994 enables the Foreign Secretary to authorise activity by the intelligence agencies outside the UK that would otherwise be unlawful under domestic law.
Serious Error	Section 231(2) of the Investigatory Powers Act 2016 defines a serious error as one where significant prejudice or harm has been caused to an individual as a result of a relevant error.
Targeted interception	Targeted interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.
Technical Capability Notice	Under section 253 of the Investigatory Powers Act 2016, the Secretary of State, with approval from a Judicial Commissioner, may issue a Technical Capability Notice to require telecommunications or postal operators to ensure they are able to provide assistance with the acquisition of communications data, interception and equipment interference. After a Technical Capability Notice has been issued and implemented, a company can act quickly and securely when a warrant is authorised.
Thematic Warrants	Thematic warrants are warrants that have more than one subject. There are two types of thematic warrant: The first individually names/describes all the subjects. Any additional subjects can only be added by a modification – for law enforcement agencies, a modification requires prior approval by a Judicial Commissioner, or retrospective approval if the modification is urgent. The second does not individually name/describe each subject, because this is not reasonably practicable. For this type of warrant, the authority does not need to add subjects by modification: action may be taken against a person, organisation or piece of equipment (depending on the type of thematic warrant) included within the general description of the subjects.

Term	Definition
The Principles	"The Principles relating to the detention and interviewing of detainees overseas and the passing and the receipt of intelligence relating to detainees" are more commonly referred to as "The Principles". These are published by the Cabinet Office and apply to the intelligence services, the National Crime Agency, the Metropolitan Police Service, the Armed Forces and the Ministry of Defence. The Principles are intended to ensure that the treatment of detainees overseas, and the use of intelligence on detainees, is consistent with the UK's human rights and international law obligations. The document seeks to provide clear guidance to staff often operating in legally complex and challenging circumstances. The Principles came into force on 1 January 2020.
Urgency provisions	Urgency provisions are the conditions under which, due to time-sensitive operational reasons (such as an imminent threat to life), legislation permits a departure from the normal authorisation process. For an investigatory power that typically needs to be subject to the "double lock", the urgency provisions mean this can be used without a Judicial Commissioner's approval in advance. If an urgency provision is used, the person who decided to issue a warrant to use the investigatory power must inform a Judicial Commissioner that it has been issued and the power has been used. A Judicial Commissioner must then either: • decide whether to approve the decision to issue the warrant and notify the authority of the Judicial Commissioner's decision; or • decide to refuse to approve the decision, in which case activity under the warrant must stop and the Commissioner may direct that any information obtained under the urgent warrant be destroyed.

Further details on the authorisation process for each of these powers can be found on our website.[40]

40 See: https://www.ipco.org.uk/investigatory-powers/the-powers/

Glossary of authorities

Intelligence Agencies	• Security Service (MI5) • Secret Intelligence Service (SIS) • Government Communications Headquarters (GCHQ) References to "UKIC" mean the United Kingdom intelligence community.
Defence	The Ministry of Defence
Law Enforcement Agencies (LEAs)	• All territorial police forces in the UK • All other police forces including the British Transport Police, Ministry of Defence Police, Royal Military Police, Royal Air Force Police, Royal Navy Police, Civil Nuclear Constabulary, Port of Dover Police, Port of Liverpool Police • His Majesty's Revenue and Customs (HMRC) • The National Crime Agency (NCA) • The Home Office (Border Force and Immigration Enforcement)
Wider Public Authorities (WPAs)	• British Broadcasting Corporation (BBC) • Care Quality Commission • Centre for Environment, Fisheries and Aquaculture Science (CEFAS) • Charity Commission • Competition and Markets Authority • Criminal Cases Review Commission • Department for Business, Energy and Industrial Strategy (Insolvency Service) • Department for Levelling Up, Housing and Communities (DLUHC) • Department for Work and Pensions (DWP) • Department for the Economy for Northern Ireland • Department for the Environment, Food and Rural Affairs (DEFRA) • Department for Transport – Air Accidents Investigation Branch (AAIB) • Department for Transport – Driver and Vehicle Standards Agency (DVSA) • Department for Transport – Marine Accident Investigation Branch (MAIB) • Department for Transport – Maritime and Coastguard Agency (MCA)

	• Department for Transport – Rail Accident Investigation Branch (RAIB) • Environment Agency • Financial Conduct Authority (FCA) • Food Standards Agency • Food Standards Scotland • Gambling Commission • Gangmasters and Labour Abuse Authority (GLAA) • General Pharmaceutical Council • Health and Safety Executive • Health and Social Care Northern Ireland • His Majesty's Chief Inspector of Education, Children's Services and Skills (OFSTED) • His Majesty's Prison and Probation Service (HMPPS) • Independent Office for Police Conduct (IOPC) • Information Commissioner's Office (ICO) • Marine Scotland • Marine Management Organisation • Medicines and Healthcare Products Regulatory Agency • National Anti-Fraud Network (NAFN) National Health Service (NHS) Counter Fraud Authority • Natural Resources Wales • Department of Justice in Northern Ireland (Prison Service for Northern Ireland) • Office of Communications (Ofcom) • Office of the Police Ombudsman for Northern Ireland (PONI) • Police Investigations and Review Commissioner (PIRC) • Prudential Regulation Authority • Royal Mail Group • Scottish Accountant in Bankruptcy • Scottish Criminal Cases Review Commission • Scottish Environmental Protection Agency (SEPA) • Scottish Prison Service • Serious Fraud Office • Social Security Scotland • The Pensions Regulator • Transport Scotland • UK National Authority for Counter Eavesdropping (UKNACE) • Welsh Government • Welsh Revenue Authority
Local Authorities	• All UK local authorities
Prisons	All prisons in England, Wales, Scotland and Northern Ireland

Fire and Rescue Services	All separately constituted Fire and Rescue services in the UK
Ambulance Services	All UK Ambulance Services

Abbreviations

AA	Automatic acquisition
AI	Artificial intelligence
AI	Authorising individual
ACL	Access control levels
AO	Authorising officer
APCC	Association of Police and Crime Commissioners
CAB	Covert Authorities Bureau
CCA	Criminal Conduct Authorisations
CDR	Call data records
CFU	Counter Fraud Unit
CIDT	Cruel, inhuman or degrading treatment
CJEU	Court of Justice of the European Union
CMA	Computer Misuse Act 1990
CMT	Compliance Monitoring Team
COM	Covert Operations Manager
CoP	Code of Practice
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CSP	Communications service provider
DPA	Data Protection Act 2018
DSA	Directed surveillance authorisation
DSO	Designated Senior Officer
DSU	Dedicated Source Unit
DV	Developed vetting
ECHR	European Convention on Human Rights
EION	European Intelligence Oversight Network

ERS	Error Reduction Strategy
FACT	Federation against Copyright Theft
FIORC	Five Eyes International Oversight Review Council
HMGCC	His Majesty's Government Communications Centre
ICR	Internet Connection Records
IIOC	Indecent images of children
IP	Internet protocol
IPA	Investigatory Powers Act 2016
IPAR	Internet Protocol Address Resolutions
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
ISA	Intelligence Services Act 1994
JC	Judicial Commissioner
KET	Knowledge Engagement Team
LPP	Legal professional privilege
LTHSE	Long-Term High Security Estate
ML	Machine learning
MoU	Memorandum of Understanding
MPS	Metropolitan Police Service
NCDS	National Communications Data Service
NCMEC	National Centre for Missing and Exploited Children
NPCC	National Police Chiefs' Council
NSIRA	National Security and Intelligence Review Agency
NSWG	National Source Working Group
NUWG	National Undercover Working Group
NFC	Near field communications
NGO	Non-governmental organisation
OCDA	Office for Communications Data Authorisations
OpSy	Operational Security Officer

OSJA	Overseas Security and Justice Assistance
PCC	Police and Crime Commissioner
PIC	Participation in crime
PSI	Prison Service Instruction
PSNI	Police Service of Northern Ireland
RN	Retention notice
RfRs	Returns for Rework
RIPA	Regulation of Investigatory Powers Act 2000
RIP(S)A	Regulation of Investigatory Powers (Scotland) Act 2000
ROCUs	Regional Organised Crime Unit
RRD	Retention, review and deletion
S4E	Selection for examination
SIO	Senior Investigating Officer
SOP	Standard operating procedure
SOU	Special operations unit
SLE	Service level expectations
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
TAP	Technology Advisory Panel
TIDU	Technical Intelligence Development Unit
TSU	Technical Surveillance Unit
TO	Telecommunications operator
UCPI	Undercover Policing Inquiry
UTC	Universal co-ordinated time
WGD	Warrant Granting Departments

Annex B. Budget

The table below gives a breakdown of the financial statements for the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) for the financial year 2022/23.

	IPCO 01/04/2022 – 31/03/2023 Budget total: £6.4million	OCDA 01/04/2022 – 31/03/2023 Budget total: £10million
	2022/23 Full Year Outturn	**2022/23 Full Year Outturn**
Pay costs	£5,009,429	£4,344,568
Travel and subsistence	£299,348	£31,446
Office supplies and services	£18,661	£10,018
Training and recruitment	£22,592	£10,551
Estates	£634,986	£292,769
IT and communications	£273,717	£1,077,425
Legal costs (including consultancy)	£32,143	£0.00
Other costs and services	£31,577	£140,955
Capital costs	£0.00	£300,000
Total	**£6,322,453**	**£6,207,732**

IPCO

For the financial year 2022/23, IPCO spent £6.3million against the annual budget allocation of £6.4million. Salary costs continued to be the largest proportion of spend.

Travel and subsistence costs have increased significantly this year as we return to more face-to-face inspections and international travel.

IPCO spent less on estates costs this year in comparison to the last financial year as no essential work maintenance or refurbishment was required.

OCDA

OCDA spent £6.2million from the annual budget allocation of £10million for the financial year 2022/23. Despite extensive recruitment, the organisation remains below full headcount which has resulted in an underspend on salaries.

There has been a slight increase in travel and subsistence costs in comparison to the last financial year. However, the expenditure remains low due to hybrid working pattern and remote meetings.

Estates costs were significantly lower in comparison to 2021 partly due to facilities management and fixed fee costs for our offices in Manchester and Birmingham having not been settled in this financial year. We estimate these costs will be around £100,000.

Annex C. Serious errors

In 2022, the Investigatory Powers Commissioner (IPC) decided that the following errors would be investigated as a potential serious error within the meaning of section 231 of the Investigatory Powers Act 2016 (IPA). Further details on serious errors are given in Chapter 18 and as noted in there, our investigations have included those made by telecommunications operators (TOs).

Under section 231, the IPC is only able to decide that an error is a serious error if:

- the error caused significant prejudice or harm to the person affected; and
- the error was a relevant one (i.e., caused by a public authority).

If both of the above apply and having considered public interest or the prejudice to an ongoing investigation, the IPC shall inform the affected person of a right of remedy via the Investigatory Powers Tribunal (IPT).

Error investigation 1

	Public authority
Human or Technical:	Human (third party)
Classification:	Incorrect data (human)
Data acquired:	Subscriber details
Description:	A national helpline reported to the police real concerns for a person it had been in contact with. The helpline passed to the police the telephone number involved in its chat. Upon receipt of this information, communications data (CD) was acquired and the police visited the address linked to the number. Officers soon realised the occupants were not connected to the incident. It was established that the wrong number had been passed to police by the helpline. Using the details of the correct number, the right person was contacted and follow-up activity could take place.
Consequence:	A person unconnected with the incident became involved. Their involvement was not deemed to have caused significant prejudice or harm. The actual caller was found safe and well. In the light of this, the delay in attending the correct address was not deemed to have caused significant harm and so did not meet the threshold of a serious error.

Error investigation 2

	Public authority
Human or Technical:	Human (third party)
Classification:	Incorrect data (human)
Data acquired:	Subscriber details
Description:	A national helpline reported to the police real concerns for a person it had been in contact with. The helpline passed to the police the telephone number involved in its chat. Upon receipt of this information, CD was acquired and the police visited the address linked to the number. Officers soon realised the occupants were not connected to the incident. It was established that the wrong number had been passed to police by the helpline. Using the details of the correct number the right person was contacted and follow-up activity could take place.
Consequence:	A person unconnected with the incident became involved. Their involvement was not deemed to have caused significant prejudice or harm. The actual caller was found safe and well. In the light of this, the delay in attending the correct address was not deemed to have caused significant harm and so did not meet the threshold of a serious error.

Error investigation 3

	Public authority
Human or Technical:	Human (third party)
Classification:	Incorrect data (human)
Data acquired:	Broadband account holder details
Description:	A national helpline reported real concerns for the safety of a person it had been in contact with. The helpline passed on the IP address involved in its chat. The resulting data for the account holder became mixed up with a similar dataset unconnected to this incident. Officers who visited the address realised that it was not linked to their incident. Once the error was identified the correct data was obtained and a welfare check carried out. Upon attendance the officers learned the caller had already been taken to hospital.
Consequence:	A person unconnected with the incident became involved. Their involvement was not deemed to have caused significant prejudice or harm and so did not meet the threshold of a serious error.

Error investigation 4

	Public authority
Human or Technical:	Human (third party)
Classification:	Incorrect data (human)
Data acquired:	Subscriber details
Description:	A national helpline reported to the police real concerns for a person it had been in contact with. The helpline passed to the police the telephone number involved in its chat. Upon receipt of this, CD was acquired that did not fit other provided information. Recontacting the helpline established the number passed was incorrect. Once the correct number was provided, its location was identified. Officers who attended the address found help was already being provided by local care services. The delay caused by the error was approximately 90 minutes.
Consequence:	The delay was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error.

Error investigation 5

	Public authority
Human or Technical:	Human (third party)
Classification:	Incorrect data (human)
Data acquired:	Subscriber details
Description:	A public authority obtained subscriber details connected to a criminal investigation. After several failed attempts to speak to them a letter was sent to their home address. The letter sought contact to arrange a voluntary interview. Prior to the interview, the investigation discovered that, due to a transposition error the subscriber for the wrong number was obtained. A letter was sent cancelling the interview along with an explanation.
Consequence:	The investigation found no significant prejudice or harm sufficient for the IPC to write to the affected person.

Error investigation 6

	Public authority
Human or Technical:	Human (third party)
Classification:	Data acquired without lawful authority
Data acquired:	Postal data
Description:	A member of a public authority obtained CD from a postal operator without the necessary authority in place. As a result of the documentation provided, the postal operator supplied the requested data. The officer then sought advice about the interpretation of the data and the unlawful acquisition was identified.
Consequence:	An investigation was undertaken to determine whether an offence under section 11 of the IPA had occurred i.e., whether a person within a public authority had knowingly or recklessly obtained CD (in this case from a postal operator) without lawful authority. The investigation established the request had been made to the postal operator by a junior member of staff in good faith for a legitimate purpose. However, as a result of a lack of knowledge and experience, the correct authorisation procedure had not been followed. As a consequence, it was determined that no section 11 offence had occurred and the matter was left to the public authority to deal with by way of formal words of advice and additional training.

Error investigation 7

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect data (system)
Data acquired:	Call data records (CDR)
Description:	A TO reported to the IPC a technical issue. It advised that a certain type of call had not been captured resulting in a shortfall of data within a requested CDR. The affected period and data types were identified with the issue briefed out to all relevant public authorities. The missing data could not be recovered.
Consequence:	A three-month joint review between IPCO and the TO concluded that there had been no discernible impact. Under section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.

Error investigation 8

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect data (system)
Data acquired:	Call data records (CDR)
Description:	A TO reported a technical issue. It advised that a time stamp issue arose when changing from GMT to BST when the CD was sought. In two of the three file types returned, the date stamp expressed all records to be in UTC+1, even when GMT was prevailing. This issue risked investigators basing enforcement activity on data potentially one hour out.
Consequence:	All files (184) were recalled, with the time stamp issue rectified. The early identification of the issue and swift response by the TO ensured that no enforcement action was taken based on a flawed interpretation of the CDR. Under section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.

Error investigation 9

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Hacking
Data acquired:	Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	In 2021, we investigated and reported on three incidents where warrants had been executed on homes. In each case, no evidence was found of the uploading of indecent images of children. These investigations concluded that there had been a criminal use of a Virtual Private Network. As a result, the IPC concluded the circumstances did not amount to a relevant error. Before steps to raise awareness about this issue were taken in March 2022, three further reports were reported to the IPC in 2022.
Consequence:	The information provided to public authorities to help identify potential hacks has become mandatory reading to adhere to the most recent iteration of the Error Reduction Strategy. No further hacks were reported to the IPC in 2022.

Error investigation 10

	Telecommunications operator
Human or Technical:	Human
Classification:	Incorrect data (human)
Data acquired:	Subscriber details
Description:	The Police became anxious to trace a person who, having reported sexual abuse, rang off without providing any details. Such was the concern the force sought CD through the use of an urgent verbal authority. On the basis of the data acquired, officers attended at an address on a number of occasions without being able to speak to an occupant. The occupant later contacted police denying any knowledge. The TO involved was recontacted and after checking realised it had passed to police incorrect details for the subscriber.
Consequence:	A person unconnected with the incident became involved. Their involvement was not deemed to have caused significant prejudice or harm and so did not meet the threshold of a serious error. The actual caller was never identified as the correct number was linked to a 'pay as you go' unregistered phone, the exact location of which could not be ascertained. The number was also linked to a history of hoax calls.

Error investigation 11

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect data (system)
Data acquired:	Call data records (CDR)
Description:	A TO reported to us a technical issue. It advised that a certain type of call had not been captured which resulted in a shortfall of data within a requested CDR. The affected period and data types were identified with the issue briefed out to all relevant public authorities. The missing data was recovered. The now complete CDR was provided in all affected cases.
Consequence:	No adverse impact was reported.

Error investigation 12

	Public authority
Human or Technical:	Human
Classification:	Targeted equipment interference – Apple "find my iPad" facility activated without authority
Data acquired:	Location details
Description:	A police force conducted an investigation into potential criminal offences by a member of staff. When the individual was arrested for the allegations, the police force activated the "find my iPad" facility during a forensic examination of their iPhone and Apple account. The facility had not previously been enabled by the user. As a result of the activity, the police visited an address where they arrested the home owner and conducted a search for the iPad.
Consequence:	This error was identified during an IPCO inspection in late 2021 and the investigation concluded during 2022. The police believed the activity had been covered by its statutory investigation powers. However, the IPC determined that a targeted equipment interference warrant should have been obtained and that the error had resulted in significant prejudice and harm to the home owner. The IPC notified the person concerned of the circumstances, that also included a related issue involving interference with separate physical property, and their right to seek redress. The case is currently before the Investigatory Powers Tribunal.

Annex D. Public engagements

The Investigatory Powers Commissioner (IPC) undertook several public engagements in 2022. Details of those engagements are given below.

Meetings with Ministers, MPs and Peers

Date	Meeting
8 June	The Rt Hon Sir Julian Lewis MP, Chair of the Intelligence and Security Committee of Parliament
13 July	The Rt Hon Yvette Cooper MP, Shadow Home Secretary and Holly Lynch MP, Shadow Minister for Security
15 November	The Rt Hon Ben Wallace MP, Secretary of State for Defence

Engagement with NGOs and Academics

Date	Event
8 March	International Communications Data and Digital Forensics Conference
25 May	Reprieve
4 October	Serious and Organised Crime Exchange, Economic Crime Conference
21 November	Privacy International

Engagement with public authorities

In addition to the meetings listed below, the IPC meets regularly those authorities who he oversees.

Date	Meeting
12 January	The Rt Hon Lord Justice Singh, President of the Investigatory Powers Tribunal
17 March	Professor Fraser Sampson, Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner
25 May	National Crime Agency Lawyers
11 July	John Edwards, UK Information Commissioner
21 July	Professor Fraser Sampson, Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner
4 October	Andy Cooke QPM DL, His Majesty's Chief Inspector of Constabulary and Fire and Rescue Services

Engagements with overseas bodies

Date	Event
9 March	Senator James Paterson and Senator Jenny McAllister, Parliament of Australia (UK)
10 – 11 March	Intelligence Oversight Working Group (Switzerland). The IPC was represented by the Chief Executive and a member of the Technology Advisory Panel (TAP).
31 March – 1 April	Norwegian Parliamentary Intelligence Oversight Committee annual conference (Norway)
3 – 5 May	Canadian National Security and Intelligence Review Agency (UK)
23 May	Dutch Review Committee on the Intelligence and Security Services (UK)
29 September	Grant Donaldson SC, Australian Independent National Security Legislation Monitor (UK)
5 – 6 October	Intelligence Oversight Working Group (UK)
6 – 7 October	European Intelligence Oversight Conference (UK)
10 – 13 October	Norwegian Parliamentary Intelligence Oversight Committee annual conference (UK)
7 – 10 November	Five Eyes Intelligence Oversight and Review Council (USA)
8 November	South African Joint Standing Committee on Intelligence (London). The IPC was represented by a Judicial Commissioner and IPCO officials.
14 – 15 November	International Intelligence Oversight Forum (France). The IPC was represented by a Judicial Commissioner and an IPCO official.
18 November	Australian National Security College delegation (London). The IPC was represented by a Judicial Commissioner, an IPCO official and a member of the TAP.

Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU

E03026099
978-1-5286-4592-8