

Annual Report of the Investigatory Powers Commissioner 2024

Annual Report of the Investigatory Powers Commissioner 2024

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 16 December 2025

Laid before the Scottish Parliament by the Scottish Ministers 16 December 2025

HC 1277

SG/2025/160



© Crown copyright 2025

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated.
To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

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

978-1-5286-5934-5

E03422044 12/25

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	5
1. Introduction by the Investigatory Powers Commissioner, Sir Brian Leveson	6
2. IPCO internal development: governance, funding and engagement	9
3. Regulatory and legislative matters	17
4. Oversight activities and challenges	23
5. Errors and breaches	40
6. Litigation in 2024	51
7. Protecting confidential or privileged information	53
8. Technology	57
9. Technology Advisory Panel (TAP) Annual Report 2024	59
10. Statistics	62
Annex A. Definitions and glossary	83
Annex B. Budget	96
Annex C. Serious errors	97

Letter to the Prime Minister

The Rt Hon Sir Keir Starmer MP
Prime Minister
10 Downing Street
London
SW1A 2AA

24 July 2025

Dear Prime Minister,

I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office (IPCO) from 1 January to 31 December 2024.

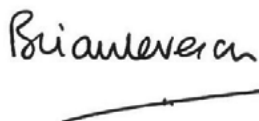
This is the first report following the merger of IPCO and the Office for Communications Data Authorisations (OCDA), which took effect on 1 March 2024. It reflects the work of the newly integrated organisation in independently authorising and overseeing the use of investigatory powers to ensure they are used in accordance with the law and in the public interest.

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 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.

In previous years, I have written to the Prime Minister separately regarding certain sensitive details that could not be published for reasons of national security. I have not done so this year as I have been able, following fact and sensitivity checks, to cover all matters in this report. If any matters subsequently emerge, I will write to you.

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 generally strong culture of compliance, dedication and professionalism demonstrated by those undertaking this vital work.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'Brian Leveson', with a horizontal line drawn underneath it.

The Rt Hon Sir Brian Leveson
The Investigatory Powers Commissioner

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



*Sir Brian Leveson,
Investigatory Powers
Commissioner.*

I am pleased to present my sixth Annual Report as Investigatory Powers Commissioner (IPC). As set out in section 234 of the Investigatory Powers Act 2016 (IPA), I am required to report to the Prime Minister about how the Judicial Commissioners carried out their functions during 2024.

A year ago, I brought the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data (OCDA) together into a single organisation.¹ I am pleased with how smoothly this transition has happened and that there has been no impact on how IPCO, as the organisation continues to be known, delivers its functions. Merging two organisations with distinct cultures and working practices across three geographical locations was not without challenge. However, these have been navigated by the leadership of my Executive Board and I recognise the determination from all staff to make this merger a success. I thank each and every one of them for their continued commitment.

As trailed in my 2023 Annual Report, this year's report looks different from those I have previously submitted. Following a review of the Annual Report process and compilation,² I agreed that a thematic approach to reporting on my functions was appropriate and would result in a more streamlined, focussed report, more accessible for readers and which I hope will enable it to be completed and published more quickly. That is not to say, however, that just because the report no longer has organisation specific chapters, that there has been any dilution in our authorisation practices or inspection methodology. The same high standards and rigour remain in all aspects of IPCO's work. Furthermore, I want to be transparent about my work to enhance public understanding of the use of investigatory powers and how they are overseen, and to build trust and confidence in IPCO as an oversight body. In 2024, I spoke more widely and publicly about our work and will continue to do so in 2025 as part of an enhanced engagement strategy.³

On the whole, I continue to observe good levels of compliance in respect of how investigatory powers are being used across the 600 public authorities I oversee. Applications seen by Judicial Commissioners and by IPCO's staff of communications data (CD) Authorising Individuals demonstrate a consistently high understanding of the statutory requirements. Inspectors routinely find good practices and procedures in place with staff applying the necessary safeguards. Through the errors regime, I see a healthy culture of self-reporting enabling systemic issues to be addressed and in rare serious cases, individuals to be notified where significant prejudice or harm has occurred. There are of course issues and challenges across the groups I oversee, and it is these matters that I have focussed on in this Annual Report.

1 See: from paragraph 2.2 for further details.

2 See: from paragraph 2.38 for further details.

3 See: from paragraph 2.18 for further details.

In my 2023 Annual Report, I referred to an investigation into an historical MI5 CHIS case, now publicly known as 'Agent X.' Although there was ongoing litigation throughout 2024, IPCO did not conduct any inspection activities on this matter during this period. As a result, it is not addressed in this Annual Report. On 2 July 2025, in response to the High Court judgment in relation to Agent X, I released a statement regarding IPCO's involvement to date⁴ and I will report further on this matter in my 2025 Annual Report.

Striking the right balance between upholding fundamental rights and the State's need to deploy investigatory powers to protect national security or to prevent serious crime is difficult and the role IPCO plays is vital to achieving this. There is no system without its flaws or drawbacks and, as the Home Office's reform of the IPA over the last few years demonstrates,⁵ there will always be new and evolving issues to address. However, from my engagement with oversight bodies across Europe, the Five Eyes and beyond, I see and hear the UK system held up as a benchmark of where independent oversight is working and enabling lawful access while protecting human rights. I am proud of what IPCO has achieved, particularly when I consider the breadth of our functions (including those I have taken on since IPCO was created in 2017) and the thoroughness in how these are carried out.

In 2024, we authorised over 300,000 applications and warrants and conducted 393 inspections, which is a continued year-on-year increase in delivery. Demand to use investigatory powers (especially CD)⁶ is increasing, while IPCO's resources have decreased, and we face new challenges such as the growing use of Artificial Intelligence by public authorities.⁷ I am aware of the financial pressures faced by the Government and the country and I acknowledge that IPCO must play its part. When in opposition, the present Home Secretary, the Rt Hon Yvette Cooper MP, said that strong powers need strong oversight.⁸ I wholeheartedly agree. Public authorities in the UK have strong investigatory powers and I and my team at IPCO provide strong oversight. I therefore ask the Government to remember this in its consideration of both funding and any legislative reform it may consider in the future.

4 See: <https://www.ipco.org.uk/news/statement-from-the-investigatory-powers-commissioners-office-ipco-re-his-majestys-attorney-general-v-bbc-and-r-on-the-application-of-beth-v-the-investigatory-powers-tribunal-2/>

5 See: from paragraph 3.3 for further details.

6 See: from paragraph 2.10 for further details.

7 See: from paragraph 8.2 for further details.

8 See: <https://www.rusi.org/news-and-comment/rusi-news/shadow-home-secretary-unveils-labour-approach-national-security-keynote-rusi-address>

Key issues covered in this report



This table highlights the principal issues examined in this report, providing a quick reference to the relevant sections.

1	Investigatory Powers (Amendment) Act 2024 The Investigatory Powers (Amendment) Act 2024 (IP(A)A) came into force in October 2024. The Act introduced targeted reforms to the IPA, including new safeguards and oversight functions for the IPC. [See: paragraphs 3.3 – 3.14]
2	Thematic inspection of relevant source activity In 2024, we conducted a thematic review of the arrangements in place for the authorisation and management of relevant source (undercover operative) activity across the UK. Overall, we identified good levels of compliance. [See: paragraphs 4.25 – 4.33]
3	Management of intercept material We continued to raise concerns about the outdated IT systems used to manage intercept material and the lack of a coherent replacement plan. We continue to urge the Home Office to treat this matter as a priority. [See: paragraphs 4.43 – 4.46]
4	Priority 2 CD applications We worked with public authorities to address the increasing number of communications data (CD) applications being graded as Priority 2 (intended for urgent operational needs only), which was placing pressure on our resources. [See: paragraphs 4.63 – 4.65]
5	Access to Foreign, Commonwealth and Development Office (FCDO) assessments In 2023, the Investigatory Powers Commissioner (IPC) was denied access to certain documents by the then Foreign Secretary, the first such refusal by a public authority. The IPC challenged this decision, leading to the documents being released in September 2024. This incident highlighted the importance of full disclosure in oversight of covert powers. [See: paragraphs 4.80 – 4.82]
6	The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees As in previous years, we continued to observe a high level of compliance with The Principles. While there were four cases where The Principles had not been correctly applied, we assessed these to be minor incidences of non-compliance. [See: paragraphs 4.94 – 4.103]
7	Errors In 2024, there was an increase in the number of errors reported by the UK intelligence community (UKIC) and the National Crime Agency (NCA). None of these errors or any of the other errors reported to us met the serious error definition. [See: chapter 5]
8	Oversight of Artificial Intelligence (AI) We defined our 'Scope of Interest in AI' and how it intersects with the use of investigatory powers and a framework, now used during inspections, to identify cases which fall within our oversight. [See: paragraphs 8.2 – 8.5]

2. IPCO internal development: governance, funding and engagement

Overview

- 2.1 This chapter highlights key developments within the Investigatory Powers Commissioner's Office (IPCO) in 2024, focusing on the merger with the Office for Communications Data Authorisations (OCDA), increasing demands on resources and internal staff developments. The chapter also covers efforts to improve efficiency, including changes to the deployment of Judicial Commissioners and enhanced staff training. Additionally, we outline IPCO's strengthened engagement with domestic and international stakeholders to support our mission of effective oversight.

Merger

- 2.2 On 1 March 2024, we announced the formal merger of IPCO and OCDA, with both organisations operating under the retained IPCO name. This milestone followed a period of progressive integration starting in 2020 when IPCO had begun consolidating back-office functions to improve efficiency and lay the groundwork for a unified organisation. The merger brought both bodies under a single governance framework, led by the Investigatory Powers Commissioner (IPC) and one Chief Executive.
- 2.3 Throughout 2024, we reviewed and embedded new ways of working, harmonised policies and procedures and built an inclusive culture through staff-led initiatives. IPCO's functions all stem from the statutory responsibilities of the IPC and the teams responsible for these functions support and complement each other. We ran internal staff workshops to develop a new mission and update our values for the new organisation in 2024, which can be found on our website.⁹
- 2.4 After the merger, we have collaborated with the Home Office to develop a new framework agreement, which sets out the governance arrangements between IPCO and the Home Office as our sponsoring department. We will publish this on our website once it is finalised.

Funding

- 2.5 Our ability to deliver effective oversight depends on having the appropriate resources to fulfil the IPC's statutory responsibilities. Since our establishment in 2017, our remit has expanded significantly, both in terms of the volume and the complexity of the work we undertake. This includes the authorisation and oversight of investigatory powers, inspections across hundreds of public authorities and the integration of new responsibilities introduced through legislative changes.

9 See: <https://www.ipco.org.uk/news/sir-brian-leveson-announces-the-merger-of-ipco-and-ocda/>

- 2.6 Against this backdrop, the question of sustainable funding is critical. The Investigatory Powers Act 2016 (IPA) recognises this in section 238(2), which sets out the duty of the Secretary of State to provide the IPC with the staff, accommodation, equipment and other facilities necessary to carry out the IPC's functions:

The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—

- (a) such staff, and*
- (b) such accommodation, equipment and other facilities and services, as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.*

Settlement for 2025/26

- 2.7 For the financial year 2025/26, the Home Secretary has allocated £15.31 million to the IPC to support the delivery of his statutory functions through IPCO. This represents an approximate 4% reduction compared to 2024/25. While this presents a significant challenge, we expect to manage the impact through the reprioritisation of activities and the implementation of efficiency measures.
- 2.8 A key area of focus has been the continued enhancement of our IT systems.¹⁰ In 2024/25, we invested in technology to streamline warrant processes and improve operational efficiency. While these improvements are expected to generate resource savings, rising demand for our services may offset these gains. In the best-case scenario, efficiencies will allow us to redeploy resources to meet this growing demand.
- 2.9 We plan to continue this investment in 2025/26, albeit at a reduced scale due to the lower funding allocation and uncertainty over future budgets. One key IT project is scheduled for completion, though its timeline has been extended to accommodate financial constraints. As a result, the delivery of anticipated benefits will be delayed and other planned projects may need to be deprioritised.

Increasing demand

- 2.10 Demand for our work has increased since IPCO was set up in 2017 and OCDA was set up in 2019. Applications for communications data (CD) have increased by 31.5% from OCDA's first full year in 2020 to the end of 2024, with an expected further increase of 8-9% in 2025.
- 2.11 The complexity of CD requests has also increased due to evolutions in technology and how people use communications services. We dedicate more time to these complex applications, placing greater demands on resources. We anticipate that this trend of increasing complexity will continue.
- 2.12 Applications for warrants have remained relatively consistent between 2022 and 2024. However, there has been a rise in some specific authorisations under the Regulation of Investigatory Powers Act 2000 (RIPA). Notably, applications to renew the deployment of an undercover officer have increased from approximately six per month in 2023 to over 10 per

10 See: from paragraph 8.6.

month in 2024.¹¹ For each renewal, we undertake an inspection of the operation, prepare a report of our findings and secure approval from a Judicial Commissioner.

- 2.13 Since we were established in 2017, the IPC has taken on additional responsibilities without any additional funding. These responsibilities include:
- overseeing the implementation and operation of 'The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees';
 - approving the retention of articles and the copying of digital devices during port stops to counter state threats under Schedule 3 to the Counter-Terrorism and Border Security Act 2019;
 - overseeing compliance by UK authorities with the UK-US Data Access Agreement;
 - overseeing the Equities Process, which underpins the way the Government Communications Headquarters (GCHQ) makes decisions on vulnerabilities in technology;
 - overseeing the express power for a covert human intelligence source (CHIS) to participate in criminal conduct through a Criminal Conduct Authorisation (CCA);
 - providing prior approval for the selection for examination of bulk interception and bulk equipment interference product in order to identify confidential journalistic material and confidential journalistic sources;
 - providing prior authorisation for the UK intelligence community (UKIC) using targeted CD requests made only for serious crime purposes; and
 - overseeing new bulk personal dataset regimes under Part 7A and Part 7B as introduced by the Investigatory Powers (Amendment) Act 2024 (IP(A)A).¹²
- 2.14 These additional requirements have varied in their impact on our workload, with some leading to substantial increases and others to more modest demands. However, it is the cumulative effect of these expanding responsibilities that underscores the need for sufficient resources to ensure we can meet our obligations effectively.

Value for money

- 2.15 We consistently seek to improve value for money when delivering our functions. We have reviewed and improved working practices, recently reduced the number of Judicial Commissioners and the number of days they work, invested in technology to improve efficiency and increased the number of remote inspections we undertake.

Future funding: Spending Review 2025

- 2.16 The Government has engaged with us, via the Home Office, in the Spending Review which is allocating resource (RDEL) for the financial years 2026/27 and 2027/28 and capital (CDEL) for 2026/27, 2027/28 and 2028/29.
- 2.17 As of July 2025, when we are submitting this report to the Prime Minister, we do not know what the outcomes of this Spending Review mean for IPCO. However, we have been clear throughout the process that we have made all the efficiencies that can be made without

11 This is based on the number of nine-month reviews of operatives that are conducted ahead of the 12-month renewal.

12 See: from paragraph 3.4.

significant change to our operating model. Any further reductions in funding for future years will likely require a change to the service we provide to HMG and public authorities. This could include:

- reducing the frequency and/or depth of our inspections which will reduce the quality of our oversight of investigatory powers; and/or
- increasing the timeframes of the Service Level Expectations we have for authorising CD applications. These are not statutory, so the IPC has the authority to change these at his discretion to reflect and align with the resources available to meet the demand. Increasing these will mean IPCO will have a longer time period within which to respond to CD applications, which is likely to slow down police investigations and could therefore have a real-world impact on solving crime and a negative impact on the victims of crime.

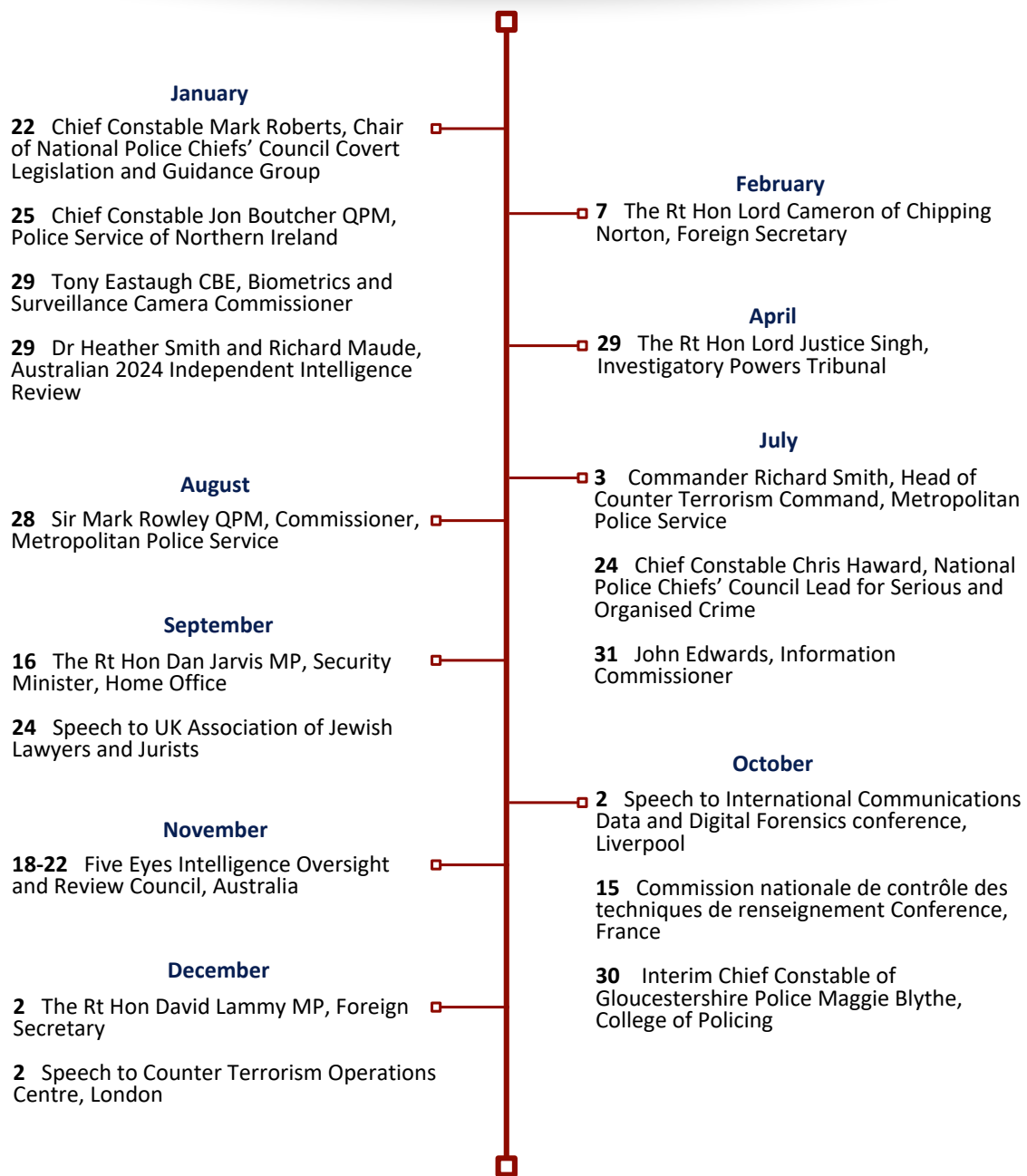
Communications and engagement

- 2.18 In 2024, we enhanced our external engagement strategy to increase transparency, build public trust and strengthen IPCO's reputation. This included a significant expansion of both domestic and international engagement, with the IPC participating in a wide range of meetings, conferences and delegation visits to discuss our work and the challenges we face. We also broadened our communications channels, using our website and social media to share key updates, inspection statistics and publications. From summer 2024, we expanded the circulation of our external quarterly newsletter to include non-governmental organisations (NGOs) and relevant media outlets.

Engagements

- 2.19 Throughout 2024, the IPC welcomed various opportunities to talk openly about our work, embracing transparency and scrutiny. Along with these engagements, the IPC has regular dialogue with those authorities whom he oversees.
- 2.20 The IPC also presented at events including the International Communications Data and Digital Forensics 2024 conference (ICDDF24), the UK Association of Jewish Lawyers and Jurists and to an audience across the counter-terrorism network at the Counter Terrorism Operations Centre (CTOC).
- 2.21 The IPC and his team continued to engage with NGOs throughout 2024 to help build a dialogue whereby topics of interest and issues of concern could be openly and honestly discussed. As part of this engagement, we held meetings with Reprieve, Liberty and Privacy International.
- 2.22 The following graphic illustrates the engagements undertaken by the IPC in 2024. In addition to the listed meetings, the IPC regularly meets with the authorities under his oversight.

Public Engagements



International engagement and strategy

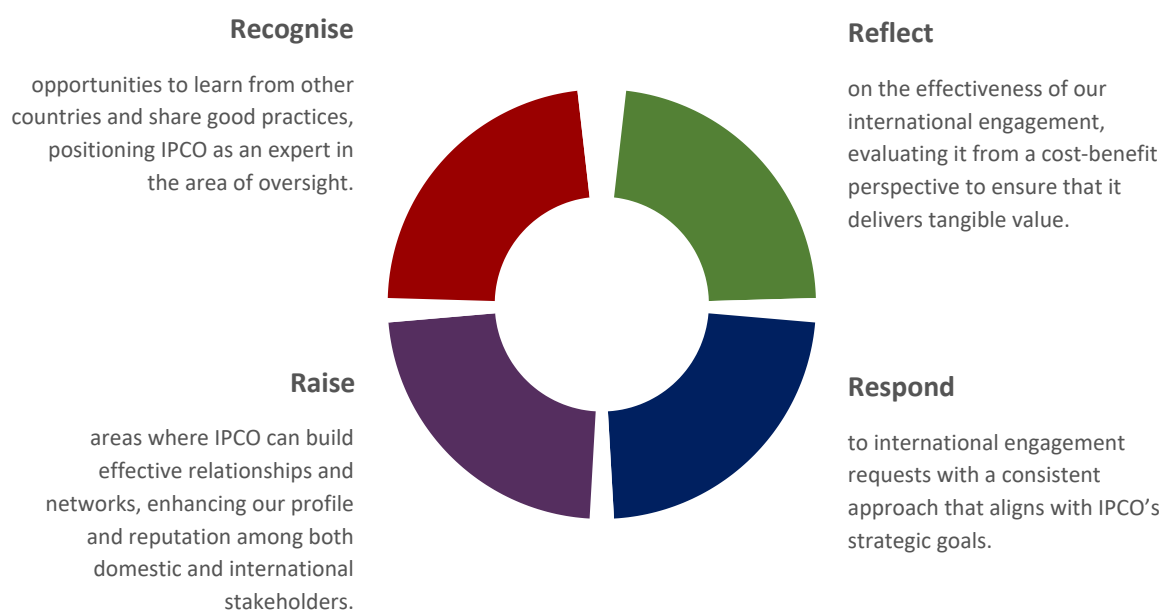
- 2.23 Over the last year, we have continued to strengthen our relationships and collaborative approach with international partners, with the objective of sharing expertise and information, fostering innovation and building partnerships that enable us to draw on the unique experiences and best practices of international bodies with similar remits.

Engagement activity in 2024

- 2.24 Our international engagement activities have developed over time, with a primary focus on bilateral meetings and multilateral conferences, roundtables and other events. We are an active participant in several international partnerships and forums and in 2024, we continued to engage with fellow oversight bodies, including at the Five Eyes Intelligence Oversight and Review Council (FIORC) meeting in Australia and the Intelligence Oversight Working Group (IOWG) meetings in Belgium and Sweden.
- 2.25 In addition, we also engaged in bilateral discussions on specific topics such as inspector training and thematic warrants and hosted international delegations on their visits to the UK. Following the FIORC 2024 conference, we have strengthened our engagement through multilateral networks, establishing new connections and collaborative opportunities.

Our international strategy

- 2.26 In 2024, we reflected on our international activities and established a strategy for our engagements moving forward.
- 2.27 The foundation of our international strategy is built on four core principles, referred to as the “four Rs”, which guide our decisions regarding international activities:



- 2.28 These principles ensure that our international engagements are aligned with our overall objectives and increase our capabilities. Our international engagement is central to our mission of promoting effective oversight, sharing expertise and learning from international counterparts. By adopting a strategic approach, guided by clear principles and priorities,

we ensure that our international activities are purposeful, impactful, aligned with our organisational goals, represent value for money and are affordable within our budget.

Public office holder and staff developments

Deployment of Judicial Commissioners

- 2.29 In April 2024, the IPC commissioned a review of the deployment of Judicial Commissioners, with an objective of ensuring the arrangements, which had been in place since IPCO was created in 2017, reflected current demands, were affordable within our budget and demonstrated value for money.
- 2.30 A working group, chaired by the Chief Executive and including four Judicial Commissioners, collated and analysed data, consulted colleagues on options and submitted recommendations to the IPC for a decision.
- 2.31 The IPC accepted the recommendation that a reduction in Judicial Commissioners to 13 (from 15), each with an annual commitment to IPCO of 80 days (reduced from 90), would provide a more efficient and affordable working model with no reduction in the service provided for authorisations.
- 2.32 In addition, the IPC accepted the recommendation to reorganise Judicial Commissioner oversight portfolios, enabling Judicial Commissioners to provide additional support to inspections and other areas of our business.
- 2.33 We implemented these changes in October 2024.

Staff training

- 2.34 IPCO's Learning and Development policy promotes continuous learning and offers diverse training options to reflect needs across different parts of the organisation.
- 2.35 Employees have access to essential tools, mandatory learning packages and a Personal Development Plan. Initiatives include core skills resources, "Lunch and Learn" sessions and a structured six-week induction programme for new starters in the Authorisations Team.
- 2.36 All operational staff, which includes those in authorisations and inspections, are expected to stay up to date with developments in CD techniques and legislation. Regular CD Practice Development Sessions (PDS) support this by enhancing decision-making and skills through real case studies and emerging issues.
- 2.37 We have also developed an in-house Management Development Programme (MDP), which provides leadership and management training for new line managers. This was extended to all grades in 2024, with positive feedback. The programme will continue in 2025 with ongoing improvements.

Review of the Annual Report structure

- 2.38 In 2024, the IPC commissioned a review on the structure, format and content of the IPCO Annual Report to ensure it delivers clarity and value. The review followed initial changes in the 2023 Annual Report where we amalgamated content on MI5, the Secret Intelligence Service (SIS), GCHQ and the Ministry of Defence (MoD) into one chapter. This

enabled issues common to these organisations to be reported together while still retaining individual comment where necessary.

2.39 We conducted the review through the following strands:

- research among the bodies we oversee including a survey for public authorities, NGOs and journalists to ascertain how the report is used, clarifying purpose and ascertaining readership;
- workshops with our staff to look at purpose, content and drafting processes;
- analysis of readership of our previous Annual Reports; and
- exploring other formats including a literature review of how other regulatory and oversight bodies (both domestically and internationally) present their findings.

2.40 Our conclusions from this review were that the historic approach of having chapters focusing on public authorities led to repetition with similar information shared in multiple chapters. This increased the length of the report and deterred readers. As a result, the IPC accepted the recommendation to change the format of the Annual Report to reframe the focus on key themes and issues from across the year. This approach has enabled us to highlight the most significant themes in our work, which we hope will help readers identify and understand these key issues without negatively impacting on our transparency objectives. We will monitor the feedback on this new format to inform our future approach.

3. Regulatory and legislative matters

Overview

- 3.1 This chapter sets out the main regulatory and legislative developments, along with any cases that have had a bearing on the work of the Investigatory Powers Commissioner (IPC) and the Investigatory Powers Commissioner's Office (IPCO) in 2024.

Thematic warrants

- 3.2 As set out in our 2023 Annual Report, we conducted a review of thematic warrants in 2023, as operated in practice by the UK intelligence community (UKIC) and law enforcement. This review resulted from concerns regarding inconsistencies arising from different interpretations of thematic warrant categories described in the Investigatory Powers Act 2016 (IPA). In 2024, we shared and discussed our findings with the Home Office and the operational community. We await further views from the Home Office and will provide an update in our 2025 Annual Report.

Implementation of the Investigatory Powers (Amendment) Act 2024

- 3.3 On 25 April 2024, the Investigatory Powers (Amendment) Act 2024 (IP(A)A) received Royal Assent, with most provisions coming into force on 14 October 2024.¹³ We set out the main changes relating to the IPC's oversight functions in our 2023 Annual Report.¹⁴ In this section, we outline further details regarding implications for our oversight functions.

Bulk personal datasets

- 3.4 The Act introduced two new subset regimes for bulk personal datasets (BPDs). Part 7A creates a new regime for BPDs in respect of which there is only a low or no reasonable expectation of privacy. Judicial Commissioners will be asked to approve both individual and category authorisations. Part 7B concerns intelligence service access to datasets held by third parties (rather than simply retained by them), which will be subject to the double lock.
- 3.5 Shortly before the commencement of the provisions, UKIC agencies asked us to review some draft applications for category authorisations under Part 7A (low/no) and we raised some concerns with the approach taken to defining the categories.

¹³ See: <https://www.legislation.gov.uk/ukxi/2024/1021/made>

¹⁴ Annual Report of the Investigatory Powers Commissioner 2023 (from paragraph 2.4). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf

- 3.6 Separately, we also discussed at some length whether the use to which the data will be put is a relevant consideration for assessing whether a dataset has a low or no expectation of privacy for the purposes of section 226A of the IPA. This is asserted at paragraphs 4.24 to 4.26 of the relevant draft Code of Practice published for the consultation.¹⁵ The Code asserts that this may be a relevant consideration to applying the test in section 226A(1) of the IPA, for example when “using data for capability development, such as building and testing machine learning models”. After careful consideration, we agree that the use to which the data will be put will be a relevant consideration, but this does not necessarily mean that the use of data for capability development and machine learning models is indicative of a low/no reasonable expectation of privacy. Depending upon the purpose of the capability or model, it might actually suggest the contrary. We will continue to keep this under review and should any category authorisation be submitted in this area it will need to satisfy a Judicial Commissioner that it has appropriate parameters.
- 3.7 Part 7B applications may need to accommodate a great deal of uncertainty as to the nature and extent of the datasets that are being accessed. As, by definition, UKIC does not hold the data, it is often limited as to its knowledge of the data held by a third party. The regime also poses an inherent difficulty when it comes to being able to audit access. In many cases this might be technically impossible or highly undesirable for operational security reasons (as acknowledged at paragraphs 5.6-5.9 of the draft Code of Practice) and UKIC understandably would not wish to leave a trail of their subjects of interest. Given the requirement for a Part 7B warrant will not be commenced until April 2025, we will report on this again in our next Annual Report.

Definition of communications data

- 3.8 As noted in previous Annual Reports, the ambiguity of the definition of communications data (CD) poses significant challenges both to public authorities and to IPCO as an oversight body. These concerns persist notwithstanding the modest changes introduced by the IP(A)A.
- 3.9 The amendments in relation to CD are twofold. Firstly, the offence in section 11 of the IPA of unlawfully obtaining CD was amended to make clear what may constitute “lawful authority” to obtain CD. The non-exhaustive list in section 11(3A) makes clear that the use by public authorities of non-CD-related powers, and voluntary disclosure by a telecommunications operator (TO), are lawful means of obtaining CD. The second change implemented by the IP(A)A is the exclusion of subscriber details from the “carve-out” for the content of communications in section 261(5).
- 3.10 These amendments address some of the operational challenges previously posed by the definition of CD. In particular, the clarity regarding alternative lawful means of obtaining CD is a welcome addition. However, further clarification of the CD definition is still required. The Home Office has made efforts to provide practical guidance in the draft Code of Practice, published for public consultation in late 2024. It nevertheless remains our view that further legislative change is likely to be necessary.
- 3.11 One example of the difficulties posed by the breadth of the current definition relates to electronic financial transaction data. This has been the subject of discussions between relevant stakeholders, including IPCO, the Home Office and the wider CD community. Such transactions would appear capable of generating CD in the form of events data within

15 See: https://assets.publishing.service.gov.uk/media/67ea6b40ba01abac8e9fe91f/E03319462_Draft_Part_7A_Code_Accessible.pdf

section 261 of the IPA. This has practical implications for the way financial information is obtained by public authorities, in particular LEAs. The complexity of these discussions and the ramifications of the application of Part 3 of the IPA to such information, have only served to highlight the pressing need for clarity in the definition of CD. As part of the consultation, we raised strong concerns with the Home Office that parts of Annex C of the draft CD Code of Practice did not reflect the correct legal analysis in respect of financial transaction data.¹⁶

Personal data breaches by telecommunications operators

- 3.12 The Act addressed a regulatory gap in relation to personal data breaches committed by TOs in respect of interception, equipment interference, CD and the bulk acquisition of CD. These data breaches must now be reported to us and, in relation to CD, they must be reported in parallel to the Information Commissioner's Office (ICO). Together with the ICO, we have put in place a process to enable the reporting and management of these breaches. The Act also enables a provision for the data subject to be notified where breaches are serious and it is in the public interest to do so, and to seek a remedy from the TO via the Investigatory Powers Tribunal (IPT).

Appointment of the Deputy Investigatory Powers Commissioner

- 3.13 The Act placed on a statutory footing the role of the Deputy Investigatory Powers Commissioner (DIPC) with the option for the IPC to appoint up to two Judicial Commissioners to the role.¹⁷ Sir John Goldring has carried out the role of DIPC on an informal basis since his appointment to IPCO in 2017 and the IPC formalised this appointment in November 2024.

IPCO's status under the Freedom of Information Act 2000

- 3.14 Section 29 of the Freedom of Information Act 2000 (FOIA) amended the list of security bodies in section 23 of FOIA to include IPCO. This provides an absolute exemption from the disclosure of material under FOIA provided directly or indirectly by both IPCO staff and the Judicial Commissioners or relating to IPCO. We advised public authorities of this change in January 2025. The IPC has been clear in his intention that this does not change his objective to be as transparent about his oversight as he can be without compromising operations or national security.

Future reform of the Investigatory Powers Act 2016

- 3.15 While the IP(A)A brought in necessary changes and new safeguards to reflect the changing threat and technological landscape, it was evident from the various reviews and reports that longer term reform of the IPA is needed. It is for the Home Office to decide how and when to take this forward, but we would urge that consideration is given to a broader codified approach to the legislation to enable clarity. At present, there is a complex patchwork of legislation that can be difficult to apply to real operational scenarios and difficult to oversee.

16 The new Communications Data Code of Practice came into force on 6 June 2025. See: <https://www.gov.uk/government/publications/communications-data-code-of-practice>

17 See: section 7, Investigatory Powers (Amendment) Act 2024 ([legislation.gov.uk](https://www.legislation.gov.uk))

- 3.16 There are also several issues where we had identified regulatory gaps which were not addressed in the IP(A)A. These should be considered by the Home Office in any future reform and include:
- Non-statutory oversight of GCHQ's receipt of confidential or privileged information: GCHQ receives intelligence reports from its foreign partners around the world, including the Five-Eyes. Some of these reports may contain confidential or legally privileged information which would have required GCHQ to notify or seek approval from a Judicial Commissioner if the same information had been obtained under a warrant issued to it under the IPA. Oversight of the receipt and retention of such information currently falls outside the IPC's remit. Notwithstanding this, GCHQ has voluntarily been treating such information no differently to product obtained under its own warrants and referring such information to a Judicial Commissioner. The IPC has asked the Government to address this potential regulatory gap and place the existing practice on a statutory footing.
 - Reporting of UKIC personal data breaches: section 108(1) requires UKIC to notify the ICO of a serious personal data breach.¹⁸ However, UKIC is relieved of this obligation "if the breach also constitutes a relevant error within the meaning given by section 231(9) of the Investigatory Powers Act 2016" (see section 108(6) of the IPA). It is unclear what the rationale is for UKIC avoiding the notification requirement to the ICO, given that we have no functions in relation to data protection compliance and cannot exercise the enforcement powers in Part 6 of the Data Protection Act 2018 (DPA). At present, this means that UKIC could commit a serious personal data breach which might not come to the attention of the competent supervisory authority for data protection unless we refer the matter. Given the possible sensitivities involved, we are not best placed to do this. This may leave a gap which could be contrary to the public interest.

IPA Codes of Practice

- 3.17 On 14 October 2024, the Home Office issued a consultation on the IPA Codes of Practice, including five existing Codes and three new Codes (Part 7A, Part 7B and the notices regime) following changes to the IPA.¹⁹
- 3.18 The Home Office encouraged public authorities to have regard to the new Codes from the date of commencement of the 2024 Act, even though the revised and new Codes would not come into force until later in 2025. Ministers informed Parliament of this decision through a written ministerial statement made on 14 October 2024.²⁰
- 3.19 The IPC raised concerns with the Home Office about encouraging public authorities to have regard to the draft Codes of Practice prior to the conclusion of the consultation and completion of the affirmative resolution procedure and the IPC set out his interpretation of how the new codes should apply in relation to the old codes and changes to the law. Nevertheless, he recognised that the Home Office had strong operational reasons for taking this approach and that this was a matter for the Government.

18 'Personal Data Breach' here means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (see s.84(4) DPA 2018).

19 See: <https://www.gov.uk/government/consultations/investigatory-powers-amendment-act-2024-codes-of-practice-and-notices-regulations>

20 See: <https://questions-statements.parliament.uk/written-statements/detail/2024-10-14/hcws124>

- 3.20 In relation to changes to the Codes of Practice, we are grateful for the engagement with the Home Office in discussing our proposed amendments and addressing our concerns.

Consultation on changes to Schedule 4 to the IPA

- 3.21 In October 2024, the Home Office consulted the IPC in accordance with section 72(2) (a) of the IPA on expanding the list of public authorities who can acquire CD as set out in Schedule 4 to the IPA.²¹
- 3.22 The IPC did not raise any concerns about the proposed additions or removals to Schedule 4. However, he was interested in the measures that each prospective public authority was putting in place to ensure their preparedness to exercise CD acquisition powers compliantly. He noted that business plans indicated that designated officers would have access to legal support and was reassured by the consideration given to policy, governance, training and operational processes, which are crucial to the effective and lawful acquisition of CD.

Operational purposes

- 3.23 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 received in 2024 included operational purposes that met the statutory test.
- 3.24 The IPA requires the Prime Minister to review the list of operational purposes annually, which occurred in September 2024.
- 3.25 As trailed in our 2023 Annual Report, we have been in discussions with the Government as to whether the list of operational purposes, in the context of bulk interception, could be of greater specificity. These discussions have progressed to include an exploration of the feasibility of modifying an operational purpose (the outcome of which is likely to have some bearing on the debate regarding their specificity). There has never been an application to modify an operational purpose and although the majority of operational purposes are likely to be static and long term, this may indicate that the specificity of the list is too high level in respect of some operational purpose descriptions, but equally it might reflect the need for UKIC to be able to respond to emerging crises quickly. We will explore the feasibility of modification as part of next year's bulk interception inspection and we plan to conclude our investigation into this issue in 2025. We will set out our conclusions in the next Annual Report.

Raising concerns with IPCO

- 3.26 In our 2019 Annual Report, we set out the process for making a disclosure to IPCO as enabled by the information gateway in section 237 of the IPA. This provides a mechanism for anyone, including current and former employees of the public authorities which we oversee, to raise with us any serious concerns they have. This process is published on our website.²²

21 These regulations came into force on 8 July 2025. See: The Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers) Regulations 2025

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

- 3.27 In 2024, we received three new disclosures of information. The first related to a government department and following investigation, the IPC concluded the allegations were not substantiated. In the second, which related to an executive agency, we were not provided with sufficient information to commence an investigation and the case was closed. The third case related to a disclosure about HMPPS. This is still under investigation and we will report on the outcome in our 2025 Annual Report.

4. Oversight activities and challenges

Summary

- 4.1 This chapter presents the Investigatory Powers Commissioner's Office (IPCO) oversight findings and emerging challenges across multiple investigatory powers during the 2024 reporting year. They have been identified from our inspections and authorisations work.
- 4.2 Below is an overview of Chapter 4, along with a guide on how to navigate the chapter:

How to navigate this chapter



To help readers access relevant content quickly, the chapter has been structured as follows:

Our Inspections

- 4.4 UK intelligence community (UKIC)
- 4.6 Law enforcement agencies (LEAs)
- 4.7 Wider public authorities (WPAs) and local authorities
- 4.10 Prison services

Regulation of Investigatory Powers Act 2000 (RIPA)

- 4.12 Covert human intelligence sources
- 4.34 Directed surveillance
- 4.38 Intrusive surveillance

Investigatory Powers Act 2016 (IPA)

- 4.43 Targeted interception (TI), targeted equipment interference (TEI) and property interference
- 4.47 Interception in the Scottish Prison Service (SPS)
- 4.52 Interception in the Northern Ireland Prison Service (NIPS)
- 4.55 Communications data (CD): LEAs, public authorities and prisons
- 4.66 Notices
- 4.72 Records and Product Management (RPM)

Intelligence Services Act 1994 (ISA)

- 4.80 Access to Foreign, Commonwealth and Development Office (FCDO) assessments

UK-US Data Access Agreement

- 4.83 Overview
- 4.90 Crime (Overseas Production Orders) Act 2019 (COPO)

The Principles

- 4.94 Key Findings
- 4.96 Review of The Principles

Our inspections

4.3 Detailed below is a summary of the most significant compliance matters identified during our inspections in 2024. These issues are considered sufficiently material to warrant inclusion in this Annual Report. Following this summary, each area is set out in greater detail to provide further context and insight into our inspection findings.

UK intelligence community (UKIC) and warrant granting departments (WGDs)

- 4.4 During 2024, we continued to inspect each of the UK intelligence agencies (MI5, the Secret Intelligence Service (SIS), Government Communications Headquarters (GCHQ)), the Ministry of Defence (MoD) and warrant granting departments (WGDs) across the full range of their covert investigatory powers. The inspection programme is subject to adjustment each year as the use of powers and compliance levels change or as new legislative developments occur. This can mean that Inspectors will review the use of some powers more than once a year.
- 4.5 Each agency has bespoke systems and processes that have been designed to aid compliance and facilitate operational requirements, with nominated personnel who interact with us on a regular basis to facilitate key parts of warrant processes and oversight functions. All dedicate significant effort towards developing and maintaining a strong culture of compliance.

Law enforcement agencies (LEAs)

- 4.6 LEAs remained a major focus of our inspection programme. We reviewed their use of a wide range of investigatory powers, including:
- targeted interception (TI): we raised concerns about the outdated IT systems used to manage intercept material and the lack of a coherent replacement plan;
 - communications data (CD): we identified misuse of Priority 2 gradings, which placed strain on our resources and risked undermining the prioritisation system.²³ We worked with LEAs and the National Police Chiefs’ Council (NPCC) to address this issue; and
 - Records and Product Management (RPM): Our inspections revealed inconsistent practices across forces, with deficiencies in governance, training and data protection compliance.



23 The priority levels for CD requests are determined by the requesting authority and reflect the relative urgency of the application. IPCO handles applications classed as Priorities 2, 3 and 4. The response times set out below are our service level expectations:

- Priority 1 (urgent) applications: dealt with by the authorities themselves
- Priority 2: applications are to be processed within six hours
- Priority 3: applications are to be processed within 24 hours (by the end of the next working day)
- Priority 4: applications are to be processed by the end of the 6th working day

Joint assessments with the Information Commissioner's Office (ICO) highlighted areas for improvement.

Wider public authorities and local authorities

- 4.7 Local authorities in the UK have access to a limited set of investigatory powers, specifically the use of covert human intelligence sources (CHIS), directed surveillance and the acquisition of CD. These powers are used sparingly. Since 2023, we have operated a risk-based inspection model, requiring written assessments of compliance to determine whether remote or in-person inspections are necessary.
- 4.8 Wider public authorities (WPAs), which include various organisations beyond local authorities, also hold statutory powers to use covert tactics. The scope of these powers varies depending on the organisation's functions, with many authorised to conduct directed surveillance and acquire CD, while only a few can use more intrusive methods like property interference and intrusive surveillance. The frequency and nature of inspections for WPAs are determined by the extent of their powers, how often they are used, and past performance. Inspections assess legal compliance, internal policy adherence, and the adequacy of staff training.
- 4.9 In 2024, we carried out 84 inspections of local authorities and 59 inspections of WPAs. On the whole, we identified good levels of compliance and did not identify any issues of non-compliance or concern that warrant reporting on in this Annual Report.

Prison services

- 4.10 In 2024, we undertook inspections of 39 prisons in England and Wales, thematic inspections across 11 Scottish prisons and inspections of all three prisons in Northern Ireland. These inspections assessed compliance with the IPA, Regulation of Investigatory Powers Act 2000 (RIPA) and Prison Rules regarding the interception of communications and use of surveillance.

Regulation of Investigatory Powers Act 2000

- 4.11 RIPA governs the use of CHIS by public authorities. We monitor compliance with RIPA to ensure the use of these powers remains necessary, proportionate and legally compliant.

Covert human intelligence sources (CHIS)

Counter Terrorism Policing (CTP) source management arrangements

- 4.12 In response to the findings of the Manchester Arena Inquiry, MI5 and Counter Terrorism Policing (CTP) committed to working together to align more closely their management of CHIS who provide information about terrorism. This work will lead to changes in how CHIS records are retained and accessed by MI5 and CTP officers and is likely to affect how we conduct our inspections of their activity.
- 4.13 We have engaged with MI5 and CTP to explore the best method of continued access to all relevant CHIS-related records (as defined by legislation). We will take a flexible approach to our inspections, ensuring that our oversight is maintained during and after this period of change, while upholding our independence and robust methodology.

Juvenile CHIS

- 4.14 In 2024, four juvenile CHIS were authorised by LEAs, a figure broadly consistent with previous years (two in 2023 and four in 2022).
- 4.15 Each of the 2024 authorisations was subject to individual inspection, with reports produced for all four. One of the CHIS had been previously authorised in 2023 and was renewed during the reporting period.
- 4.16 Juvenile CHIS authorisations remain rare and are granted only in exceptional circumstances. In most cases, the intelligence obtained relates to serious youth violence and would not be accessible through adult CHIS.
- 4.17 LEAs continue to manage juvenile CHIS cases with care and diligence. The issues identified during inspections were generally minor and focused on refinement. Development points included:
- ensuring that any decision made to meet the juvenile CHIS without an appropriate adult present had a well-documented rationale made by the Senior Authorising Officer (SAO);
 - ensuring that the SAO was making decisions regarding the management of juvenile CHIS and these decisions were not being delegated to lower ranking officers;
 - Criminal Conduct Authorisations (CCAs) could not cover activities by the parents of the CHIS and could relate only to the juvenile CHIS themselves; and
 - the consideration of 'cost effectiveness' is not an appropriate factor when considering the use or conduct of a juvenile CHIS. This is particularly important given the heightened vulnerability of juvenile sources. Decisions must be based solely on necessity, proportionality and the protection of the individual, rather than considering any perceived operational or financial efficiency.
- 4.18 We remain satisfied with the high levels of compliance and care demonstrated by public authorities in these cases. In all inspections, enhanced welfare considerations and risk assessments were evident, reflecting the vulnerable status of juvenile CHIS. No authorisations were found to be inappropriate or unnecessary.

Criminal Conduct Authorisations (CCAs)

- 4.19 Section 29B of RIPA enables a relevant source or CHIS to participate in criminal conduct in specific circumstances, namely in the interests of national security; for the purpose of preventing or detecting crime or of preventing disorder; or in the interests of the economic well-being of the UK.
- 4.20 Criminal conduct is authorised separately from the section 29 use and conduct authorisation. Occasionally a description of the criminal conduct authorised by the CCA was included within the section 29 authorisation commentary for relevant source and CHIS. These instances have significantly reduced since 2021, but in 2024 we continued to find examples during inspection.
- 4.21 Given the serious criminality investigated utilising relevant source (undercover operative) activity, it is almost inevitable that operatives undertake criminal conduct to ingratiate themselves with those they are investigating, and to enhance and maintain their covert role.

- 4.22 Overall, the quality and content of relevant source CCAs was found to be of a good standard. However, on occasions we noted that CCAs lacked specificity with only a general descriptor of the criminality to be undertaken documented, rather than detail required by paragraph 6.22 of the CHIS Code of Practice which states “the authorisation should have clear parameters set out for the CHIS to ensure they are clear about the criminal conduct in which they are authorised to participate”.
- 4.23 Most LEAs utilising CHIS authorise criminal conduct in relation to declaration of financial reward while in receipt of certain state benefits, to protect them from being identified as a CHIS. We have observed that processes have matured and staff involved are well versed in its application. On inspections, we have identified some instances where there has been a lack of evidence of reissuing permissions and limitations with the CHIS at renewal of an authorisation. While a thematic approach is permissible for this specific type of criminal conduct, LEAs should guard against treating the authorisations as an administrative process only.
- 4.24 Other use of CCAs continues to relate primarily to the acquisition of prohibited items, notably firearms, stolen property and illegal drugs. In most cases these were well described, authorised and managed. A small number of errors were reported or found on inspection relating to a failure to notify us within defined timescales and use of vague or ambiguous wording for conduct.

Thematic inspection of relevant source activity

- 4.25 In late 2023, the IPC commissioned a thematic review of the arrangements in place for the authorisation and management of relevant source (undercover operative) activity across the UK.
- 4.26 During 2024, we inspected every undercover unit, which included a visit by an Inspector to interview staff, complete a bespoke questionnaire and to inspect a selection of operations.
- 4.27 The inspections focused on the standard of authorisations and associated documentation, such as risk assessments, the identification of common compliance matters, existing processes, management structures, quality assurance processes and oversight practices.
- 4.28 This was the first thematic inspection of the relevant source tactic, albeit regular inspections of this tactic are carried out during our annual inspections and through the nine-month inspection process prior to the renewal of operatives' authorisations.
- 4.29 The findings from the inspection process have been collated and a standalone report was shared with the Chair of the National Undercover Working Group (NUWG) in 2025.
- 4.30 Overall, our report identified good levels of compliance for the authorisation and management of the relevant source tactic, often within high-risk scenarios. The report highlighted good practice and 17 recommendations which have been fully endorsed by Chief Constable Trevor Rodenhurst the NUWG lead.
- 4.31 Those involved in the management and authorisation of relevant source operatives were found to be professional in approach, enthusiastic and keen to achieve high standards of compliance while delivering lawfully audacious and progressive operational activity.
- 4.32 Several key observations were identified, in addition to some more common compliance matters.

- 4.33 Our observations will be shared with the relevant source community along with an action plan to address issues raised.

Directed surveillance

- 4.34 The following case study was selected to illustrate the use of directed surveillance in the context of counter-corruption investigations within the prison estate.
- 4.35 An authorisation for directed surveillance was granted at the enhanced level, as required by legislation and outlined in Annex A of the 2018 Covert Surveillance and Property Interference Code of Practice. The deployment formed part of an investigation into an inappropriate relationship between an employee of His Majesty's Prison and Probation Service (HMPPS) and a prisoner.
- 4.36 The application, which involved the deployment of covert audio and video equipment, clearly explained the likelihood of acquiring confidential material and included a mitigation plan. The equipment was not monitored live but recorded during specific time periods when the subjects were likely to be present, with confirmation supported by permanent CCTV.
- 4.37 The authorisation was granted by the HMPPS Director General. While the acquisition and handling of confidential information were appropriately managed and the application and authorisation were of a high standard, we raised some best practice points for future consideration.

Intrusive surveillance

- 4.38 This case study was selected to illustrate significant shortcomings in the preparation and presentation of an intrusive surveillance authorisation. The documentation lacked the clarity, specificity and rigour required under the Code of Practice.
- 4.39 In 2024, His Majesty's Prison and Probation Service (HMPPS) obtained an intrusive surveillance authorisation. There was some uncertainty as to whether an authorisation was required, given that it did not appear to involve the acquisition of private information. However, the application lacked sufficient detail to justify this position. It did not clearly describe the intended conduct or the equipment involved. Nor was the location of the equipment identified. While an oral briefing was reportedly provided to the Secretary of State, paragraph 6.5 of the Code of Practice requires such information to be clearly set out in the written application and supporting documents.
- 4.40 The application also failed to address the potential for technical malfunction or human error. No provisions were made for accidental activation or misuse of the equipment, an omission of concern given the risk of collateral intrusion.
- 4.41 Although the broad language used may have been intended to preserve flexibility, greater specificity is required for what amounts to a quasi-thematic authorisation. The general benefits were outlined, but the application lacked sufficient detail to demonstrate necessity and proportionality.

Investigatory Powers Act 2016

- 4.42 The Investigatory Powers Act 2016 (IPA) provides a comprehensive framework for the use of investigatory powers by law enforcement and intelligence agencies. It consolidates and updates previous legislation, establishing safeguards and oversight mechanisms for the use of interception, equipment interference, CD acquisition and bulk powers. We oversee the use of these powers to ensure they are used lawfully, proportionately and in accordance with the safeguards set out in the Act.

Targeted interception (TI)

IT system for the management of intercept material

- 4.43 We have consistently raised concerns about the ageing IT system used by LEAs to manage interception warrants and material, including the dissemination of intercept product. This system, managed by the Home Office, has long been due for replacement. Although a new system was initially planned for launch in 2020, delays and a subsequent project reset in 2021 pushed the target to 2025/26. The revised system offered reduced functionality, placing the burden on LEAs to develop enhancements. Throughout this period, we urged the Home Office to prioritise the delivery of a compliant replacement.
- 4.44 In July 2024, the Home Office informed us that it would no longer deliver a central replacement system. Instead, LEAs would be responsible for developing their own solutions, with the existing system maintained in the interim. The IPC wrote to the programme's Senior Responsible Owner expressing disappointment at the lack of progress and concern over the decision to close this part of the programme. While we accept that multiple systems may be viable, each must be fully compliant with the IPA. We have asked the Home Office to keep the IPC regularly informed of developments.
- 4.45 While the existing system is currently stable, and being supported by the Home Office, reliance on this system in the absence of new ones being delivered does remain a significant concern. During our 2024 inspection of the Home Office, the IPC reiterated these concerns in the subsequent report. Our Chief Executive continues to attend the Programme Board as an observer, monitoring progress and raising issues as necessary.
- 4.46 We recognise the complexity of developing new systems while maintaining operational continuity. However, the absence of a coherent and comprehensive plan to ensure all LEAs have sustainable, IPA-compliant systems in place before the current system is decommissioned is unacceptable. We continue to urge the Home Office to treat this matter as a priority.

Interception in the Scottish Prison Service (SPS)

- 4.47 Between March and August 2024, we conducted a thematic inspection of 11 prisons across Scotland to assess compliance with section 49 of the IPA, which permits the lawful interception of communications in prisons only when exercised under powers conferred by or under Prison Rules.
- 4.48 Our inspection included interviews with security managers, analysts, researchers and key staff responsible for call monitoring and mail handling, alongside a review of relevant records.

- 4.49 We found inconsistent operational practices and varying levels of compliance with the directions issued under Prison Rules. In many cases, staff operated without clear guidance, creating a vulnerability whereby the SPS could not demonstrate that interception activity was both necessary and proportionate. The IPC's subsequent report emphasised the need for SPS to ensure consistent application of its expectations across the prison estate and to consider revising guidance, or recommending amendments to the relevant directions where necessary, to ensure compliance with the IPA.
- 4.50 The IPC issued 12 points for action by SPS including:
- a requirement to ensure that prisons employed a standardised process for informing prisoners of monitoring arrangements;
 - a requirement to review current phone call monitoring processes, which encompassed the recording and evidencing of justification, formal approval, reviews, and cancellation;
 - a requirement to ensure procedures were in place to avoid the inadvertent monitoring of exempted calls;
 - a requirement to review the wording on its public-facing website to make clear that general correspondence could and may be intercepted and monitored in accordance with legislation (noting that standard announcements are heard by both parties to a telephone call before any recording takes place); and
 - a requirement to review existing procedures for monitoring general correspondence.
- 4.51 Progress against these points for action will be monitored during 2025.

Interception in the Northern Ireland Prison Service (NIPS)

- 4.52 During the summer of 2024, we conducted inspections of the three prisons in Northern Ireland: HMP Maghaberry, HMP Magilligan and HMP Hydebank Wood, supplemented by a visit to the Prison Service Headquarters at Stormont.
- 4.53 Overall, the inspections identified NIPS had a good understanding of the requirements of the rules governing the interception of communications and activity conducted under RIPA. The three prisons were fully discharging their legal obligations to inform prisoners that their communications are subject to interception.
- 4.54 We found a good level of knowledge among prison staff in relation to their obligations under the IPA and RIPA, good levels of accountability and strong support from senior managers. We identified one area of non-compliance which was the absence of an overarching policy for data retention and records management.

Communications data (CD)

Paragraph 1.5 of the CD Code of Practice

- 4.55 At the 2023 inspection of MI5's use of CD, we found that it had entered into arrangements with companies that would be telecommunications operators (TO) in respect of at least some areas of their business. These arrangements were unremarkable as it is unlikely to be a surprise that UKIC will seek information from any source that might enable it to fulfil its intelligence requirements. The issue here, however, is whether MI5 and the GCHQ arrangements, to the extent this invited the voluntary disclosure of CD, breached the 2018 CD Code of Practice.

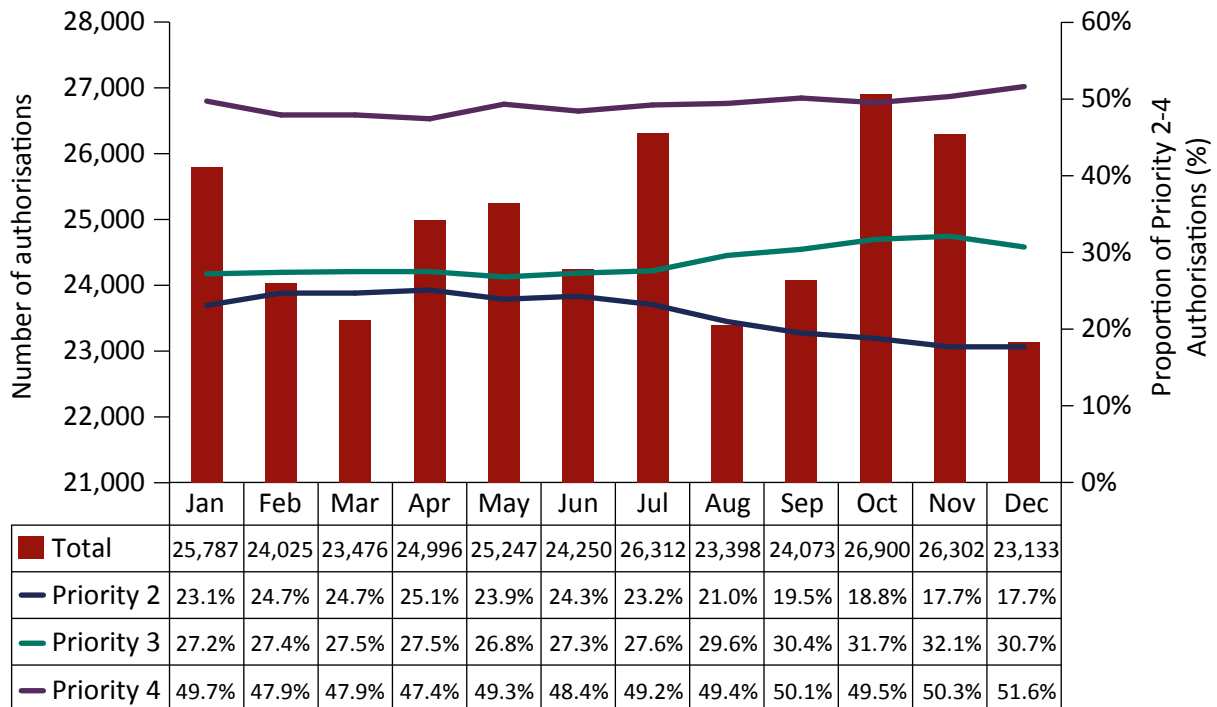
- 4.56 Paragraph 1.5 of the 2018 CD Code of Practice states: "Relevant public authorities should also not require, or invite, any postal or TO to disclose CD by relying on any exemption to restrictions on disclosing personal data under relevant data protection legislation."
- 4.57 Paragraph 1.5 of the 2018 Code of Practice is also mentioned at paragraph 15.11 which states:
- "....it is not an offence to obtain CD where it is made publicly or commercially available by the TO or postal operator or otherwise where the TO or postal operator freely consents to its disclosure. In such circumstances the consent of the operator provides the lawful authority for the obtaining of the data. However, as set out in paragraphs 1.3-1.5, relevant public authorities should not require, or invite, any postal operator or TO to disclose CD by relying on any exemption to restrictions on disclosing personal data under relevant data protection legislation."
- 4.58 This paragraph is important as it seems to confirm that voluntary disclosure of CD has always been "lawful authority" for the purposes of section 11 of the IPA – a fact now placed beyond all doubt by new section 11(3A)(c) of the IPA. Accordingly, the voluntary provision of CD in response to a request from UKIC is a regulatory and not a criminal liability issue.
- 4.59 As trailed in our 2023 Annual Report, we identified concerns MI5 had been applying a different interpretation to us of paragraph 1.5 and may have therefore acquired CD in contravention of that paragraph. In subsequent discussions, it emerged GCHQ shared MI5's interpretation. We undertook to set out our view once MI5 had provided us with its considered analysis which it did in May 2024.
- 4.60 The crux of the issue was the meaning of paragraph 1.5 of the 2018 Code. MI5 and GCHQ argued that the voluntary disclosure of CD in response to a request from UKIC did not require the TO to rely on any exemptions under relevant data protection legislation. In particular, it was argued that the transparency requirement in Article 5(1)(e) UK General Data Protection Regulation (GDPR) was satisfied solely by the existence of the UKIC statutory information gateways and duties set out in sections 19-21 of the Counter-Terrorism Act 2008, section 2(2)(a) of the Security Service Act 1989 and (for GCHQ's purposes) section 4(2)(a) of the Intelligence Services Act 1994 (ISA).
- 4.61 The IPC disagreed with this submission and held that it was wholly unrealistic for MI5 and GCHQ to suggest that transparent processing is achieved based on a data subject i) having knowledge of complex legislation; and ii) having a 'reasonable expectation' that data would be provided in circumstances where the provision of data is entirely voluntary. Legislation can rarely be characterised as constituting plain language that a data subject would understand and this was not such a case. Moreover, just because a data controller, such as a TO, has discretion to provide data to UKIC lawfully under UKIC's information gateway, does not mean that data subjects would necessarily expect their confidential data *will be* disclosed to the state in the absence of a legal obligation. A possibility provided for in legislation cannot be equated with a reasonable expectation.
- 4.62 Accordingly, the IPC concluded MI5 and GCHQ had made a relevant error by not having had regard to paragraph 1.5 of the 2018 Code when making requests for, or entering into, information sharing arrangements with companies that operated, at least in part, as a TO. Notwithstanding this conclusion, the IPC recognised the force in UKIC's arguments as to why any strict adherence to paragraph 1.5 of the Code would be unworkable given the broad definition of TO and the impossible task of knowing (especially in advance of a request) whether any data requested might have been acquired by a TO as CD. It is for this

reason that the Government has proposed that paragraph 1.5 of the Code be removed in the next version and this is a matter for Parliament to consider.²⁴

Priority 2 CD applications

- 4.63 During this reporting period, we identified a concerning increase in the number of CD applications graded as Priority 2—the highest level considered by our Authorisations Team. This grading, which requires applications to be processed within six working hours, is intended for urgent operational needs.
- 4.64 The proportion of Priority 2 applications more than doubled between 2019 and April 2024, when it reached 25%. This placed significant strain on our resources and delayed the processing of routine applications. Inspections revealed that some public authorities were misusing the grading system, in some cases breaching the CD Code of Practice.
- 4.65 We worked with public authorities and the NPCC to address this issue. By November 2024, the proportion of Priority 2 applications had declined to 18%. While this was a positive development, the matter remains under close scrutiny and will continue to be a focus of our oversight.

24 This has been removed from the new Communications Data Code of Practice which came into force on 6 June 2025. See: <https://www.gov.uk/government/publications/communications-data-code-of-practice>

Table 4.1: Monthly authorisation volumes and proportional breakdown by priority (2–4), January to December 2024**Notes:**

¹ This chart reflects only those authorisations dealt with by IPCO via the Case Management System (CMS) and does not represent the total number of authorisations dealt with by IPCO received through other systems.

² Applications for CD are graded by the applicant based on priority level, which corresponds to a Service Level Expectation (SLE) set by the IPC:

- a. Priority 2: applications are to be processed within six hours.
- b. Priority 3: applications are to be processed within 24 hours (by the end of the next working day).
- c. Priority 4: applications are to be processed by the end of the 6th working day.

Notices**National Security Notices**

- 4.66 Section 229(3)(b) of the IPA requires the IPC to keep under review the giving and operation of National Security Notices (NSNs) issued under section 252 of the IPA. NSNs are issued to TOs and require them to take such specified steps as the Secretary of State considers necessary in the interests of national security. Judicial Commissioners must also review and approve the decision to issue any notice.
- 4.67 While we are unable to confirm nor deny whether any NSNs have been issued, we are satisfied that UKIC and the Home Office have the appropriate policies and practices in place to operate any such notices to ensure they would serve a clear purpose, would be necessary in the interests of national security and would not result directly in any privacy intrusion.
- 4.68 The Investigatory Powers (Amendment) Act 2024 introduced a new requirement at section 20(6) for NSNs and Technical Capability Notices (TCNs) to be renewed at the end of a two-

year relevant period. All extant notices will therefore go through a renewal process within two years of the new Act coming into force. This is a welcome change that will enhance our oversight of these notices, particularly where the details remain fairly static and would not otherwise come to our attention.

Technical Capability Notices

- 4.69 On 7 April 2025, the Investigatory Powers Tribunal (IPT) handed down a procedural decision confirming a claim by Apple against the Home Secretary in relation to the Secretary of State's powers to make TCNs under the IPA 2016.²⁵ Under section 253, TOs and postal operators may be required to maintain the technical capability that ensures they can comply when subsequently served with lawful warrants for interception, equipment interference, or data acquisition. Such a notice can only be issued if the Secretary of State deems it necessary and proportionate, and this decision is independently reviewed and approved by a Judicial Commissioner.
- 4.70 We welcome the decision of the Tribunal to order that the bare facts of the case be disclosed to the public as we consider it is vitally important for there to be a mature and informed public debate about lawful access capabilities. It is not helpful to that debate for a lawful access capability to be referred to crudely (and erroneously) as a 'backdoor'; it must be emphasised that a TCN cannot result in the provision of any data to a public authority without the acquisition of that data being subject to separate authorisation under the IPA, overseen by IPCO. It is important that the public debate is not presented simply as privacy on the one hand, and a government free-for-all on the other. This cannot be farther from the truth; lawful access can be achieved in a way that strikes a balance between maintaining strong encryption and ensuring law enforcement and the Government can protect the public from terrorism, serious crime and hostile state activity.
- 4.71 Given the litigation is ongoing, we will not discuss the matter further in this Annual Report beyond wishing to correct the record as to the way in which the privacy debate has been presented in certain media reports.

Records and Product Management (RPM)

Law enforcement

- 4.72 Safeguarding material acquired through covert investigatory powers remains a core focus of our oversight of LEAs. Over the past six years, progress towards full compliance with RPM standards has been inconsistent across police forces. In some cases, this has been due to a lack of prioritisation or delays in upgrading covert IT systems. Despite efforts by the NPCC to standardise practices, forces continue to operate with varying policies and retention schedules.
- 4.73 Between August and October 2024, we conducted joint assessments with the ICO. These provided an opportunity to review our inspection approach, identify shared concerns and agree a joint reporting mechanism for areas of non-compliance.

25 *Apple Inc v Secretary of State for the Home Department* [2025] UKIPTrib 1

- 4.74 The findings of these joint assessments were consistent with our general inspection findings identified throughout recent years and supported a pattern of common trends:
- a lack of governance structure for information management and an absence of internal audit mechanisms to assess compliance with data protection obligations specific to the handling of covert material;
 - failure to include data protection officers in the decision-making process for the retention and review of covert material;
 - deficiencies in policies and procedures;
 - a lack of training and awareness;
 - an absence of data protection impact assessments;
 - organisations that have engaged senior records management specialists and accepted accountability for RPM at senior levels have achieved greater levels of compliance; and
 - despite other weaknesses, information security is well managed with robust measures in place to keep covert material secure and protected from unauthorised access or disclosure.
- 4.75 In response to these findings, the scope of our inspections has been expanded in 2025/26 to ensure compliance with legal and regulatory obligations. The IPC has made clear that Chief Officers should be prepared to demonstrate adherence to data protection and GDPR principles, including the use of data protection impact assessments, records of processing activity, information risk management and relevant data sharing agreements.

UKIC

- 4.76 The IPA imposes requirements on UKIC to ensure that it has satisfactory arrangements in place to protect and minimise intrusion from the material it obtains from the exercise of investigatory powers. These arrangements include data retention limits, handling restrictions, sharing requirements, system monitoring, security measures and training.
- 4.77 In 2023, we requested that MI5 and GCHQ review their internal allocation and audit of removable media with a focus on devices used to retain, handle, transfer or analyse IPA or RIPA data. The term removable media relates to such items as USB sticks, tablets or laptop computers. Both agencies were unable to locate a considerable number of devices that potentially held material with security classifications ranging from OFFICIAL-SENSITIVE to TOP SECRET, albeit most items unaccounted for were encrypted or required a PIN to access. We assessed that the losses were due to a previous lack of robust audit systems managing the issuing and return of removable media.
- 4.78 Mitigations to prevent recurrence have included a refresh of the procedures used to manage the acquisition and issuing of removable media, including maintaining a record of why they are required for use by individual personnel and a tracking system to ensure that all issued items are registered and returned at the end of their use. We are keeping this matter under review.

Intelligence Services Act 1994

- 4.79 The ISA provides the statutory framework for the functions of the UK's intelligence services. It includes provisions for authorising activities such as property interference and activity

overseas that would otherwise be unlawful. We oversee these authorisations and this includes examining the government legal advice underpinning them under a limited waiver.

Access to Foreign, Commonwealth and Development Office (FCDO) assessments

- 4.80 In our 2023 Annual Report, we referred to documents we had become aware of during the November 2023 inspection of the Foreign, Commonwealth and Development Office (FCDO). These were documents that were explicitly referenced in the applications for certain section 7 ISA authorisations. Our request, following the inspection, to view these documents was refused. This matter was escalated by FCDO officials to the (then) Foreign Secretary who, on 3 July 2024, refused the request on the ground that he considered the documents fell outside our remit. Instead, the FCDO suggested that sharing the summary of the conclusions reached by the Foreign Secretary, as had been done previously, “struck the right balance”.
- 4.81 This was the first time the IPC had been refused access to a document by any public authority and the IPC took this extremely seriously to avoid a disturbing precedent being set. The IPC personally reviewed the matter and concluded that the then Foreign Secretary had erred in his analysis of relevance and remit. Accordingly, the IPC invited the new Foreign Secretary to review his predecessor’s decision with the benefit of the IPC’s considered analysis and receipt of a formal request under the IPC’s powers to compel disclosure of documents. This resulted in the provision of the documents to us in September 2024 and formed part of constructive discussions at the FCDO inspection in November 2024. Other documents of a similar type were provided promptly upon request.
- 4.82 This episode involved a departure from the highly transparent manner in which the FCDO normally engages with IPCO and we are confident lessons have been learned. It should serve as a reminder to all public authorities of the importance of absolute transparency in maintaining public trust and confidence when it comes to the oversight of covert powers: it is for IPCO to determine the relevance of documents and we will pursue any instance of non-disclosure using all means available to us.

UK-US Data Access Agreement

- 4.83 We inspected each of the UK authorities who request data under the UK-US Data Access Agreement (DAA) as part of our broader 2024 programme of interception inspections. These inspections consisted of looking at the controls and governance in place, and then reviewing the associated records, systems and policies. Overall, we observed high levels of compliance with, and understanding of, the DAA from staff working at the intercepting agencies.
- 4.84 During 2023 and 2024, we discussed with the Home Office and MI5 the issue of proportionality of specific factors (e.g., an email address or account identifier) where data was requested from US under the DAA. This issue had arisen as a result of significant variance in the volume and type of stored data provided by US TOs when compared with the foreseeability of intrusion under ordinary interception – i.e., the potential for up to six months ‘forward facing’ data collection.
- 4.85 An additional challenge also arose because the proportionality considerations for individual factors can vary quite significantly between different TOs. For instance, some TOs may only hold metadata or user information and contact lists, but not content of messages, while others, may hold and return large amounts of content going back several years.

- 4.86 The proportionality considerations for approvers can therefore be very different, depending on the TO or the factor an agency is seeking to intercept as this will need to justify not simply the data sought, but the data likely to be returned when it comes to the proportionality of the request.
- 4.87 We wrote to MI5 to set out our concerns that insufficient consideration was being given to the proportionality of targeting factors that would invoke the DAA. In response, MI5 proposed making changes to require investigators to provide the parameters of requests for historic, stored data in internal tasking systems and suggested that we could examine these during inspections, since the requirement under the DAA is for the Judicial Commissioner to consider the necessity and proportionality of the targeting decision, that is, the individual being targeted, rather than the specific factor targeted.
- 4.88 We did not agree with this analysis and considered that MI5 was conflating the principles of necessity with proportionality, but we decided to render the debate as to the interpretation of the DAA academic. Pursuant to section 235(2) and (3) of the IPA, we required MI5 (and all other public authorities) to provide the time period for any historic, stored data requests for a relevant targeting decision as part of the information provided for any additional review (see IPCO Advisory Notice 1/2023 for an explanation of the additional review process).²⁶ This enables Judicial Commissioners to be fully satisfied as to the proportionality of any relevant targeting decision at the point targeting begins.
- 4.89 Following this requirement, MI5 took steps to implement the changes towards the end of 2024, including updated language for its warrant handbook. Furthermore, we wrote to other public authorities to inform them of fulfilling this requirement.

Crime (Overseas Production Orders) Act 2019

- 4.90 As part of our oversight of the UK's use of the DAA, we oversee where the Crime (Overseas Production Orders) Act 2019 (COPO) is being used. COPO orders must be approved by a Circuit Judge.
- 4.91 There are three Requesting Agencies (RA) that have obtained data under the agreement in 2024 utilising COPO, the National Crime Agency (NCA), the Metropolitan Police Service (MPS) and MPS-Counter Terrorism Command (SO15).
- 4.92 Our oversight responsibilities include:
- keeping under review the compliance by public authorities with the terms of the DAA;
 - conducting periodic audits of the activity being undertaken with RAs to ensure the correct application of procedures including the identification, recording and reporting of breaches of the DAA; and
 - reviewing records, internal guidance, training, governance and targeting procedures.
- 4.93 In 2024, our inspections identified good standards of compliance, with robust management procedures. The cases we reviewed were relatively low in number as this is a developing capability. We expect the number of COPO orders granted to rise during 2025/26 and our inspections will increase commensurately.

²⁶ 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

The Principles

- 4.94 This is the fifth year that we have overseen “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 effect on 1 January 2020.
- 4.95 The Principles is a publicly available Cabinet Office policy that applies to MI5, SIS, GCHQ, the MoD, the NCA and SO15, referred to collectively as the Principles Partners.

Key findings

- 4.96 Overall, we observed a high level of compliance with both the letter and the spirit of The Principles by all Principles Partners. Their application of The Principles is now at a high level of maturity. Each Principles Partner provides its personnel with relevant training, produces written guidance and has a central compliance team of specialists with in-depth knowledge.
- 4.97 The cross Principles Partners Team has also matured and shares best practice, builds knowledge, collates allegations of unacceptable conduct and helps strengthen risk assessments. We appreciate that Principles Partners have resourcing constraints but continue to encourage each Partner to resource adequately the Principles Partner Team to help provide consistency, especially since Partners report to different Ministers.
- 4.98 The Principles are often applied to complex cases in high-risk environments where limited information is known. This requires careful judgement, good processes and accurate written records. In the vast majority of cases, we observed that these were demonstrated to a high standard. However, with a focus on ever better compliance we noted a small number of areas where improvements could have been made.
- 4.99 During 2024, we identified that some agencies including SO15, the MoD and GCHQ may benefit from restructuring their assessment forms, which are used to record considerations when The Principles are engaged and a risk assessment is therefore required. They should be altered to state explicitly which action or actions trigger engagement of the Principles, whether any potential action taken by the agency would be causative or non-causative to the risk of the detainee being subjected to unacceptable conduct, and whether there was knowledge or belief, a real risk, or a lower than real risk of each form of unacceptable conduct. Categories of unacceptable conduct include unlawful killing, torture, extraordinary rendition, cruel, inhuman and degrading treatment (CIDT), rendition or unacceptable standards of arrest and detention.
- 4.100 We considered that restructuring the assessment forms would give personnel greater clarity when applying The Principles based on our oversight of two previous cases. On one occasion, the MoD incorrectly completed a risk assessment for the foreign authority it was engaging with and not the foreign authority that was holding the detainee. In a further case, SO15 did not correctly distinguish between its Principles risk assessment and the risk assessments under the Overseas Security and Justice Assistance (OSJA), leading to a recommendation that the form that should be used for each process should be more clearly defined.
- 4.101 In 2024, the Principles Partners informed us about four cases where The Principles had not been correctly applied; three by MI5 and one by SO15. We marked all four cases as a minor incident of non-compliance and judged that there was either a lower than real risk a detainee had been subjected to unacceptable conduct or a low risk that receipt of intelligence could be perceived as encouraging or condoning unacceptable conduct.

Review of The Principles

- 4.102 The Principles policy states that The Principles should be reviewed by the Cabinet Office every five years. In 2024, the Cabinet Office began scoping this review and, in accordance with the policy, sought the views of the IPC. The IPC considered this an important opportunity to reflect on how The Principles were operating and to make some amendments, including those which would enable clarification and provide increased transparency on the workings of the policy. The IPC has also advocated for the involvement of non-government organisations (NGOs) in the review given the perspective they would bring.
- 4.103 We understand the Cabinet Office intends to report on its review findings in 2025 and we will provide an update in our 2025 Annual Report.

5. Errors and breaches

Overview

- 5.1 Investigating errors and breaches by the public authorities we oversee is an important part of our work. The impact of errors on the rights of individuals can be grave. Accordingly, public authorities are expected to have thorough procedures in place to comply with the legislation and Codes of Practice to mitigate the risk of errors occurring.
- 5.2 We find that public authorities take errors and breaches seriously and there is a strong culture of reliable self-reporting, with public authorities informing us of the majority of errors themselves. This doctrine of self-reporting also suggests that quality assurance and oversight arrangements are sufficiently robust in most authorities to prevent errors becoming systemic.
- 5.3 We also discover potential errors during our inspections, which are then investigated by the authority concerned and formally reported to us. 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. Our website includes details about the types of error we investigate.

Summary

- 5.4 In 2024, there was an increase in the number of errors (333) reported by the UK intelligence community (UKIC) from the 222 reported in 2023, none of which indicated any systemic failures (see from paragraph 5.8). There was also an increase in the number of errors reported by the law enforcement interception agencies, largely resulting from an increase in errors reported by the National Crime Agency (NCA) (see from paragraph 5.15).
- 5.5 In respect to law enforcement agencies (LEAs), wider public authorities (WPAs), local authorities and prisons, there was a decrease in the number of surveillance, property interference and covert human intelligence source (CHIS) errors (see from paragraph 5.19) and an increase in communications data (CD) errors (see from paragraph 5.30).
- 5.6 At the end of 2023 and during 2024, we investigated two incidents reported by the Ministry of Housing, Communities and Local Government (MHCLG) relating to the use of CHIS via external contractors. Although the intelligence was not used operationally and did not meet the threshold for a serious error, the Investigatory Powers Commissioner (IPC) found MHCLG lacked the necessary Regulation of Investigatory Powers Act 2000 (RIPA) policies and procedures, which has now been addressed (see from paragraph 5.24).

- 5.7 Section 231(1) of the Investigatory Powers Act 2016 (IPA) requires the IPC to inform a person of any relevant error if considered serious, i.e., that it has caused them significant harm or prejudice and is in the public interest to inform them. A relevant error is defined as an error made by a public authority rather than a telecommunications operator (TO). In 2024, we did not find any errors that met this definition across any of the powers that we oversee.

UK intelligence community (UKIC) errors

- 5.8 UKIC continues to maintain a strong culture of recording, investigating and reporting IPA errors. In 2024, none of the errors we looked at indicated a systemic failure of safeguards or an attempt to act unlawfully or circumvent IPA safeguards.
- 5.9 Other errors reported to us include those that sit outside of the IPA, such as cases where 'The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees' had not been correctly applied and breaches under the UK-US Data Access Agreement (DAA). We have an agreement with the relevant agencies that they record and report any breach relating to these matters in the same manner as an IPA error. Each report is recorded and managed as an IPA error. Table 5.1 includes this additional information as well as IPA errors.
- 5.10 The 2024 statistics highlight an increase in the total number of errors reported by MI5 and the Government Communications Headquarters (GCHQ). MI5 had a sharp increase in bulk personal dataset (BPD) errors. This resulted from MI5 implementing strengthened processes to audit the justifications recorded by staff to examine BPDs with most of those errors arising from typographical mistakes made by staff when recording details of a person of interest or their communication identifiers. The slight increase in CHIS-related errors resulted from minor misunderstandings when authorising covert activity within complex cases. GCHQ recorded an increase in bulk interception errors; again, these stemmed from improved staff reporting and internal reviews that increased the volume of reports, but on review did not indicate increased intrusion or the over-retention of data.

Table 5.1: UK intelligence community (UKIC) errors, 2024

	Agency			Total
	MI5	SIS	GCHQ	
Bulk personal datasets (BPD)	113	6	1	120
Bulk interception and bulk equipment interference ¹	0	0	75	75
Interception	23	3	8	34
IPA Safeguards	5	0	16	21
Bulk communications data (BCD) ²	13	0	5	18
Covert human intelligence sources (CHIS)	15	2	0	17
Data Access Agreement (DAA)	5	0	9	14
Directed surveillance (DSA)	12	0	1	13
Communications data (reportable) (CD)	9	1	0	10
Targeted equipment interference (TEI)	4	2	1	7
Property interference and intrusive surveillance (PI/IS)	4	0	0	4
Section 7 Intelligence Services Act 1994 (s7 ISA)	0	0	0	0
The Principles	0	0	0	0
Total	203	14	116	333

Notes (applicable to tables 5.1-5.4 and figure 5.1):

¹ Bulk interception and bulk equipment interference errors were previously reported under interception and equipment interference figures respectively.

² Bulk communications data errors were previously reported under communications data errors.

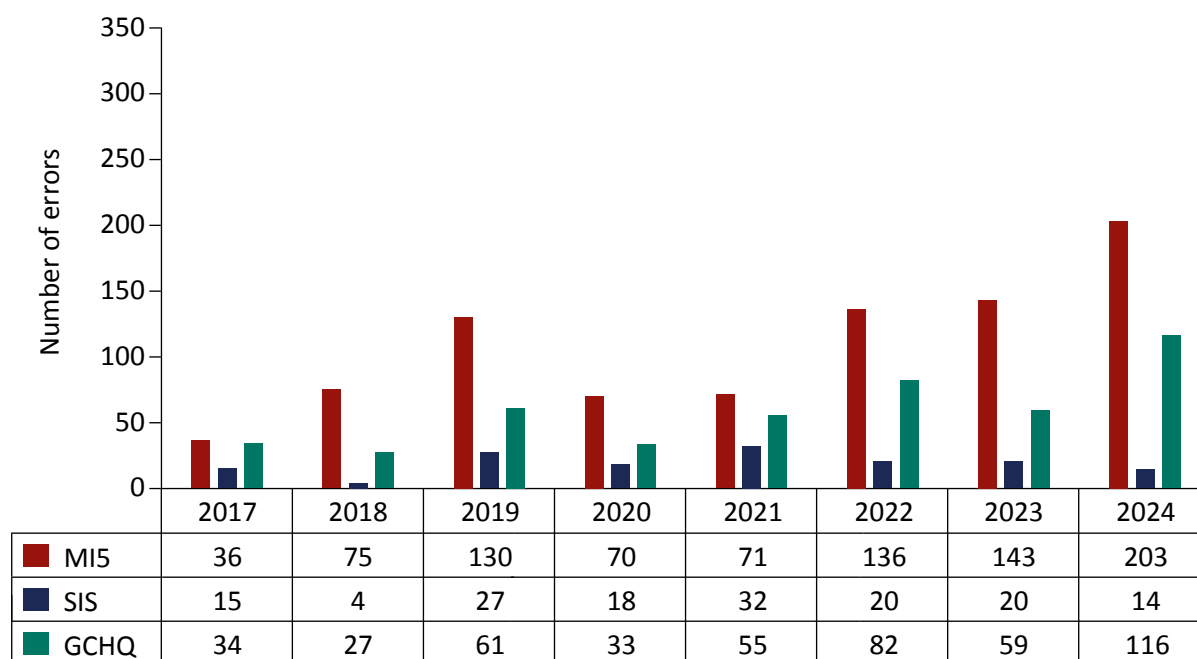
Figure 5.1: UKIC errors, 2017 to 2024

Table 5.2: MI5 errors, 2017 to 2024

	2017	2018	2019	2020	2021	2022	2023	2024
Covert human intelligence sources	4	3	5	3	0	9	6	15
Directed surveillance	11	8	13	7	4	23	18	12
Property interference & intrusive surveillance	7	4	6	1	6	10	4	4
Bulk personal datasets	3	1	14	11	11	20	43	113
Interception	11	22	23	25	30	47	22	23
Equipment interference	0	0	1	2	1	6	11	4
Bulk interception & bulk equipment interference	-	-	-	-	-	-	0	0
CD (reportable)	0	37	55	14	19	20	9	9
Bulk CD	-	-	-	-	-	-	18	13
Systems	0	0	13	7	0	-	-	-
IPA Safeguards	-	-	-	-	-	-	1	5
The Principles	-	-	-	0	0	1	0	0
DAA breaches	-	-	-	-	-	-	11	5
Total	36	75	130	70	71	136	143	203

Notes (applicable to tables 5.2-5.4):

¹ Cells marked with “-” under The Principles, IPA Safeguards and DAA Breaches indicate that these categories were introduced in the respective year and data collection began from that year onward.

² Cells marked with “-” under Systems reflect a methodological change. From 2023, systems-related errors have been reclassified and are now reported under other relevant categories.

Table 5.3: Secret Intelligence Service (SIS) errors, 2017 to 2024

	2017	2018	2019	2020	2021	2022	2023	2024
Covert human intelligence sources	10	3	9	1	6	4	0	2
Directed surveillance	1	0	0	1	1	0	5	0
Bulk personal datasets	1	0	10	6	18	13	0	6
Interception	3	1	4	8	3	0	4	3
Equipment interference	0	0	3	0	0	1	0	2
Bulk interception & bulk equipment interference	-	-	-	-	-	-	0	0
CD (reportable)	0	0	1	1	0	1	1	1
Bulk CD	-	-	-	-	-	-	0	0
Systems	0	0	0	0	1	-	-	-
IPA Safeguards	-	-	-	-	-	-	0	0
Section 7 ISA	0	0	0	1	1	0	9	0
The Principles	-	-	-	0	2	1	1	0
DAA breaches	-	-	-	-	-	-	0	0
Total	15	4	27	18	32	20	20	14

Table 5.4: Government Communications Headquarters (GCHQ) errors, 2017 to 2024

	2017	2018	2019	2020	2021	2022	2023	2024
Covert human intelligence sources	0	0	0	0	0	1	0	0
Directed surveillance	0	0	3	0	0	0	0	1
Property interference & intrusive surveillance	0	1	1	0	0	0	1	0
Bulk personal datasets	0	0	1	3	0	0	0	1
Interception	32	15	51	13	30	71	7	8
Equipment interference	0	0	3	3	8	5	2	1
Bulk interception & bulk equipment interference	-	-	-	-	-	-	38	75
CD (reportable)	0	11	1	1	7	4	1	0
Bulk CD	-	-	-	-	-	-	-	5
Systems	0	0	0	13	9	1	-	-
IPA Safeguards	-	-	-	-	-	-	6	16
Section 7 ISA	2	0	1	0	0	0	0	0
DAA breaches	-	-	-	-	-	-	4	9
The Principles	-	-	-	0	1	0	0	0
Total	34	27	61	33	55	82	59	116

5.11 We received one error from the Ministry of Defence (MoD) in relation to directed surveillance.

Errors relating to the decommissioning of covert cameras at MI5

- 5.12 Following the identification of an error relating to the failure to remove access to a covert surveillance camera when a related directed surveillance authorisation had ceased to have effect, MI5 undertook a proactive review of its internal processes. This was to ensure robust camera access management practices remained in place to ensure compliance with paragraph 5.24 of the Covert Surveillance and Property Interference Code of Practice (2018).
- 5.13 The review identified 10 additional cases where covert cameras continued to capture still-images beyond the period of authorisation or where the associated directed surveillance authorisation had not been cancelled as soon as reasonably practicable. MI5 reported the further errors to us detailing each case where over-retention had occurred and the period of time the cameras were active beyond authorisation. In all cases such material was placed in locations where general access is denied and marked for erasure.

Warrant granting departments

- 5.14 In 2024, we received one error from the Home Office which related to targeted interception (TI). In this case a request was correctly approved, but a technical system fault resulted in the submission being incorrectly recorded.

Interception agencies

- 5.15 From late 2023, and throughout 2024, we noted that the number of relevant errors relating to the handling of material originating from TI reported by the NCA increased significantly. These related to cases managed directly by the NCA, some Metropolitan Police Service (MPS) cases and National Police Chiefs' Council (NPCC) police force investigations where the TI capability is facilitated via the NCA.
- 5.16 We identified multiple factors contributing to this increase, including training issues and failure to follow guidance. In addition, the NCA had conducted some proactive investigations that had resulted in the identification of historic as well as current problems relating to the handling of intelligence when it was passed to the relevant NPCC sensitive intelligence unit for further dissemination to operational teams.
- 5.17 While work to address the cause of these problems is ongoing, by the end of 2024 the rate of reported errors showed no signs of decreasing. This is a matter of substantial concern to the IPC who has raised it with the Director General of the NCA. We will continue to conduct inspections to examine in depth the NCA's implementation of its IPA data handling arrangements, training and mitigations.

Table 5.5: Interception agencies errors, 2021 to 2024

	NCA	MPS	Police Scotland	PSNI	HMRC
2021	16	6	Not known	Not known	1
2022	10	3	0	1	5
2023	18	0	3	2	14
2024	47	1	2	2	4

- 5.18 In addition to the figures above, there were six DAA breaches reported to us: one from the MPS and five from the NCA.

Law enforcement agencies, prisons, wider public authorities and local authorities: surveillance, property interference and covert human intelligence sources (CHIS)

- 5.19 The number of errors reported in 2024 remained low in proportion to the overall volume of compliant authorisations. A total of 82 errors were recorded, representing a significant decrease from 2023. None met the threshold of a serious error causing significant prejudice or harm to the individual concerned.

Table 5.6: Total surveillance, property interference, CHIS and equipment interference errors for LEAs, wider public authorities, local authorities and prisons, 2021 to 2024

	Number of errors			
	2021	2022	2023	2024
Directed surveillance	53	30	49	43
Property interference	15	15	24	19
Intrusive surveillance	0	0	3	4
Covert human intelligence sources (including relevant sources)	12	15	43	14
Targeted equipment interference	0	5	12	2
Total	80	65	131	82

- 5.20 Over half of the reported errors related to directed surveillance. This is likely due to the high volume of directed surveillance authorisations compared to other powers such as CHIS, property interference and intrusive surveillance. These more intrusive powers are used less frequently and typically by a smaller number of experienced public authorities, which may contribute to lower error rates.
- 5.21 As in previous years, most surveillance errors stemmed from human error, for example, commencing surveillance before authorisation took effect, continuing activity after cancellation, or exceeding the authorised scope. Our inspections assess how such unauthorised material is handled and, unless required for legal proceedings or another statutory purpose, public authorities are expected to destroy it.
- 5.22 CHIS-related errors were primarily due to “status drift,” the failure to recognise and authorise a source once their behaviour met the statutory definition of a CHIS. We also identified a small number of cases where CHIS exceeded the scope of their authorisation and engaged in unauthorised criminal activity. The 2022 CHIS Code of Practice requires public authorities to have clear policies in place to manage such situations.
- 5.23 We remain alert to the impact of personnel changes, particularly among Central Authority Bureaux (CAB) Managers and Authorising Officers, which can increase the risk of errors or reduce compliance standards. It is essential that new or inexperienced officers are supported in their roles and encouraged to engage with regional and national counterparts to share best practice. For organisations that use these powers infrequently, such as local authorities, regular professional development on compliance with RIPA remains vital.

Ministry of Housing, Communities and Local Government (MHCLG)

- 5.24 In October 2023, MHCLG reported two errors involving the unauthorised use of CHIS by its Recovery Strategy Unit (RSU), which was investigating non-compliance with building safety responsibilities – specifically the remediation of unsafe cladding.
- 5.25 The activity giving rise to the first error took place in October and November 2022. The second took place in April and May 2023. Concerns as to RIPA compliance were first raised internally in July 2023, MHCLG undertook internal inquiries and sought legal advice which culminated in the report to us in late October 2023.
- 5.26 In the two cases reported to us as errors, the external contractors were tasked by the Department to use human intelligence sources. This was achieved using one or more intermediaries: individuals with a network of 'sub-sources' with knowledge of the relevant field; in this case, the residential leasehold industry. The contractors instructed these intermediaries to gather the information sought by MHCLG. Only the contractors (i.e., the companies which MHCLG engaged) knew that their client was a Government department. Neither the intermediaries nor their sub-sources were aware of this. The intermediaries used a false cover story to explain why they were seeking the information. In the first error, seven sub-sources were spoken to and, in the second, 10.
- 5.27 MHCLG took the view, with which we agreed, that this amounted to establishing or maintaining a relationship for a covert purpose within the definition of a CHIS in section 26(8) of RIPA. Accordingly, we investigated the errors, interviewing individuals who had worked in the relevant team at the relevant time. It was apparent that MHCLG held very little information as to what activity had been carried out or the product obtained from the sub-sources, having received only a sanitised summary of key points of interest. We therefore also met with representatives of the two relevant external contractors, who were able to provide further information together with their own records of the activity which took place.
- 5.28 While a substantial amount of background information was gathered, none of it was used operationally. The IPC determined that the errors did not meet the threshold for serious error notification.
- 5.29 At the time, MHCLG had no policies or procedures in place to ensure RIPA compliance. Since then, it has ceased all intelligence gathering beyond open source research and has begun developing appropriate RIPA and non-RIPA policies. We note that MHCLG brought this issue to our attention swiftly and engaged with our investigation in a transparent and cooperative manner. Our 2025 follow-up inspection confirmed that MHCLG has made substantial progress towards implementing all recommended actions resulting from our review.
- 5.30 This matter was further complicated by MHCLG's absence from the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (the 2010 Order); Schedule 1 to which specifies the official(s) empowered to grant RIPA authorisations within a public authority. No such officials have ever been specified for MHCLG, despite it being named in Part 1 of Schedule 1 to RIPA as an authority able to authorise directed surveillance and CHIS activity. This means that, unless the 2010 Order is amended, MHCLG is unable to conduct covert activity under a RIPA authorisation. These errors have therefore highlighted one of several discrepancies between Schedule 1 and the 2010 Order, which result in a lack of clarity as to whether and how a public authority can exercise its RIPA functions. The IPC expects the Home Office to rectify this.

Law enforcement agencies, prisons, wider public authorities and local authorities: communications data (CD) errors

- 5.31 Errors are categorised under the 2018 Communications Data Code of Practice as 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. Proposed revisions to the Code for 2025 will set out a single category of relevant error that will require notification to the IPC where CD has been acquired. The breakdown of errors for 2024 is shown in table 5.7.

Table 5.7: Reportable communications data errors, 2018 to 2024

Cause	Number of errors						2024
	2018	2019	2020	2021	2022	2023	
LEAs	758	755	741	899	835	1,195	1,361
Telecommunications operators	127	230	253	332	184	346	360
Postal	0	0	0	6	0	0	0
Other public authorities	13	14	10	15	13	10	2
Workflow	5	12	1	7	0	0	7
Total	903	1,011	1,005	1,259	1,032	1,551	1,730

- 5.32 Although we saw an increase in the number of reportable errors, this is just a small percentage (0.50%) of the total of number of CD authorisations.²⁷ A further breakdown of types of CD errors is provided in table 5.8.
- 5.33 It remains the case that most errors are the result of human failing 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.

Table 5.8: Breakdown of communications data errors by type and responsibility, 2024

	Applicant	SPoC	TO/PO
Incorrect identifier	405	226	95
Time/date	56	349	65
Excess/no data	0	0	194
Other (incl. system error)	10	23	6
No IPA authority	87	207	0
Total	558	805	360

- 5.34 We continue to encourage public authorities to record mistakes found within initial applications before they are formally sent for authorisation. This is not a requirement of the Code of Practice but can help to find failings or vulnerabilities in procedures before they develop into recordable errors or systemic issues.

²⁷ In 2024, 345,567 CD authorisations were made.

- 5.35 In 2024, TOs reported 39 errors directly to us. The remainder of TO errors (321) were brought to our attention via public authorities. Though prejudice and harm can befall affected persons directly linked to a mistake by a TO, the IPC can make a serious error determination only if the relevant error is made by a public authority and is therefore a relevant error within the meaning of the IPA (see section 231(9) of the IPA).
- 5.36 We work closely with the Information Commissioner's Office (ICO) and supply summaries of all TO errors to the ICO within a prescribed period so that enforcement action can be taken if appropriate.
- 5.37 Although the number of reportable errors has risen, it is reassuring that only nine relevant reportable errors were assessed as being potentially serious.
- 5.38 The Investigatory Powers (Amendment) Act 2024 (IP(A)A) added some clarity to the types of data now defined as CD. This followed advice published by the Home Office in 2023 which addressed the increased use of online activity in banking, streaming, connected vehicles and deliveries.²⁸ In the past this data would have been obtained using data protection powers. During the transition we saw the failure to apply this guidance contributing to a rise in the number of errors recorded.
- 5.39 Resolving the use of an internet protocol address to a property or an individual is still the biggest risk of a serious error occurring. To reduce that risk, the Home Office and relevant partners developed the Error Reduction Strategy (ERS) in 2017. At its heart the ERS requires a series of "safety checks" known as "peer reviews" that, when applied diligently, can significantly reduce or eliminate the risk of a serious error occurring.
- 5.40 For the very first time, the ERS in its entirety will feature in the 2025 revised CD Code of Practice. Its publication will provide insight into the processes developed to prevent serious errors.

Serious error investigations: CD

- 5.41 In relation to CD, the circumstances which we would investigate as potentially serious include:
- 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;
 - errors that result in the wrongful disclosure of a large volume of CD or a particularly sensitive dataset; and
 - where CD has been acquired in the absence of an authorisation.
- 5.42 The 2018 Code of Practice requires errors to be sent to IPCO within five working days. Each report will be assessed for the potential of the error being defined as serious under the categories above.
- 5.43 In 2024, we conducted nine investigations into potentially serious errors in relation to CD. Details of these are set out in Annex C.
- 5.44 We did not consider any of these errors to be serious enough to write to any of the affected persons. These cases involved police seeking to prevent death, harm or injury to people in crisis where, as a result of an administrative mistake, officers attended the wrong address.

28 See: from paragraph 3.8.

Although this was unfortunate, the IPC considered the people at the wrong address had not suffered significant prejudice or harm.

Telecommunications operator breach

- 5.45 Early in 2024, we became aware through reporting mechanisms in place with public authorities that anomalies had been identified within records being disclosed by a TO in response to authorisations granted under the IPA to acquire CD.
- 5.46 While the impact on individual authorisations appeared minor in nature, the scale of these anomalies caused us concern. All police forces and most LEAs were impacted to some degree.
- 5.47 Although the exact cause of these anomalies took some time to establish, it was quickly identified they were the result of the record retrieval process within the TO and not a fault on the part of the public authority seeking to acquire the data.
- 5.48 As this issue resulted from failures in systems used by the TO, and not mistakes made by public authorities in failing to comply with a requirement of the Act or its Code of Practice, the circumstances did not meet the definition threshold of a relevant error. As such, our involvement was limited.
- 5.49 We worked closely with the Home Office who took a leading role to manage the response to the situation. Our involvement comprised investigating sufficiently to reassure the IPC that no person had suffered prejudice or harm as a result of these system failures. In addition, we approved a revised process to submit requests to the TO that was quickly established to remove the risk of inaccurate disclosures while the system faults were rectified.

6. Litigation in 2024

Overview

- 6.1 This chapter sets out the main legal developments and cases that have had a bearing on the work of the Investigatory Powers Commissioner (IPC) and Investigatory Powers Commissioner's Office (IPCO) in 2024.

Operation VENETIC

- 6.2 Operational VENETIC was the National Crime Agency's (NCA) operation to penetrate the encrypted EncroChat communications platform. In 2020, the NCA applied for a targeted equipment interference (TEI) warrant for this purpose. There has subsequently been 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.
- 6.3 We reported on *SF and Ors v. National Crime Agency* [2023] UKTrib 329 in our 2023 Annual Report. Since then, on 20 September 2024, in *Palmer v. National Crime Agency* [2024] EWCA Civ 1095,²⁹ the Court of Appeal (CoA) refused permission to appeal against that decision. The CoA stated that the purpose of the Investigatory Powers Act 2016 (IPA) was to protect privacy and ensure that those who apply for, issue and approve warrants were governed by coherent and comprehensible rules which would enable them to ensure that any criminal liability, unlawful acts, exposure to civil liability, or penalties were not incurred.
- 6.4 The issues on appeal were whether:
- section 9 of the IPA required the NCA to obtain a targeted interception (TI) warrant;
 - the Investigatory Powers Tribunal (IPT) had wrongly held that it lacked jurisdiction to consider whether the NCA had breached section 10 of the IPA by not having a mutual assistance warrant;
 - the operation was a "single investigation" for the purposes of section 101(1)(c) of the IPA; and
 - the IPT had erred in holding that EncroChat was used exclusively for criminal purposes.
- 6.5 The CoA decided that the IPT had been entitled to decide that section 9 should be restricted to prohibiting requests to overseas authorities to intercept communications sent to, or by, an individual who was believed to be in the UK. Section 9 should be read as only applying to a request to a foreign state to intercept communications where that interception would need a TI warrant if carried out in the UK. The CoA rejected the contention that section 9 also applied to the interception of stored communications.

29 See: <https://www.bailii.org/ew/cases/EWCA/Civ/2024/1095.html>

- 6.6 The CoA also decided that section 10 applied to requests for help from foreign authorities and was not limited to requests concerning individuals believed to be in the UK. A request to which section 10 applied could not be made by a person in the UK to an overseas authority unless a mutual assistance warrant had been issued. There was no error of law in the IPT's approach. It is a recurring theme of the IPA that the relevant authorities had to apply for the warrant which would make their proposed activity lawful, but also that they had carefully to consider, in relation to interception and related matters, whether any warrant might be necessary and, if so, which one.
- 6.7 The CoA also decided that the IPT was entitled to accept the evidence that the NCA had made a contemporaneous assessment that EncroChat was used almost exclusively for criminal purposes and there was no evidence to suggest otherwise. The CoA also held that the IPT had not erred in law in concluding that the operation was a "single operation or investigation". It was significant not only that the operation related to EncroChat, but also that its limits were coterminous with the activities of the French authorities.
- 6.8 The CoA concluded that none of the proposed grounds of appeal raised an arguable point of law and would not raise an important point in principle or practice, which is a prerequisite for a right of appeal from the IPT on a point of law.

Litigation against IPCO: *R (Horsfall) v. Investigatory Powers Commissioner* (2024)

- 6.9 On 21 November 2023, Mr Horsfall made a data subject access request to the IPC. The request was for information about whether any errors had been reported to IPCO about disclosure to Merseyside Police by His Majesty's Prison and Probation Service (HMPPS) or the Ministry of Justice (MoJ) in relation to calls between Mr Horsfall and his legal representatives. We provided a neither confirm nor deny (NCND) response. Mr Horsfall subsequently made a complaint to the Information Commissioner's Office (ICO) and sought permission to bring a claim for judicial review against the IPC.
- 6.10 Permission to bring the claim was refused without a hearing on the 25 October 2024. Mr Horsfall renewed his claim at a hearing on the 25 November 2024. Permission to bring the claim was refused as he did not demonstrate that our use of an NCND response was irrational or unlawful in the circumstances.
- 6.11 On 20 November 2024, the ICO determined that the IPC had complied with his data protection obligations.

7. Protecting confidential or privileged information

Overview

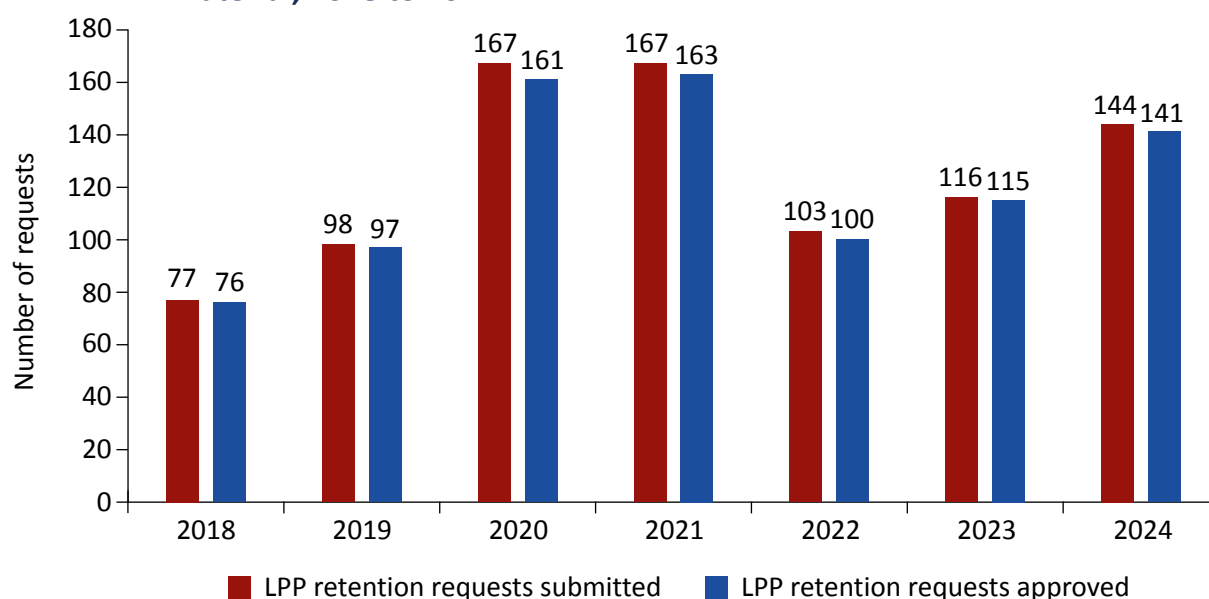
- 7.1 The Investigatory Powers Act 2016 (IPA) and its Codes of Practice provide additional safeguards for certain forms of confidential and legally privileged information. Judicial Commissioners have a statutory role in authorising and overseeing the acquisition and retention of such material. Safeguards are also set out in the Police Act 1997, the Regulation of Investigatory Powers Act 2000 (RIPA),³⁰ 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 without appropriate oversight.

Legal Professional Privilege (LPP)

- 7.2 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.
- 7.3 In 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.
- 7.4 In the event that public authorities do obtain LPP material in their exercise of investigatory powers, they must inform us if they wish to retain that material for a purpose other than destruction. When making their decision as to retention, 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.
- 7.5 In 2024, 144 applications were made in relation to the retention of LPP material. Of these, Judicial Commissioners approved 141.

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

Figure 7.1: Number of requests submitted and approved for the retention of LPP material, 2018 to 2024



Confidential journalistic material and sources of journalistic information

- 7.6 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 and demonstrate an overriding requirement in the public interest. We expect these applications to be rare.
- 7.7 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 the IPA and RIPA 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.

Communications data (CD) relating to journalists and sources of journalistic information

- 7.8 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 2018 Communications Data (CD) Code of Practice.
- 7.9 Under section 77 of the IPA, authorisations for CD seeking to identify a journalistic source require the prior approval of a Judicial Commissioner. The Judicial Commissioner must be satisfied that there is an overriding requirement in the public interest to approve an application to identify a source of journalistic information.
- 7.10 In 2024, 11 applications were made under section 77. LEAs and wider public authorities made five such applications, all of which were investigated further as part of our *ex post facto* oversight. A summary of these is set out below:

Case 1

- 7.11 The first case (one application) was submitted in support of a harassment investigation. This involved two freelance journalistic photographers suspected of stalking an individual to take pictures. CD was acquired for both to corroborate the accounts given during police interviews and identify contact between the two around the time of the incidents. There was no intention to use the data to identify any journalistic sources. The application was approved by a Judicial Commissioner.

Case 2

- 7.12 The second case (one application) concerned an anonymous call made to a journalist reporting the location of an explosive device. Incoming call data on the journalist's mobile phone was sought to identify the caller. In this instance, determining whether the messenger was a journalistic source or a criminal seeking to anonymously disseminate a warning, was subject of enhanced consideration. We assessed that the informant should be considered a journalistic source and a Judicial Commissioner's approval was sought and provided.

Case 3

- 7.13 The third case (one application) presented similar circumstances to Case 2 in that an anonymous call was made to the landline of a regional newspaper reporting the location of two explosive devices. A period of one hour of incoming call data was requested to identify the caller. On the basis that any or all numbers might feasibly relate to legitimate journalistic sources in contact with the newspaper around the same time, the Judicial Commissioner approved the application.

Case 4

- 7.14 The fourth case (two applications) involved an unknown person offering to sell personal data to a journalistic publication. The applications presented a sound intelligence case for suspecting that the information being offered had been unlawfully obtained following a breach of confidentiality and the law. These applications were approved by a Judicial Commissioner who concluded that there is a strong public interest in identifying those who breach laws designed to protect personal data.

Other applications relating to journalists and sources of journalistic information

- 7.15 Looking at the use of other powers, our inspections have not identified any concerns in relation to the handling of journalistic material. While there was a single occasion when an applicant should have sought a higher authority level for its application because of the prospect of obtaining journalistic material, no such material was in fact obtained.
- 7.16 The number of applications to acquire journalistic material in other powers will always be substantially 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.

- 7.17 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.
- 7.18 In 2024, 59 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.
- 7.19 As with CD, applications relating to sources of journalistic information must all be considered by a Judicial Commissioner (even if not relating to journalistic sources). In 2024, there were 106 warrant applications to identify a journalistic source.

Additional safeguards for health records

- 7.20 The intelligence agencies may apply for a specific bulk personal dataset (BPD) warrant to retain and examine a dataset that 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.

8. Technology

Overview

- 8.1 This chapter sets out our approach to understanding and overseeing the impact of Artificial Intelligence (AI) on privacy within the context of investigatory powers and technology developments within IPCO.

IPCO's Scope of Interest in AI

- 8.2 In 2024, we developed our formal "Scope of Interest" in AI, setting out how AI intersects with the use of investigatory powers.³¹ As AI technologies become increasingly embedded in national security and law enforcement operations, it is essential that their use is subject to robust and independent oversight.
- 8.3 Our framework outlines the types of AI systems and use cases that fall within our remit. These include AI tools used to support applications for investigatory powers, assist with the conduct of authorised activity, analyse data obtained through those powers or manage the retention, sharing or deletion of such data. We are particularly focused on how AI may increase the scale, speed or depth of intrusion into individuals' privacy, and the potential for unintended collateral intrusion.
- 8.4 We have defined a set of criteria to help identify when a system qualifies as AI for the purposes of our oversight. These include systems that operate autonomously, can adapt in response to new information or generate new outputs such as text, images, or predictions. Our interest is not limited to bespoke AI tools but also includes off-the-shelf or AI features embedded within commonly used software.
- 8.5 This framework now informs our inspection programme. We are engaging with public authorities to understand how AI is being used in practice and to ensure that its deployment remains lawful, necessary and proportionate in the context of investigatory powers. We will continue to monitor developments closely and provide further updates in our 2025 Annual Report.

IPCO's technology and adoption of AI

- 8.6 As mentioned in Chapter 3, we have continually maintained and improved our IT systems to support our changing operations both in terms of authorisations and oversight. We continue to look to the future, considering new and emerging technology and how adoption could support us to deliver our objectives.

31 See: <https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCOs-Scope-of-Interest-in-AI.pdf>

- 8.7 In 2024, we identified potential improvements to our system that handles warrants. Our aim was to reduce duplication, streamline processes, increase efficiency, improve our management information and ultimately, reduce the risk of errors. We started work to improve the system late in 2024 and we expect Phase 1 to complete in mid-2025. We plan to continue this system upgrade in phases over a few years. Due to a reduced funding allocation and uncertainty about funding in future years, we have had to spread the cost over a longer-time horizon, delaying the project's completion and its anticipated benefits. The longer-term aim is that this will be part of a cross-HMG warrants process using mutually supporting and integrated systems, thereby reducing duplicated effort and friction across the system.
- 8.8 In 2024, we amended the communications data (CD) Case Management System (CMS) by refining our ability to capture reasons why applications are returned to applicants. In addition, we enabled more authorities to submit applications on our CMS via our Request Application Authorisation (RAA) tool, thereby improving efficiency, and made changes to our search tools to enable better interrogation of the CMS.
- 8.9 These improved systems will enhance our ability to deliver effective oversight. For example, we are building into the new warrants management system a feature that will enable Judicial Commissioners to flag warrants for particular review as part of inspections and help Inspectors to access them more easily. Additionally, we made progress in improving the technology available to Inspectors, with the aim of enabling remote access to certain law enforcement records. The first remote inspection using this technology took place in early 2025. We anticipate that this development will make inspections more efficient and flexible, reducing the time and cost associated with travel, particularly for shorter inspections of forces with lower use of relevant powers without reducing the rigour of our oversight. It is also expected to minimise disruption to public authorities and, in some cases, enable simultaneous reviews across multiple organisations, which will be especially valuable in the context of thematic audits. We will provide an update in our 2025 Annual Report.
- 8.10 In late 2024, we began early exploration of how IPCO could benefit from AI tools to support our work. We built our understanding of HMG guidance on government use of AI, in particular the principles, strong governance requirements and how and why AI should be adopted. We used this understanding, alongside our knowledge of existing points of friction and inefficiency in our systems, to identify a few potential ideas where we could apply AI to deliver improvements and the parameters in which these would work. We are clear that we will keep a human in the loop and will not be outsourcing our decision-making to AI tools. This work continues and we will provide an update in our 2025 Annual Report.

9. Technology Advisory Panel (TAP) Annual Report 2024

- 9.1 In accordance with section 246(6) of the Investigatory Powers Act 2016 (IPA), the Technology Advisory Panel's (TAP) Annual Report to the Investigatory Powers Commissioner (IPC) must be copied to the Secretary of State and Scottish Ministers. The 2024 Report was submitted in June 2025 and is reproduced below.

Foreword from Dame Muffy Calder, Chair of the TAP



*Dame Muffy Calder,
Chair of the TAP.³²*

It has been a privilege to chair the TAP throughout 2024, a year in which the pace of technological change has shown no signs of slowing. The TAP continues to play a crucial role in providing expert advice to IPCO on emerging technologies and their implications for investigatory powers.

Over the past year, the Panel has engaged with a range of public authorities, participated in inspections and contributed to vital discussions on how investigatory powers are exercised in a rapidly evolving technological landscape. Our work has not only supported the Judicial Commissioners but has also helped deepen the Panel's understanding of complex operational contexts, enabling us to offer more effective advice.

I want to take this opportunity to thank my fellow Panel members for their expertise and dedication, and to recognise the invaluable collaboration we've had with IPCO and wider stakeholders. As we look ahead, the TAP remains committed to ensuring that technological advancements are understood and appropriately considered in the exercise of investigatory powers, with privacy safeguards at the forefront.

A handwritten signature in blue ink that reads 'M Calder'.

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

Remit of the TAP

- 9.2 The TAP was set up under the IPA (sections 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 development of techniques to use investigatory powers while minimising interference with privacy.

32 Photo by Ian Georgeson Photography for the RSE's Women in Science in Scotland exhibition.

Membership of the TAP

9.3 The TAP comprises experts with backgrounds in academia, government, and industry, ensuring a breadth of knowledge. Since 1 March 2022, Dame Muffy Calder has chaired the TAP. Biographies of all TAP members can be found on the IPCO website, and TAP members during 2024 included:³³

- Daryl Burns;
- John Davies;
- Karen Danesi;
- Professor Richard Mortier; and
- Professor Dame Alison Etheridge

Key achievements in 2024

9.4 The TAP continued its vital work in 2024, advising IPCO on emerging technological issues and their implications for investigatory powers. Throughout the year, the TAP engaged with key stakeholders, participated in several events and undertook research to enhance the panel's understanding of technological developments.

9.5 This year saw the reintroduction of the TAP's 'Portfolios of Work,' which encompasses a range of current and emerging technologies, each headed by a member of the TAP. This work will set the strategic direction of the TAP.

9.6 One of the key technologies highlighted in these portfolios is Artificial Intelligence (AI). The TAP has been actively supporting the IPC and his office in deepening their understanding of AI and how it relates to investigatory powers. This support has been multifaceted, including assisting in the drafting of IPCO's 'Scope of Interest in AI,' which outlines the areas of AI that are most relevant to its work.³⁴ Additionally, the TAP has provided ongoing technical assistance, helping IPCO to consider how to oversee public authorities using AI in relation to investigatory powers and how to consider adoption of AI use cases for its own operations.

Engagements

9.7 TAP members participated in a range of engagements throughout 2024, contributing their expertise to key discussions and initiatives. Notable engagements included:

- participation in the International Oversight Working Group (IOWG) technical meeting in Brussels in April; and
- delivery of a presentation to all IPCO staff in June.

Workshops

9.8 The TAP continued its involvement in workshops, sharing insights and exploring technological challenges with internal and external partners.

33 See: <https://www.ipco.org.uk/who-we-are/technology-advisory-panel/>

34 See: from paragraph 8.2.

Inspections

9.9 Throughout the year, TAP members participated in IPCO inspections, primarily in order to provide advice on related technology and processes as well as to develop Panel members' wider experience and knowledge, to strengthen their advice to the Judicial Commissioners. TAP members participated in several inspections over the year, including at:

- MI5;
- Secret Intelligence Service (SIS);
- Government Communications Headquarters (GCHQ);
- Police Scotland;
- Metropolitan Police Service (MPS); and
- the National Crime Agency (NCA).

Looking ahead

9.10 The TAP will continue advising on technological trends, privacy safeguards and their integration into investigatory powers, ensuring that the IPC and his office have the upmost support in carrying out their oversight work. Two areas for attention will be AI and proportionality and impacts of future telecommunications technologies (5G, 6G).

10. Statistics

Overview

- 10.1 Each year, we compile data on the use of investigatory powers. With the changes we implemented in 2020 to improve our data collection process now fully embedded, our current focus is on using these refined methods to ensure the effective and proportionate collection of data. Our goal is to gather the necessary data in a manner that is both precise and proportionate.
- 10.2 We are mandated to provide statistics on investigatory powers as stipulated by section 234 of the Investigatory Powers Act 2016 (IPA). While we adhere to these statutory requirements, we also strive for maximum transparency without compromising national security or unduly impeding the operational effectiveness of those we oversee. We try to avoid presenting statistics that could be partial or misleading. Consequently, our statistical publications may be limited in scope in areas where detailed contextual information is not feasible, particularly concerning the activities of intelligence agencies.
- 10.3 We believe the statistics we have chosen to publish accurately reflect the use of investigatory powers and the extent of authority exercised. Where feasible, we maintain consistency with previous years' formats to facilitate comparative analysis. We invite feedback on the relevance of the statistics presented and the transparency of our reporting.³⁵

Warrants and authorisations

- 10.4 In 2024, 363,656 warrants and authorisations were issued across all powers. Table 10.1 provides a further breakdown of this number. Law enforcement agencies (LEAs) continue to account for the highest proportion of authorisations due to their significant use of communications data (CD) powers.

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

Table 10.1: Investigative and other powers authorised by public authority sector, 2020 to 2024

	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	17,693	298,800	1,461	425	332	318,711
2023	14,892	319,562	2,371	518	272	337,615
2024	17,330	342,864	2,567	631	264	363,656

Notes:

¹ Figures from public authorities (collected through an external statistical questionnaire) include all CD authorisations, including those not submitted to IPCO. These may be authorised under alternative sections of the IPA (e.g., national security under section 61) and are therefore not directly comparable with IPCO's internal figures.

² We identified potential double-counting and inconsistent reporting practices in external returns for 2022 and 2023. These figures have now been corrected.

- 10.5 Table 10.2 sets out the total number of warrants and authorisations issued, considered and approved in 2024. This table also includes details on specific notifications to the Investigatory Powers Commissioner's Office (IPCO), as well as the total number of submissions that were refused by Judicial Commissioners. In 2024, a total of 13 applications were refused.
- 10.6 Judicial Commissioners also have the option to request further information on an application before making a decision. There may also be internal discussion with our Legal Team, inspectorate and Technology Advisory Panel (TAP). In 2024, there were 93 cases where Judicial Commissioners sought external clarification and for most of these, sufficient information was provided, or the application was revised by the applicant to enable it to be approved.³⁶

³⁶ To note, this figure excludes communications data applications returned for rework.

Table 10.2: Breakdown of authorisations, notifications and refusals, including those considered by a Judicial Commissioner, 2024

	Considered by a Judicial Commissioner	Approved, issued or given	Refused by a Judicial Commissioner
Covert human intelligence sources (CHIS) including juveniles and relevant sources	-	2,453	-
CHIS criminal conduct authorisations	658	658	n/a
Relevant source notifications ¹	-	908	-
Directed surveillance	n/a	7,157	n/a
Intrusive surveillance	515	515	0
Property interference under section 5 of the Intelligence Services Act 1994	n/a	436	n/a
Property interference under the Police Act 1997	-	986	-
Bulk personal datasets – class warrant	90	89	1
Bulk personal datasets – specific warrant	69	69	0
Directions under section 219 of the Investigatory Powers Act 2016	0	0	0
Directions under section 225 of the Investigatory Powers Act 2016	0	5	0
Bulk communications data acquisition warrant	24	24	0
Communications data authorisation ²	n/a	345,567	n/a
Requests to identify journalistic sources using communications data under section 77 of the Investigatory Powers Act 2016	13	13	0
Bulk interception warrant	27	27	0
Targeted examination of interception warrant	104	104	0
Targeted interception warrant	3,059	3,058	1
Bulk equipment interference warrant	29	29	0
Targeted examination of equipment interference warrant	105	105	0
Targeted equipment interference warrant	3,036	3,028	8
Mutual assistance warrant	0	0	0
Request to retain legal professional privileged material	144	141	3

Notes:

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

² Figures from public authorities (collected through an external statistical questionnaire) include all CD authorisations, including those not submitted to IPCO. These may be authorised under alternative sections of the IPA (e.g., national security under section 61) and are therefore not directly comparable with IPCO's internal figures.

Statutory purpose of applications

10.7 Table 10.3 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 10.3: Authorisations by statutory purpose, 2021 to 2024

Statutory purpose	Number of authorisations			
	2021	2022	2023	2024
Prevent/detect crime	268,697	256,091	326,080	278,598
Preventing death or injury	36,663	47,853	60,134	54,303
National security	13,772	16,374	13,276	13,803
Identify person	814	979	1,051	980
Interests of public safety	418	537	839	575
Economic well-being	360	223	292	512
Other	142	116	67	57

Notes:

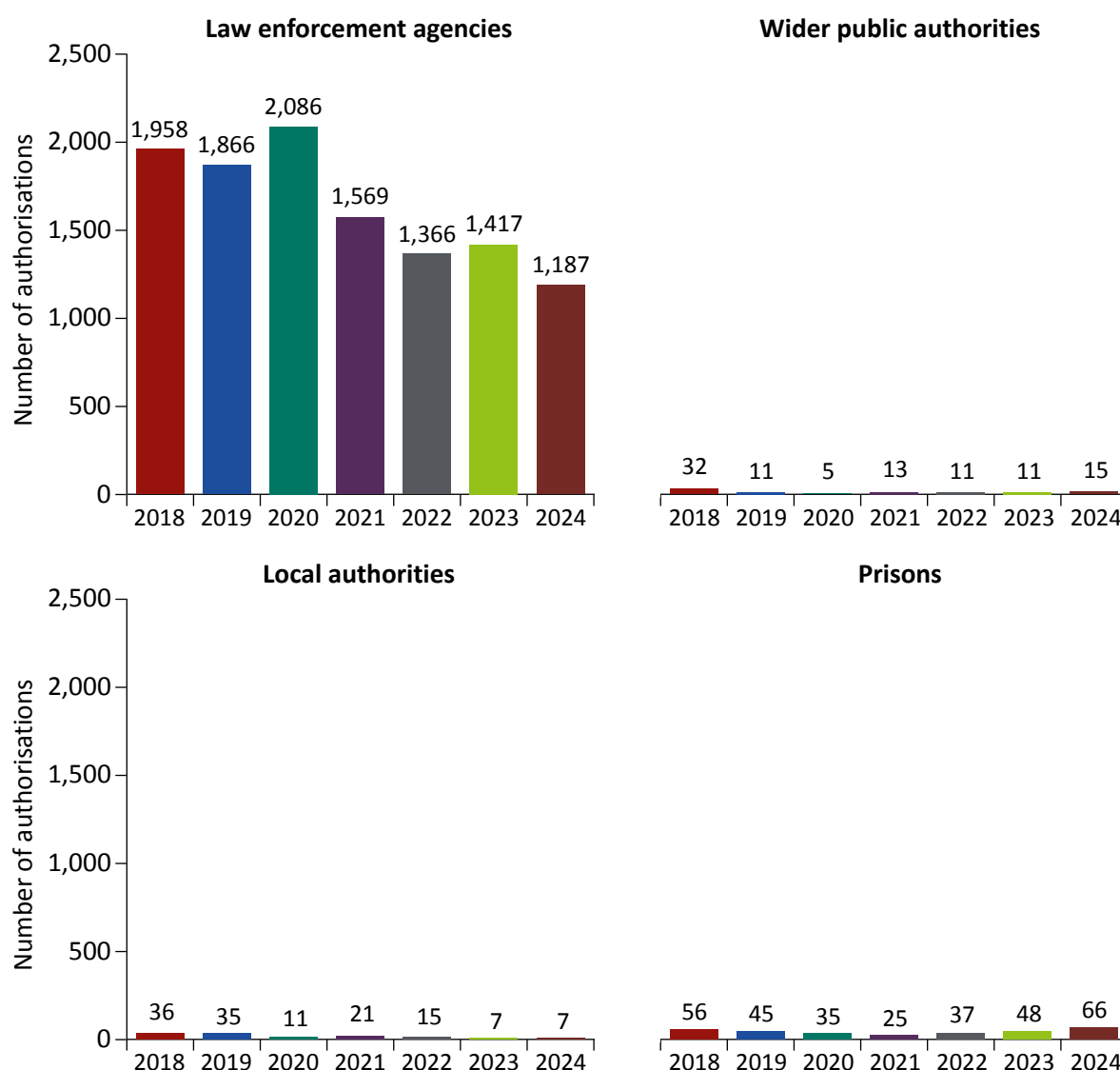
¹ The breakdowns by statutory purpose and crime type are derived solely from external returns and are subject to variation in how public authorities categorise authorisations. These figures may not align with total volumes or internal reporting.

² We identified potential double-counting and inconsistent reporting practices in external returns for 2022 and 2023. These figures have now been corrected.

Covert human intelligence sources (CHIS)

10.8 Figure 10.1 shows the total number of covert human intelligence sources (CHIS) authorisations made in 2024 across LEAs, wider public authorities (WPAs), local authorities and prisons. In total, 1,275 authorisations were made in 2024 across all sectors. Of the 1,187 authorisations to LEAs, seven of these were urgent.

Figure 10.1: Covert human intelligence sources across law enforcement agencies, wider public authorities, local authorities and prisons, 2018 to 2024



Juvenile CHIS

- 10.9 Of the 1,275 CHIS authorisations granted, only four related to juveniles. None of these individuals were under the age of 16 at the time the authorisation was granted.

Criminal Conduct Authorisations

- 10.10 The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 amended the Regulation of Investigatory Powers Act 2000 (RIPA) with criminal conduct authorisations being made from August 2021. In 2024, Judicial Commissioners were notified of 1,018 individuals authorised under this legislation. The number of CHIS or relevant source Criminal Conduct Authorisations (CCAs) made under section 29B of RIPA where a CCA was obtained totalled 739. It is worth noting that a single authorisation for criminal conduct may involve multiple people and a single operative might be authorised on a number of operations throughout the year.

Relevant sources

- 10.11 Renewals for authorisations for relevant sources (or LEA undercover police operatives) must be approved by a Judicial Commissioner at the 12-month stage. Table 10.4 sets out the number of relevant source applications and authorisations since 2020.

Table 10.4: Relevant sources authorisations and applications, 2020 to 2024¹

	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
2023	642	545	0	128	0
2024	549	465	4	102	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.

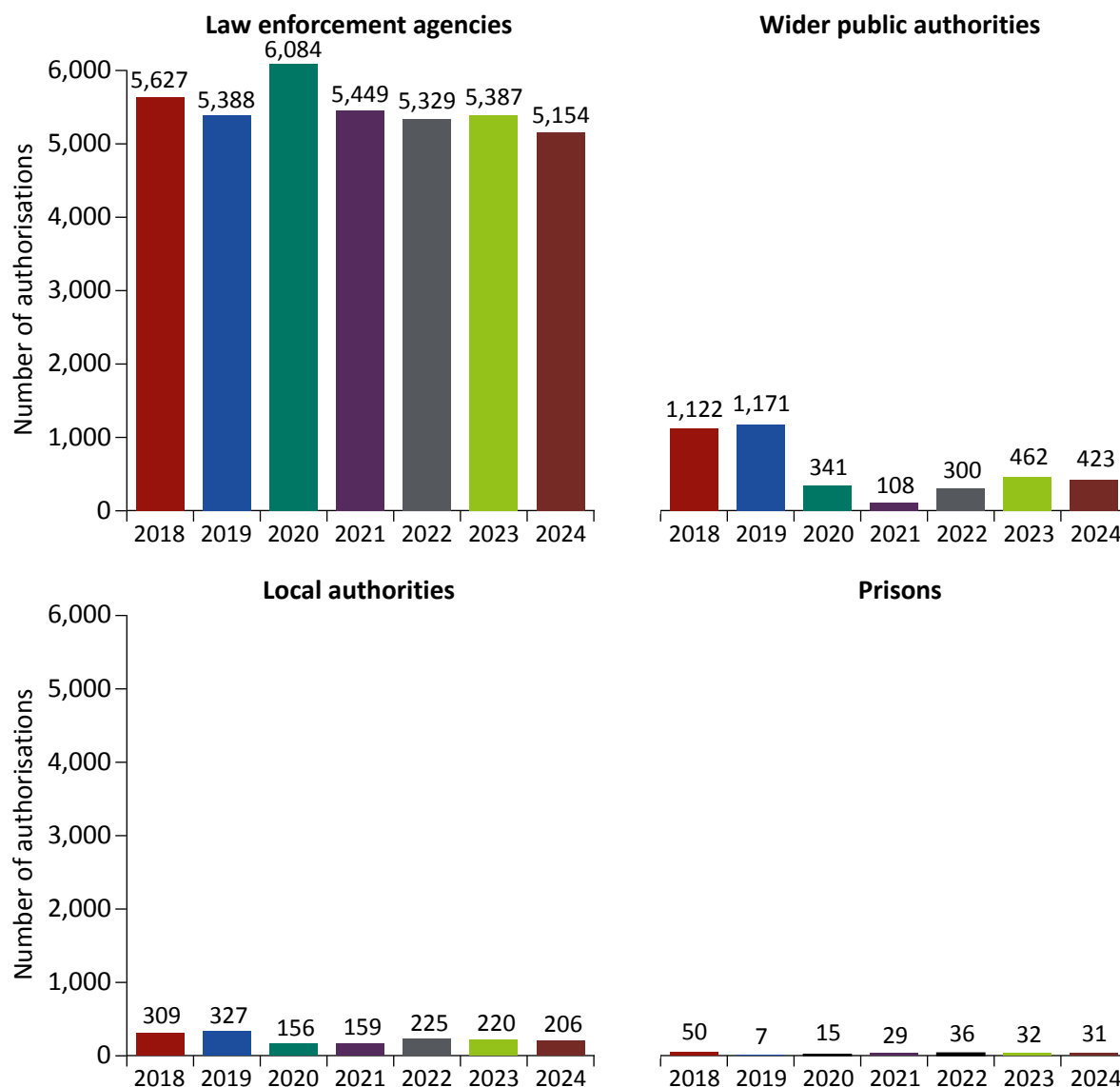
² Applications include notifications to IPCO of authorisations and applications to renew authorisations after 12 months.

³ Refusals relate to applications to renew only.

Directed surveillance

- 10.12 Figure 10.2 shows that a total of 5,814 directed surveillance authorisations were made in 2024 across LEAs, WPAs, local authorities and prisons. Of these authorisations, 499 authorisations were made under urgent provisions.
- 10.13 In 2024, 30 applications were granted where legal professional privilege (LPP) was either sought or likely to be obtained. A further 11 applications were granted which either sought or were likely to obtain confidential material (other than LPP).

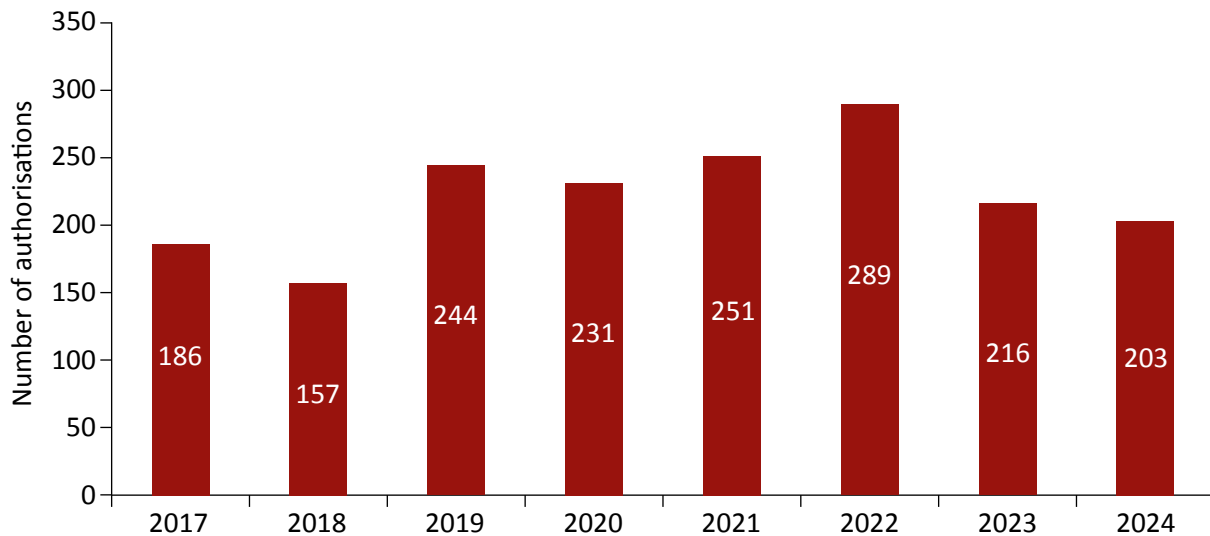
Figure 10.2: Directed surveillance authorisations across law enforcement agencies, wider public authorities, local authorities and prisons, 2018 to 2024



Intrusive surveillance

10.14 In 2024, 203 authorisations were granted to LEAs. Of these, nine were urgent authorisations and two authorisations either sought or were likely to obtain confidential or privileged material which was other than LPP. A further 25 were granted where LPP was either sought or likely to be obtained.

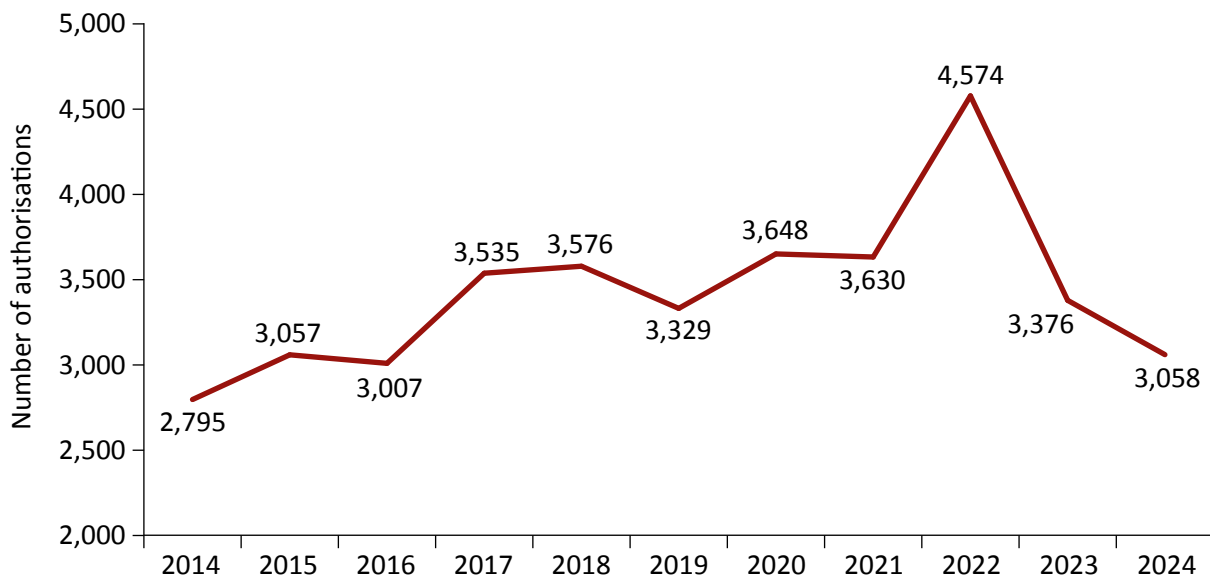
Figure 10.3: Intrusive surveillance authorisations for law enforcement agencies, 2017 to 2024



Targeted interception (TI)

10.15 Figure 10.4 shows the number of targeted interception (TI) warrants authorised in 2024. A total of 3,058 authorisations were made, of which 264 were urgent.

Figure 10.4: Targeted interception authorisations for the UK intelligence community and law enforcement agencies, 2014 to 2024



10.16 Table 10.5 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 2018 Code of Practice, all warrants that involve 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 2018 Code of Practice.

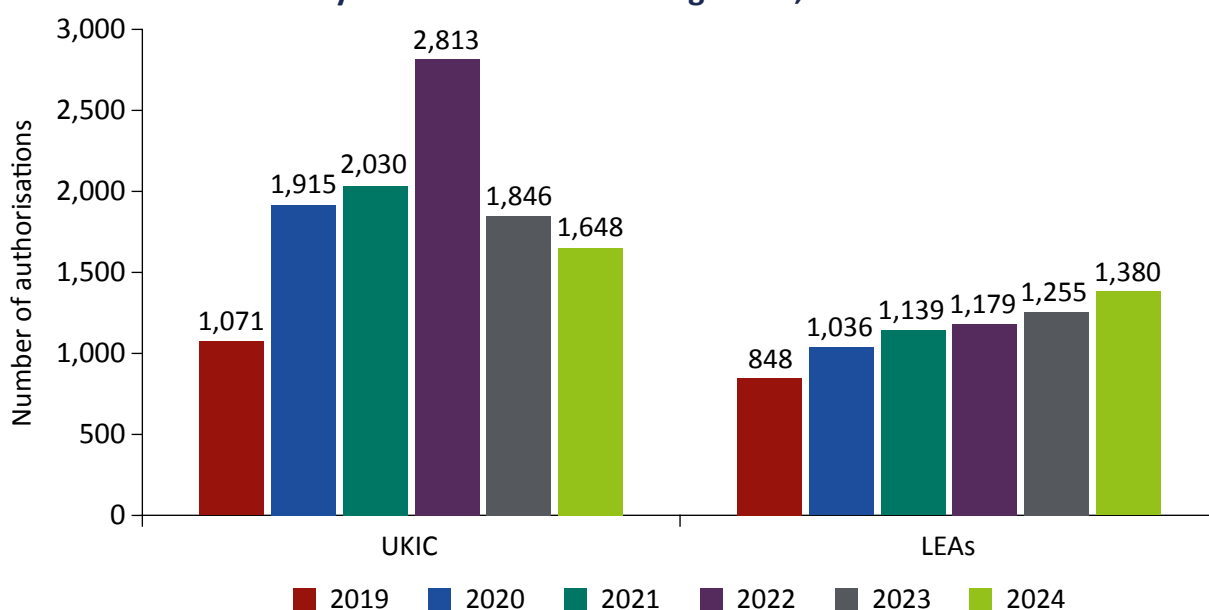
Table 10.5: Targeted interception warrants involving confidential material, 2020 to 2024

	LPP – sought	LPP – possible	Sensitive professions
2020	12	359	35
2021	11	187	11
2022	29	211	59
2023	14	313	88
2024	11	436	88

Targeted equipment interference (TEI)

10.17 In 2024, 3,028 authorisations were granted to use targeted equipment interference (TEI) powers, of which 565 were urgent. As was the case over the past four years, the three WPAs with access to TEI powers made no use of them in 2024.

Figure 10.5: Targeted equipment interference authorisations for the UK intelligence community and law enforcement agencies, 2019 to 2024



10.18 Table 10.6 shows that confidential material was only sought or likely to be obtained in a small number of TEI warrants.

Table 10.6: Targeted equipment interference warrants involving confidential material, 2020 to 2024

	LPP – sought	LPP – possible	Sensitive professions
2020	14	207	66
2021	15	64	14
2022	29	499	63
2023	12	213	88
2024	17	339	83

Communications data (CD)

10.19 In total, 345,567 CD authorisations of all kinds were made in 2024. These included applications made under section 60A, as authorised through IPCO; warrants authorised under section 61 in the interests of national security (which were not authorised through IPCO); and those made under the urgent provisions. Table 10.7 shows the totals by sector and, as was the case in previous years, LEAs remain the greatest users of the power, responsible for over 330,000 of all authorisations made.

Table 10.7: Communications data authorisations, 2020 to 2024

	UKIC	LEA	WPA	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	287,374	1,150	258	259	298,241
2023	8,458	308,239	1,898	291	192	319,078
2024	10,820	332,033	2,129	418	167	345,567

Notes:

¹ *Figures from public authorities (collected through an external statistical questionnaire) include all CD authorisations, including those not submitted to IPCO. These may be authorised under alternative sections of the IPA (e.g., national security under section 61) and are therefore not directly comparable with IPCO's internal figures.*

² *We identified potential double-counting and inconsistent reporting practices in external returns for 2022 and 2023. These figures have now been corrected.*

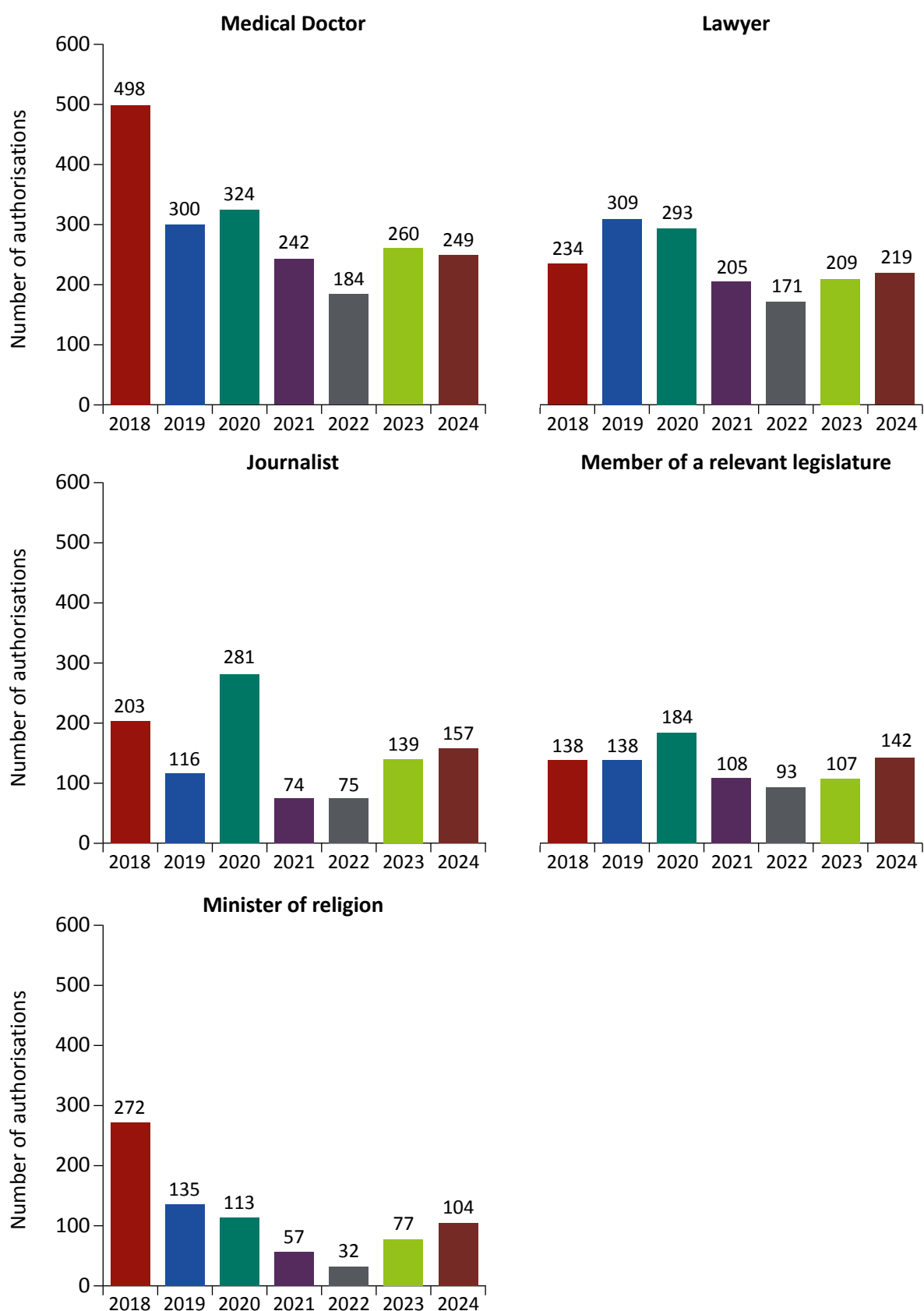
10.20 CD applications are used to request one or more data items. Given the volume of requests, there is a margin of error in the reported numbers. That said, the nature of our oversight means that this does not reduce the level of confidence we have in those authorities. In 2024, around 1.4 million data items were obtained, similar to 2023.³⁷

10.21 Figure 10.6 sets out the number of authorisations obtained in relation to sensitive professions. With the exception of relevant subscriber data, CD acquired and disclosed under the IPA does not include the content of communications. 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 against the public interest. The 2018 CD 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 relevant legislatures, ministers of religion or doctors.

10.22 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 to attribute phone numbers or email addresses to perpetrators.

³⁷ This figure excludes UKIC authorisations.

Figure 10.6: Communications data authorisations involving members of a sensitive profession, 2018 to 2024



- 10.23 A total of 11 applications for CD were made to confirm or identify a journalist's source, two of which were urgent. There were no Judicial Commissioner refusals in relation to these applications. A further 106 applications were made across all powers to identify journalists' sources.
- 10.24 Table 10.8 shows the number of CD authorisations for each of the seven statutory purposes. Prevention and detection of crime remains the principal purpose, representing 80% of the total authorisations.

Table 10.8: Communications data authorisations by statutory purpose, 2020 to 2024

	2020	2021	2022	2023	2024
Prevention and detection of crime	263,383	257,338	242,460	314,229	267,162
Preventing death or injury	31,257	36,663	47,853	60,140	54,303
National security	11,470	10,425	9,011	8,824	10,734
Identify person	581	814	979	1,051	980
Public safety	221	246	474	804	529
Economic well-being	60	45	14	60	74
Investigations into alleged miscarriages of justice	4	6	8	34	8

Notes:

¹ The breakdowns by statutory purpose and crime type are derived solely from external returns and are subject to variation in how public authorities categorise authorisations. These figures may not align with total volumes or internal reporting.

² We identified potential double-counting and inconsistent reporting practices in external returns for 2022 and 2023. These figures have now been corrected.

- 10.25 For each CD authorisation where the statutory purpose is "prevention and detection of crime", public authorities which 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 table 10.9), which is why the total number of crime types exceeds the number of authorisations shown in table 10.7 above.
- 10.26 Table 10.9 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 (32.6%), followed by sexual offences (15.9%) and violence against the person (10.6%).

Table 10.9: Communications data authorisations by crime type under the “prevent and detect crime” statutory purpose, 2020 to 2024

Statutory Purpose	2020	2021	2022	2023	2024
Violence against the person	26,443	23,371	28,463	46,827	37,364
Violence against the person – homicide	14,392	13,976	14,561	18,570	12,628
Theft offences	5,950	4,947	7,491	7,242	9,197
Terrorism offences	2,048	2,050	1,649	2,055	1,368
Sexual offences	30,815	34,800	39,524	46,983	55,741
Robbery offences	6,917	5,277	8,375	12,262	11,414
Public order offences	2,977	3,058	2,462	2,988	2,757
Possession of weapons offences	13,336	12,154	6,993	20,049	14,507
Other	37,343	27,572	13,341	21,303	21,075
Miscellaneous crimes against society	9,153	11,128	18,636	17,359	13,714
Harassment	7,056	9,435	9,762	13,738	12,929
Fraud and Deception Offences	15,955	20,392	19,968	24,105	26,829
Drugs Offences	81,861	87,277	125,494	146,191	114,527
Criminal Damage	551	666	636	662	1,094
Burglary	11,513	11,183	13,333	19,586	14,942
Arson	1,447	1,052	1,249	1,606	1,125
Total	267,757	268,338	311,937	401,526	351,211

Notes:

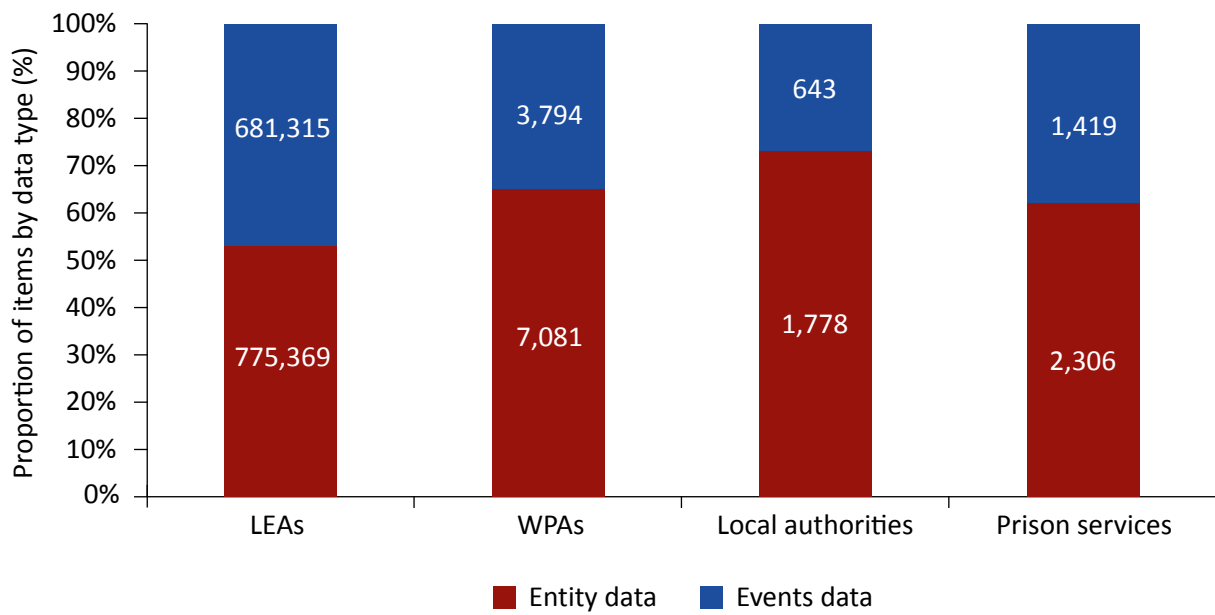
¹ The breakdowns by statutory purpose and crime type are derived solely from external returns and are subject to variation in how public authorities categorise authorisations. These figures may not align with total volumes or internal reporting.

² We identified potential double-counting and inconsistent reporting practices in external returns for 2022 and 2023. These figures have now been corrected.

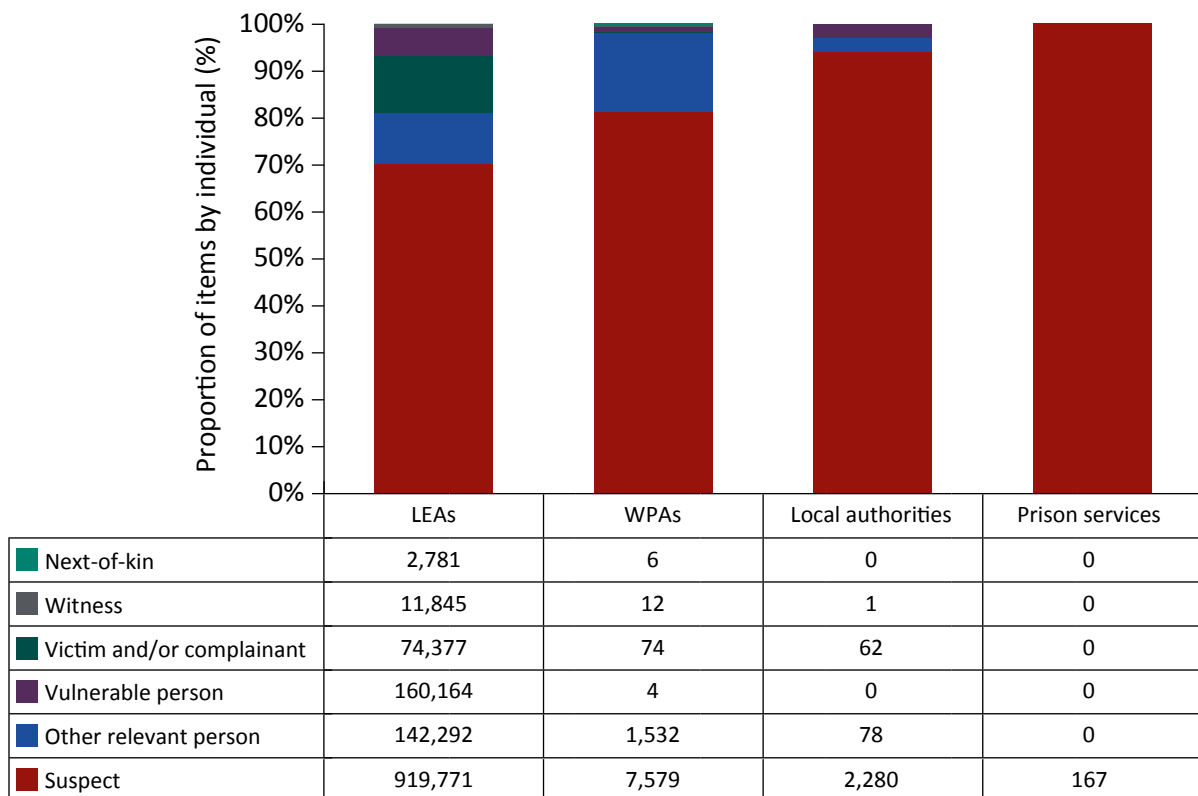
10.27 Figure 10.7 shows the total number of CD items sought in authorised applications by whether the items of data were categorised as either events or entity data.³⁸

38 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.

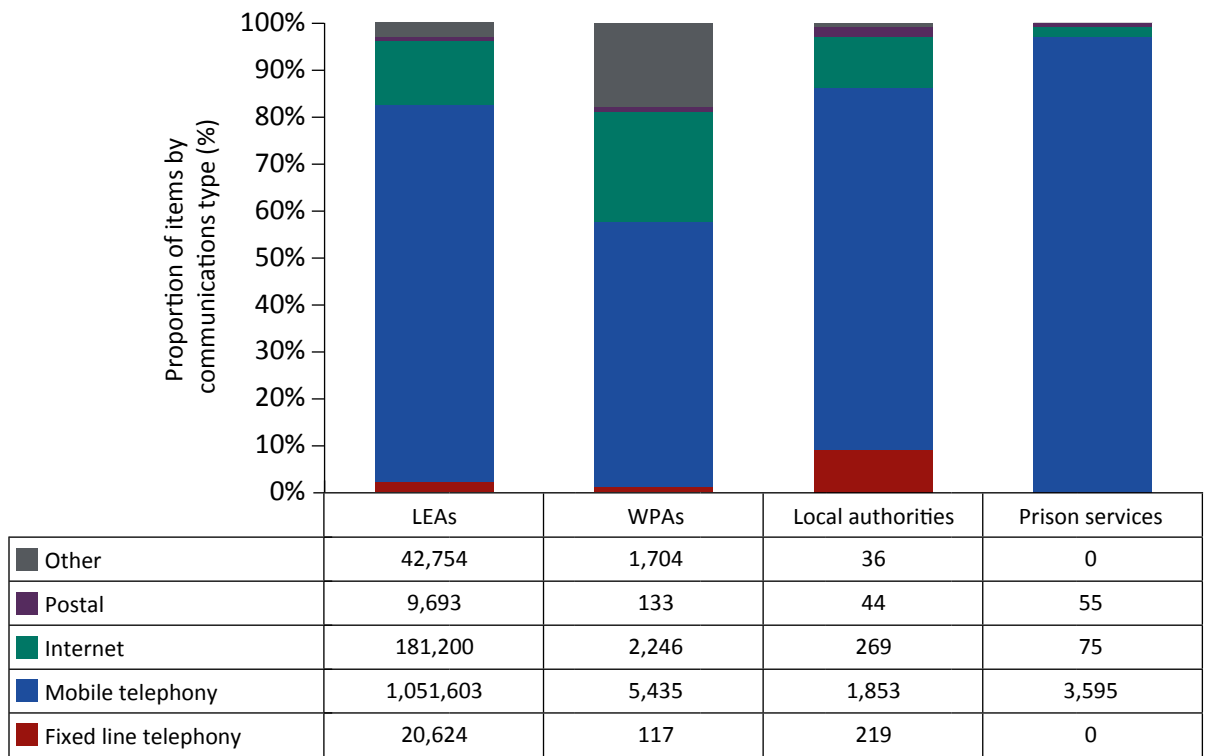
Figure 10.7: Communications data items by data type, 2024

10.28 Figure 10.8 sets out the number of items of CD sought categorised by the subjects of the authorisations. One authorisation may relate to more than one category of subject.

Figure 10.8: Communications data items by individual (subject), 2024

10.29 Figure 10.9 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 10.9: Communications data items by communications type, 2024



Applications submitted to IPCO

- 10.30 In 2024, IPCO received a total of 329,098 CD applications, as shown in table 10.10. This represents a continued increase in volume compared to 2023, with consistently higher application numbers recorded throughout the year.
- 10.31 Over the five-year period from 2020 to 2024, the number of CD applications submitted directly to IPCO has shown a consistent upward trend. Internal figures show an average annual increase of approximately 10%, with year-on-year growth ranging from 8.3% to 11.5% (see table 10.10 for a detailed breakdown). This trend reflects sustained operational demand.
- 10.32 It is important to note that these internal statistics differ from externally reported figures. Internal data is centrally managed and subject to robust quality assurance, providing a reliable and consistent basis for assessing long-term trends. In contrast, external data is collected from a wide range of public authorities and is more susceptible to variation in recording practices, definitions and data quality.

Table 10.10: Applications submitted to IPCO, 2020 to 2024

		2020	2021	2022	2023	2024
Total applications		226,383	245,272	270,842	301,957	329,098
Year-on-year change (%)		-	8.3%	10.4%	11.5%	9.0%
Decisions made		223,322	242,535	266,755	295,904	320,539
Of which	Authorised	199,482	222,009	245,125	273,099	291,345
	Returned	23,596	20,244	21,529	22,688	29,129
	Rejected	244	282	100	117	65
Withdrawn		3,051	2,736	4,087	6,053	8,558
Applications with no decision at year end (31 December)		10	1	0	0	1

Notes:

¹ These figures are derived from IPCO's internal systems and reflect applications submitted directly to IPCO. They are subject to robust validation and quality assurance processes. These data are considered reliable and consistent across reporting periods.

² In contrast, external statistics are collected from a wide range of public authorities, each with varying recording practices and data quality controls. These differences can lead to discrepancies between the two datasets, particularly in total volumes, statutory purpose classifications and crime type breakdowns. While internal data provides a stable and reliable baseline, external data offers broader coverage but is more susceptible to inconsistency.

- 10.33 While in 2024 there was a slight increase in the number of applications returned for rework, the data indicates a general improvement in the quality of CD applications over the longer term. A fluctuation in returns for rework (RfR) figures is likely attributable, at least in part, to the increasing complexity of CD applications and wider definitions of what is now considered to be CD.
- 10.34 The number of applications we returned for rework during 2024 was an illustration of the level of scrutiny that was applied to every application and the data shown below provides assurance that our high standard of case consideration has remained consistent.
- 10.35 Table 10.11 highlights that the primary reason for returning an application to the submitting authority was that an Authorising Individual assessed the application did not meet 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. We regularly share information on RfR with law enforcement and public authorities to help them improve the quality of applications.

Table 10.11: Returns for Rework (RfR) reasons, 2020 to 2024

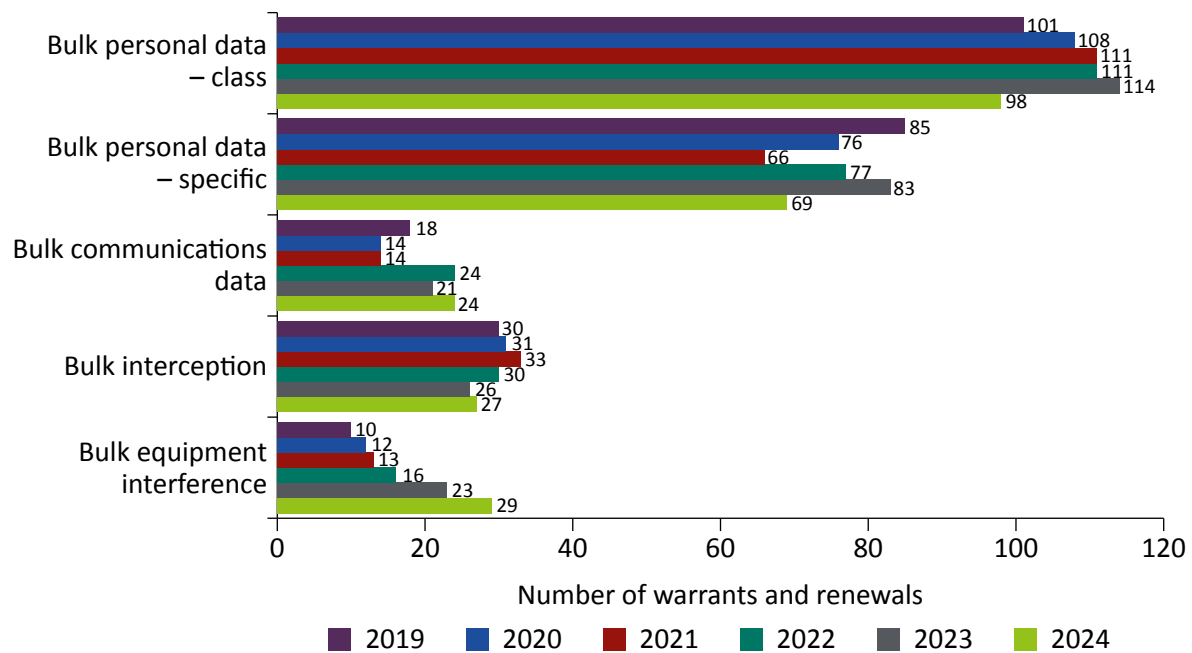
Reason	2020	2021	2022	2023	2024
Necessity	2,832 12%	4,389 18%	4,720 17%	4,471 14%	8,320 18%
Proportionality	2,832 12%	2,988 12%	4,135 15%	4,458 14%	5,710 12%
Dates/Times	2,596 11%	3,516 15%	3,669 13%	4,066 13%	4,752 10%
Consequential ticked/not ticked	1,888 8%	1,383 6%	2,129 8%	2,652 8%	4,704 10%
Accuracy	1,652 7%	1,922 8%	1,725 6%	2,665 8%	3,639 8%
Consequential Justification	1,652 7%	1,805 8%	1,667 6%	0 0%	0 0%
Attribution	1,416 6%	1,244 5%	1,657 6%	2,576 8%	3,082 7%
Collateral intrusion	1,180 5%	1,000 4%	1,592 6%	1,267 4%	2,005 4%
Forward facing	944 4%	952 4%	1,025 4%	1,867 6%	2,466 5%
Data Type	944 4%	587 2%	695 3%	1,108 3%	1,395 3%
Other (up to 21 categories)	5,663 24%	4,183 17%	4,183 15%	7,285 22%	10,112 22%
Total	23,599 100%	23,969 100%	27,197 100%	32,415 100%	46,185 100%

Note:

Applications can be returned for rework for more than one reason. Therefore, the total number of RfR reasons exceeds the number of applications returned in table 10.10.

Bulk powers

10.36 Figure 10.10 shows the number of authorisations (including renewals) for each class of bulk warrant since 2019.

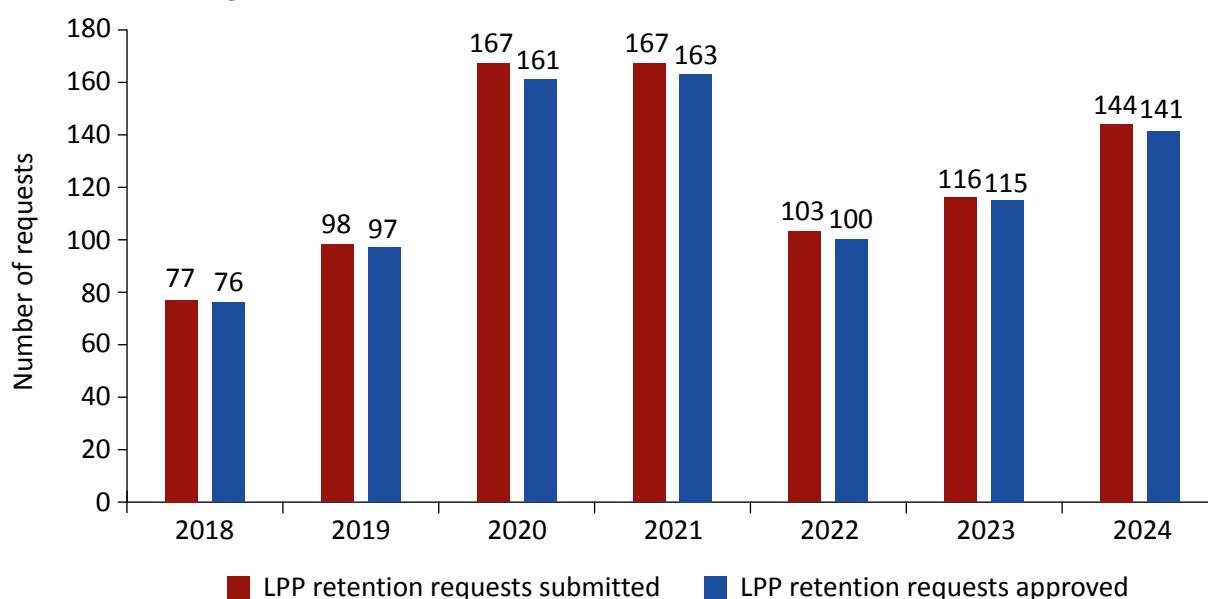
Figure 10.10: Bulk warrants and renewals by type, 2019 to 2024

10.37 The Investigatory Powers Act 2016 (Remedial) Order 2024 brought in the requirement to obtain authorisation from a Judicial Commissioner prior to an analyst selecting for examination bulk interception content where the purpose was to acquire confidential journalistic material or identify a source of journalistic information (or where this was highly likely). In 2024, there were eight authorisations for such content. The Investigatory Powers (Amendment) Act 2024 (IP(A)A) introduced a similar requirement for bulk equipment interference and in 2024, Judicial Commissioners made 15 authorisations relating to such content.

Legal professional privilege (LPP) material

10.38 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 2024, we approved 141 requests from 144 applications.

Figure 10.11: Number of requests submitted and approved for LPP material, 2018 to 2024



Intelligence Services Act 1994

- 10.39 Section 5 of the Intelligence Services Act 1994 (ISA) relates to interference with property or wireless telegraphy by the intelligence agencies. In 2024, 436 section 5 warrants were granted by the Secretary of State (these are not subject to Judicial Commissioner approval).
- 10.40 Section 7 of the ISA applies to acts done outside the UK and which are necessary for the proper discharge of a function of the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) only. In 2024, 92 section 7 warrants were issued by the Secretary of State (these are not subject to Judicial Commissioner approval).

The Principles

- 10.41 '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.
- 10.42 Table 10.12 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 occurrence 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.
- 10.43 As in previous years, there are important caveats to the data presented here.

- 10.44 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 (for example, in response to a major terrorist plot) 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.
- 10.45 Secondly, as The Principles makes clear, consulting Ministers does not imply that action will or will not be authorised.

Table 10.12: Cases reviewed under The Principles, 2020 to 2024

Number of cases reviewed		2020	2021	2022	2023	2024
Cases reviewed on inspection		93	68	104	85	101
Cases reviewed proactively due to contentious legal or policy issues		8	7	7	2	1
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	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	3	9
	Personnel identified a real risk of CIDT and submitted for approval	15	17	17	22	22
	Personnel identified a real risk of rendition and submitted for approval	3	0	0	0	0
	Personnel identified a real risk of unacceptable standards of arrest and/or detention and submitted for approval	28	34	54	45	50

- 10.46 It is important to note that, in respect of The Principles, our oversight concerns the process which informs a Minister's decision; however, unlike in other aspects of our work, we do not review the Minister's decision itself on judicial review grounds. The IPC does not consider it appropriate to present statistics on areas that are outside of his direct oversight and has decided that the current data presented in the Annual Report in respect of our oversight of The Principles is appropriate. The operation of The Principles is complex and providing meaningful statistics that demonstrate how the policy has been used without divulging details of specific cases has always been a difficult balance to strike and we will continue to keep their presentation under review.

The UK-US Data Access Agreement

10.47 In 2024, Judicial Commissioners conducted additional reviews of 3,265 necessity and proportionality statements for relevant targeting decisions when an individual is targeted for the first time under a general descriptor on a thematic TI warrant and targeted CD authorisations for the purpose of acquiring data pursuant to the UK-US Data Access Agreement (DAA). The number of additional reviews does not reflect the number of times a new targeting decision under the DAA is made. This is because an additional review is not required where an individual is named under a targeted warrant or added to a thematic warrant by way of major modification.³⁹

³⁹ See: from paragraph 4.83 for more details.

Annex A. Definitions and glossary

10.48 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	<p>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.</p> <p>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.</p>
Communications data	<p>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.</p>
Covert human intelligence sources	<p>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.</p> <p>“Relevant source” 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.</p> <p>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 or detecting economic crime or of preventing disorder; or in the interests of the economic well-being of the United Kingdom.</p>
Covert surveillance	<p>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.</p> <p>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.</p>
Directed surveillance	<p>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.</p>

Term	Definition
Double lock	<p>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. Other than in urgent circumstances, only with authorisation from one of our Judicial Commissioners can a warrant be issued.</p> <p>This is the double lock process. It ensures a two-stage approval for the use of investigatory powers.</p>
Equipment interference	<p>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.</p>
Interception	<p>Interception is the process that makes the content of a communication available for examination by someone other than the sender or recipient of the communication. (NB: examination is the process by which material is selected to be read, looked at or listened to by the persons to whom it becomes available as a result of interception and could include listening to telephone calls or opening and reading the contents of a person's letters or emails).</p>
Intrusive surveillance	<p>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.</p>
Modification	<p>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.</p>
National Security Notice	<p>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 (NSN) to direct a UK telecommunications operator to act in the interests of national security.</p> <p>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.</p>

Term	Definition
Operational purpose	The IPA established 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 IPA, the full list of operational purposes is approved by the Prime Minister.
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 install a listening device covertly 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 UK 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	<p>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 (TCN) to require telecommunications or postal operators to ensure they are able to provide assistance with the acquisition of communications data, interception and equipment interference.</p> <p>After a Technical Capability Notice has been issued and implemented, a company can act quickly and securely when a warrant is authorised.</p>

Term	Definition
Thematic Warrants	<p>Thematic warrants are warrants that have more than one subject. There are two types of thematic warrant:</p> <p>The first individually names/describes all the subjects. Any additional subjects can only be added by a major modification, which must be notified to a Judicial Commissioner. For equipment interference by law enforcement agencies, a major modification requires prior approval by a Judicial Commissioner, or retrospective approval if the modification is urgent.</p> <p>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, although individual factors (such as their telephone numbers or email addresses) would be added by internally authorised minor modifications.</p>
The Principles	<p>“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.</p> <p>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.</p> <p>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.</p>

Term	Definition
Urgency provisions	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> decide 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.
Wireless telegraphy	Wireless telegraphy refers to the conveying of information using electromagnetic energy with a frequency of less than 3,000 gigahertz.

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	<ul style="list-style-type: none"> • Security Service (MI5) • Secret Intelligence Service (SIS) • Government Communications Headquarters (GCHQ) <p>References to “UKIC” mean the United Kingdom intelligence community.</p>
Defence	Ministry of Defence
Law Enforcement Agencies (LEAs)	<ul style="list-style-type: none"> • 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) • National Crime Agency (NCA) • The Home Office (Border Force and Immigration Enforcement)
Wider Public authorities (WPAs)	<ul style="list-style-type: none"> • 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 and Trade (Insolvency Service) • Department for Work and Pensions (DWP) • Department for the Economy for Northern Ireland • Department for 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

	<ul style="list-style-type: none"> • 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 • Maritime Management Organisation • Medicines and Healthcare Products Regulatory Agency • Ministry of Housing, Communities and Local Government (MHCLG) • National Anti-Fraud Network (NAFN) • National Health Service (NHS) Business Services Authority • 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
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
ACCIPIF	Authorised Communications Controls and Interception Policy Frameworks
AI	Artificial intelligence
AI	Authorising individual
ACL	Access control levels
AO	Authorising officer
APCC	Association of Police and Crime Commissioners
BCD	Bulk communications data
BEI	Bulk equipment interference
BI	Bulk interference
BPD	Bulk personal dataset
CAB	Covert Authorities Bureau
CCA	Criminal Conduct Authorisations
CDR	Call data records
CETA	Centre for Emerging Technology and Security
CFU	Counter Fraud Unit
CHIS	Covert human intelligence sources
CIDT	Cruel, inhuman or degrading treatment
CJEU	Court of Justice of the European Union
CMA	Computer Misuse Act 1990
CMS	Case Management System
CMT	Compliance Monitoring Team
CoA	Court of Appeal
COM	Covert Operations Manager
CNE	Computer Network Exploitation
CoP	Code of Practice
COPO	Crime (Overseas Production Orders) Act 2019
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service

CSA NS	Chief Scientific Advisor for National Security
CSP	Communications service provider
CST	Council for Science and Technology
CTOC	Counter Terrorism Operations
CTP	Counter Terrorism Police
DAA	Data Access Agreement
DCMS	Digital Culture, Media and Sports
DIPC	Deputy Investigatory Powers Commissioner
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
EIO	European Investigation Order
EION	European Intelligence Oversight Network
ERS	Error Reduction Strategy
2FA	Two-Factor Authorisation
FACT	Federation against Copyright Theft
FIORC	Five Eyes Intelligence Oversight Review Council
FOIA	Freedom of Information Act 2000
FSA	Finite State Automata
HMGCC	His Majesty's Government Communications Centre
HOIE	Home Office Immigration Enforcement
ICR	Internet Connection Records
IIOC	Indecent images of children
IP	Internet protocol
IPA	Investigatory Powers Act 2016
IP(A)A	Investigatory Powers (Amendment) Act 2024
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
LEA	Law Enforcement Agency
LPP	Legal professional privilege
LTHSE	Long-Term High Security Estate
ML	Machine Learning
MoU	Memorandum of Understanding
NAFN	National Anti-Fraud Network
NCDS	National Communications Data Service
NCMEC	National Centre for Missing and Exploited Children
NCND	Neither confirm nor deny
NPCC	National Police Chiefs' Council
NSIRA	National Security and Intelligence Review Agency
NSWG	National Source Working Group
NTAC	National Technical Assistance Centre
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
PET	Privacy Enhancing Technology
PIC	Participation in crime
PIO	Police Prison Intelligence Officers
PSI	Prison Service Instruction

RA	Requesting Agencies
RAA	Request Application Authorisation
REPHRAIN	National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online
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
RPM	Records Product Management
RRD	Retention, review and deletion
SAO	Senior Authorising Officer
S4E	Selection for examination
SLE	Service Level Expectation
SIS	Secret Intelligence Service
SIO	Senior Investigating Officer
SOI	Subject of Interest
SOP	Standard operating procedure
SOU	Special operations unit
SLE	Service level expectations
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
SVAP	Security Vetting Appeals Panel
TAP	Technology Advisory Panel
TI	Targeted Interception
TEI	Targeted Equipment Interference
TIDU	Technical Intelligence Development Unit
TSU	Technical Surveillance Unit
TO	Telecommunications operator
UCPI	Undercover Policing Inquiry
UTC	Universal co-ordinated time

UKDA	UK Designated Authority
UKIC	UK Intelligence Community
WGD	Warrant Granting Departments
WPA	Wider Public authority
ZKP	Zero Knowledge Proofs

Annex B. Budget

The table below gives a breakdown of the financial statement for the Investigatory Powers Commissioner's Office (IPCO) for the financial year 2024/25.

Budget total: £15.9million	
Period: 1 April 2024 to 31 March 2025	
	Full year outturn
Pay costs	£10,968,708
Travel and subsistence	£420,473
Office supplies and services	£31,193
Training and recruitment	£29,088
Estates	£1,292,441
IT and communications	£1,278,266
Legal costs (including consultancy)	£18,623
Other costs and services	£1,749
Capital costs	£1,251,862
Total	£15,292,404

For the financial year 2024/25, we spent £15.3 million against an annual budget allocation of £15.9 million, which consisted of £14 million of resource spending (RDEL) and £1.3 million of capital spending (CDEL).

A significant proportion of this expenditure relates to pay costs for staff, Judicial Commissioners and the Technology Advisory Panel (TAP). The pay budget allocation for staff costs has remained unchanged since 2017 despite there being increased costs through changes to the workforce, salary increases and staff payments, which include recruitment and retention payments, allowances for additional hours worked (AHW) and costs associated with secondments.

There has been a moderate increase in travel and subsistence expenditure. This is primarily due to increased international engagement and the general rise in costs due to inflation.

Our estates costs increased compared to the previous financial year as a result of inflation and rising cost of utilities, facilities management and fixed fee costs.

The capital budget allocated for financial year 2024/25 was £1.6 million and the actual year to date spend on capital was just under £1.3 million. This was made up of expenditure on improvements to our IT systems and our London office.

Annex C. Serious errors

In 2024 the Investigatory Powers Commissioner (IPC) decided that the following errors would be investigated as potential serious errors within the meaning of section 231 of the Investigatory Powers Act 2016 (IPA).

Error investigation 1

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Customer information relating to an Internet protocol address resolution (IPAR)
Description:	<p>A public authority resolved several IP addresses in connection with child grooming offences. Police officers attended an address connected to one of them and questioned the occupants. A possible error was suspected when no link was identified with the key suspect of the investigation. Upon review, it was found that the IP address supplied to the public authority had been truncated for technical reasons. This was highlighted by the telecommunications operator in a declaration attached to the data.</p>
Consequence:	<p>Police visited a person unconnected to this incident. The effect on those visited was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error. The known issue with the data supplied by the telecommunications operator has been brought to the attention of relevant staff.</p>

Error investigation 2

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Subscriber and call data records
Description:	<p>A national helpline reported to the police concerns regarding a person it had been in contact with. The helpline passed the police the mobile internet connection details which had been used by the caller during the engagement. The police member of staff looking to show the whereabouts of the caller, selected the incorrect time zone when making a request for data from the telecommunications operator. As a result, the data passed back was incorrect and police officers, looking to ensure the wellbeing of the caller, attended the wrong address. After speaking to the occupants, it was clear that a mistake had occurred. The correct data was then obtained and the correct address visited. The delay caused by the error had not negatively affected the original caller.</p>
Consequence:	<p>The delay was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error. The use of the Error Reduction Strategy (ERS) which looks to prevent such mistakes, was reiterated to the staff member involved.</p>

Error investigation 3

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Subscriber
Description:	A police force received a 999 call from a suicidal person. Before the whereabouts of the caller could be established the call was ended. When passing the details of the number used by the caller a digit was recorded incorrectly. When a subscriber check was conducted, it therefore showed an unconnected person and address in another force area. Officers attended the address given, in an attempt to ensure the wellbeing of the caller. The mistake was identified and the correct data then obtained. When the genuine caller was identified there was no indication that greater harm befell them as a result of the delay caused by this mistake.
Consequence:	The delay was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error. The importance of recording such details correctly was highlighted to the personnel involved.

Error investigation 4

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Subscriber and call data
Description:	A police officer obtained communications data (CD) to support an investigation into a missing person. The officer mistakenly used a telephone number from another investigation in which CD was not being sought. The incorrect number was therefore passed to the relevant telecommunications operator who provided data. This material was analysed and an address found which police officers visited in an attempt to locate the missing person. The mistake was then discovered. When the correct data was obtained there was no indication that greater harm befell the missing person as a result of the delay caused by this mistake.
Consequence:	Police visited a person unconnected to this incident. The effect on those visited 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
Classification:	Data acquired without lawful authority
Data Acquired:	Account information
Description:	An investigator within a public authority acquired CD from a telecommunications operator without lawful authority to do so. Incorrect legislation had been utilised. Once discovered, 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 without lawful authority. The investigation established the request had been made in good faith and owing to inexperience. As a consequence, it was determined that no Section 11 offence had occurred.
Consequence:	The public authority dealt with this matter internally, a course of action that was deemed appropriate by the IPC after a review of the case. Measures were put in place to ensure the unlawfully acquired data would not feature in any legal proceedings.

Error investigation 6

	Public authority
Human or Technical:	Human
Classification:	Data acquired without lawful authority
Data Acquired:	Account details
Description:	A financial investigator within a police force submitted a request to a financial institution for CD without lawful authority to do so. Data was acquired as a result. Once discovered, the force undertook an internal investigation 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 without lawful authority. The investigation established the request had been made owing to a lack of training and knowledge. Consequently, it was determined that no Section 11 offence had occurred.
Consequence:	Additional training was provided to relevant staff and the data was destroyed. The IPC was informed of the steps that had been taken and deemed them appropriate in the circumstances described.

Error investigation 7

	Public authority
Human or Technical:	Human
Classification:	Incorrect Data
Data Acquired:	Subscriber and call location-based data
Description:	Communications data to locate a missing person was obtained. A number was identified and called. With no reply its location was obtained and the incident transferred to the relevant policing area. When the original call data was rechecked, a mistake was identified in the last digit of the number. The other force was immediately contacted and cancelled. The missing person was found locally safe and well.
Consequence:	The delay was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error. The importance of checking numbers before submission was highlighted to the officer involved by a supervisory officer.

Error investigation 8

	Public authority
Human or Technical:	Human
Classification:	Incorrect Data
Data Acquired:	Subscriber and call location-based data
Description:	A crime in action led officers to obtain from a witness the mobile number of the victim. A verbal authority to acquire CD was approved. Based on the CD returned, lines of inquiry were commenced. Within an hour, a second number for the victim was provided and CD acquired. When both datasets were compared, anomalies were apparent. Further contact with the witness confirmed they had provided incorrect digits. Discovery of the error coincided with the victim calling family enabling police to locate them safe and well.
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 9

	Public authority
Human or Technical:	Human
Classification:	No IPA authority
Data Acquired:	None
Description:	A telecommunications operator (TO) provided us details of attempts made by officers to acquire CD without an approved application in place. No CD was actually provided and the TO notified the specified point of contact (SPoC) Unit so advice could be given.
Consequence:	This resulted as a consequence of the application of new guidance on the definition of CD ⁴¹ during the transition from data previously provided under a Data Protection Act request now falling under a requirement to obtain that data under an IPA authorisation. Similar occurrences were found with other TOs, but no CD was released and officers were informed of the need to contact their CD SPoC Unit. We raised this issue in forums to Senior Responsible Officers and telecommunications operators were advised to continue to monitor the situation for compliance.

41 See: from paragraph 3.8.

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