

IPCO

Investigatory Powers
Commissioner's Office

OCDA

Office for Communications
Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2021

IPCO

Investigatory Powers
Commissioner's Office

OCDA

Office for Communications
Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2021

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 20 March 2023

Laid before the Scottish Parliament by the Scottish Ministers 20 March 2023

HC 910

SG/2023/6



© Crown copyright 2023

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

978-1-5286-3724-4
E02807467 03/23

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. Developments in 2021	11
3. Relevant litigation in 2021	16
4. Protecting confidential or privileged information	23
5. Communications and engagement	26
6. Technology Advisory Panel	29
7. The Office for Communications Data Authorisations	37
8. MI5	41
9. Secret Intelligence Service	47
10. Government Communications Headquarters	52
11. The Ministry of Defence	58
12. The Principles	60
13. Law Enforcement Agencies and Police	65
14. Wider Public Authorities	85
15. Local Authorities	89
16. Prisons	94
17. Warrant Granting Departments	99
18. Errors and Breaches	101
19. Statistics	110

Annex A. Definitions and glossary	125
Annex B. Budget	134
Annex C. Serious errors	136
Annex D: Public engagements	151

Letter to the Prime Minister

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

October 2022

Dear Prime Minister,

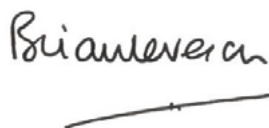
I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) from 1 January to 31 December 2021.

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

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

I continue to be impressed by the dedication and professionalism of the authorities I oversee in undertaking this vital work, particularly in the light of pressures faced over the last two years. It is evident that compliance with the legislation remains a high priority in all aspects of their work.

Yours sincerely,



The Rt Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

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

I am pleased to present this report covering the activities of my offices during 2021. This was my second full year as the Investigatory Powers Commissioner (IPC) and was, once again, a year that has been challenging both for my teams and all of the public authorities I oversee.

As required by section 234 of the Investigatory Powers Act 2016 (IPA), this report sets out details of how the functions of the Judicial Commissioners were carried out during 2021. This includes the activities of the Office for Communications Data Authorisations (OCDA), which also operates under my jurisdiction.

I will use my introduction this year to make a number of general observations before I go on to draw out some specific matters that arose during 2021. These are then covered in more detail in the relevant parts of the report.

General observations

It is essential that the public has confidence that the most intrusive investigatory powers are being used where necessary and in accordance with the law. The work done by both IPCO and OCDA, under the direction of the Judicial Commissioners, is critical in checking and assessing compliance and offering reassurance that an appropriate approach is being taken across the full range of public authorities who can use these powers. In this report, I hope we have been able to explain how we conduct our oversight, both through our authorisations and inspection work, and where things have gone well or where improvements can be made. Both IPCO and OCDA have matured considerably over the last three to four years and, contrary to initial concerns about the likely impact of the additional layers of oversight they bring, I am pleased to see how the challenge is welcomed and taken very seriously.

In the same vein, I was pleased to read the report of Joseph Cannataci, the UN Special Rapporteur on the right to privacy, following his visit to the United Kingdom in 2018.¹ I welcome the observations made by the Special Rapporteur and, despite his own initial reservations, his recognition of the value added by IPCO in its oversight of the use of investigatory powers. I am aware that comments are sometimes made about the IPC “marking his own homework” as IPCO is responsible for overseeing the work of OCDA. Although I personally am satisfied that this does not invoke any conflict of interest, I have taken the decision to appoint one of my Judicial Commissioners to oversee the OCDA quality assurance and compliance reviews. This will provide further reassurance that OCDA is fulfilling its statutory functions effectively and in accordance with the IPA.

1 See: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session46/Documents/A_HRC_46_37_Add.1_AdvanceEditedVersion.docx

It is important to note the evolving and expanding role of IPCO. In the last few years, my oversight functions have been expanded to cover new areas including responsibilities under Schedule 3 to the Counter-Terrorism and Border Security Act 2019² and the Covert Human Intelligence Sources (Criminal Conduct) Act 2021. Ultimately, it is for the Government and Parliament to decide the functions of the IPC but it is critical for me that we do not detract from or dilute the very high level of scrutiny and oversight that we provide across the full range of our responsibilities. As such, it is an important principle that any additional new functions should be considered carefully and the appropriate resources, both in terms of Judicial Commissioners and officials, provided.

Similarly, it remains a key principle that all functions of the IPC should have a statutory footing. In this respect, I welcome the commitment from the Home Office to make clear, through a statutory instrument, the basis of my oversight of the Government Communications Headquarters (GCHQ) Equities Process³ and the National Crime Agency (NCA) and the Metropolitan Police Service's (MPS) compliance with 'The Principles relating to the Detention and Interviewing of Detainees Overseas'. I am grateful for the work on this to date and hope this objective can be met by the end of 2022. Discussions continue with the Ministry of Defence (MoD) about whether my oversight of its policies governing its use of overseas covert human intelligence sources (CHIS) and overseas surveillance activity should also be placed on a statutory basis.

While the ongoing Covid-19 pandemic continued to put pressure on our working practices in 2021, both IPCO and OCDA responded with alacrity over the year. We have maintained business as usual but have also taken the opportunity to review and, where appropriate, enhance the way the organisations operate. IPCO carried out 450 inspections across all public authorities in 2021, using a mix of remote and in-person activity appropriate to the organisation under review.⁴ This model means we have been able to maximise efficiencies, both for ourselves and for those we are inspecting, without compromising the rigour of our oversight. Separately, Chapter 7 shows how the revised operational structures put in place by OCDA in 2021 have enabled us to build in the necessary resilience to respond to fluctuations in applications. I am also pleased that I did not need to request that the Secretary of State reinvoke section 22 of the Coronavirus Act 2020 which, in March 2020, provided for the appointment of temporary Judicial Commissioners to enable IPCO to continue its scrutiny of authorisations.⁵

I am very grateful to be supported in this role by our experienced Judicial Commissioners. Judicial scrutiny of applications is a fundamental safeguard, ensuring that the use of covert powers to keep the public safe is balanced with the importance of privacy in a democratic society. However, while IPCO continues to attract applicants with distinguished judicial experience, the process for appointing Judicial Commissioners has unfortunately become increasingly and unnecessarily drawn out. I make this comment not as a criticism of those who I know are working to improve things but, rather, by way of an observation that the length of this process may deter future applicants from wishing to take up this important role. This is a situation we must avoid.

Similarly, while there is not a problem with getting people to apply for roles at IPCO or OCDA, the length of time it takes to complete all of the vetting and pre-employment checks to onboard new recruits results in a significant proportion of successful candidates withdrawing from the process. While this Civil Service-wide issue is not unique to IPCO and OCDA, this has left both organisations carrying many vacancies for longer periods of time than is sustainable. The fact there has been no

2 A separate report on the operation of Schedule 3 in 2020 and 2021 will be made to the Home Secretary.

3 See: <https://www.gchq.gov.uk/information/equities-process>

4 A further breakdown of our inspections for 2021 can be found on our website. See: <https://www.ipco.org.uk/what-we-do/inspections/inspection-statistics/>

5 The Investigatory Powers (Temporary Judicial Commissioners and Modification of Time Limits) Regulations 2020 have now expired.

impact on delivery of work to date is purely down to the commitment and additional work of those already employed. This is not a situation that can be sustained indefinitely without consequences.

On that note, I must comment on how everyone across IPCO and OCDA has taken in their stride the upheavals of the last two years and continued to deliver excellent work. Against a backdrop of vacancies, the pandemic and new or increasing demands on their time, this has been truly remarkable. I wish to express my gratitude for their continued dedication in delivering the functions as required of us under the IPA.

I am also grateful for the continuing support of the Technology Advisory Panel (TAP). You can read more about its work in Chapter 6 but, as the world becomes more complex, it is essential that those tackling wrongdoing can access the best tools available to them. Although the IPA was drafted to be technology-neutral, we are often faced with questions about the appropriate authorisation for a particular new technique or on how our oversight can keep pace with emerging technologies. The guidance of the TAP, alongside the expertise of the Inspectorate and our Legal Team, are all essential to us getting this right.

Matters arising in 2021

I am satisfied that working within the legislation and the relevant Codes of Practice remains a top priority for the public authorities I oversee. Our inspections reveal high levels of compliance overall and we see a positive response to our findings. The relatively small number of refusals of authorisations do not, as some suggest, indicate we are simply a rubber stamp. Rather, it shows the quality of engagement and understanding of what we expect to see and the efforts that are made to ensure that the necessity and proportionality justifications are addressed adequately before applications are submitted. Applications of concern are also often withdrawn for reconsideration by the applicant if queries are raised by Judicial Commissioners, rather than waiting for a refusal.

Given that I oversee the use of covert investigatory powers by over 600 public authorities, it is understandable that my report covers a lot of ground. There are a number of issues, however, which are set out later in more detail but to which I would like to draw particular attention, namely:

- **Police Scotland use of undercover operatives:** Following an internal review by Police Scotland of its use of undercover operatives, two inspections were carried out in 2021. Police Scotland has taken immediate action in response to our recommendations and I will continue to monitor their progress in 2022. [See: paragraph 13.26].
- **Handling of targeted interception (TI) material by police Regional Organised Crime Units (ROCU):** Our data assurance programme, which reviews compliance with the safeguards in the legislation and relevant Codes of Practice, identified a number of issues with how ROCUs were handling and storing TI material received from both the NCA and the MPS. Although the key issues have now been resolved, this is an area which will be a focus for inspections in 2022. [See: paragraph 13.48].
- **Home Office error:** In 2021, I was alerted to an error by the Home Office relating to its long-standing arrangements for signing out-of-hours IPA warrants. The Home Office immediately put in place arrangements to rectify the problem and the matter remains under investigation by the Home Office. In the interim, I wrote to all intercepting agencies asking them to review their out-of-hours processes alongside the IPA and the Codes of Practice to make sure they were compliant. We will follow up on the responses in our 2022 inspections and will report on any compliance issues in my next report. [See: paragraph 17.3 and 18.15].

- **Litigation:** In Chapter 3, I have set out the legal developments that have had a bearing on IPCO's work. Of particular significance are the discussions we have had with the Government to understand the implications for our oversight of bulk interception following the judgment of the European Court of Human Rights in *Big Brother Watch v UK*.
- **Data assurance:** In 2019, IPCO commenced a thorough review of all the public authorities I oversee to ensure the responsibilities for data handling, retention and destruction were properly understood. This is not a short-term project for organisations and, while work continues to achieve compliance, I want to take this opportunity to recognise the level of progress that has been made. We have now integrated our data assurance work into our standard inspections and, as such, further details are provided in relevant chapters in this report. [See: paragraphs 13.74-13.79 for law enforcement agencies (LEA)s; 14.13 for wider public authorities; 15.16-15.18 for local authorities; and 16.24-16.25 for prisons.]
- **Legally privileged material:** The Judicial Commissioners and Inspectorate have begun a review of the handling of legally privileged material which has no intelligence value itself but is included within material that does and which needs to be retained. I am keen to ensure that the best protections are in place for such material but this is not a straightforward issue. The review will span all three intelligence agencies and we will report further in due course. [See: paragraph 8.29 for MI5; paragraph 9.33 for the Secret Intelligence Service (SIS); and paragraph 10.40 for GCHQ].
- **Directed surveillance:** In line with previous years, there continues to be a good level of compliance across MI5 in its use of investigatory powers. However, this is the fifth year we have reported improvements that need to be made in the authorisations by MI5 for directed surveillance. We have flagged this as an issue which requires urgent remedial action. [See: paragraphs 8.12-8.13].
- **Covert Human Intelligence Sources (Criminal Conduct) Act 2021:** This Act introduced a new requirement to notify the IPC of all authorisations for CHIS to carry out criminal activities. Further details can be found in Chapter 2 [see: paragraphs 2.2-2.5] with analysis of our first review of the use of the new powers by MI5 and LEAs in paragraph 8.10 and paragraphs 13.16-13.19 respectively. In Chapter 13 [see: paragraph 13.10], I have also included a spotlight on the importance of the welfare of CHIS.
- **Management of intercept material:** I remain concerned about performance and compliance issues in the system used by LEAs to manage intercept material. [See paragraphs 13.45-13.46]. While I am reassured that there are now plans in place to deliver a replacement system, this is still not expected for a number of years. I have asked my team to engage with this programme but also to continue to monitor the current system to ensure any new compliance concerns are addressed as a matter of urgency.
- **Targeted equipment interference (TEI) thematic inspections:** Since the initial thematic inspection of TEI in 2019, my Inspectors have seen much improvement in the assessment of collateral intrusion and the need to reduce the risks involved. As this is an area with emerging and developing technologies, these inspections are increasingly important to ensure that the principles of necessity and proportionality remain at the core of decision making. [See: paragraphs 13.41-13.43.]
- **Acquisition of communications data (CD) in police misconduct cases:** In Chapter 13 [see: paragraphs 13.60-13.63], I set out the progress which has been made by LEAs to ensure that the criminal threshold for acquiring CD is met in internal professional standards investigations, an issue which was first raised in 2019.
- **Freedom of expression:** We have noted on our 2021 CD inspections that there has been an increase in cases where CD is being sought to investigate complaints made about posts on social media platforms. This will be a focus for 2022 as we look to raise awareness of

ensuring due consideration is given between the use of this power and an individual's right to privacy and freedom of expression under the European Convention on Human Rights (ECHR). [See: paragraphs 13.64-13.66.]

- **Prisons:** I continue to be concerned about the arrangements for interception of communications in prisons. I welcome the engagement of Her Majesty's Prison and Probation Service (HMPPS) in working with us to ensure that the rules and arrangements underpinning the interception and monitoring of prisoners' communications are as robust as possible. [See: paragraphs 16.14-16.21.]
- **The Principles:** 2021 was the second full year of operation of 'The Principles relating to the Detention and Interviewing of Detainees Overseas' since they replaced the Consolidated Guidance in January 2020. I am pleased with the high levels of compliance with The Principles that we see on our inspections. Full details of our oversight of this area can be found in Chapter 12.

Looking ahead to 2022

2022 is already shaping up to be another demanding year, both in terms of fully embedding our new ways of working post Covid and having new areas and functions to deal with. A particular focus for us in 2022 will be contributing to the statutory review of the operation of the IPA which is due in the latter part of the year. Given the critical role played by IPCO in ensuring privacy is protected and safeguards are applied, I welcome the Home Office's engagement with my officials as thinking about the review has progressed.

We expect to see the entry into force of the UK-US Data Access Agreement which will require me to keep under review compliance by public authorities within the UK with the terms of the agreement. It will also be the first full year of the new Criminal Conduct Authorisations and I hope that IPCO's regular reviews and inspections will provide some valuable insights into how this new power has been used. Furthermore, while it came into force in June 2020, the full impact of the operation of my new functions under Schedule 3 to the Counter-Terrorism and Border Security Act 2019 will only start to make an impact in 2022; I am required to report separately to the Home Secretary on the operation of those provisions and will do so in due course.

As ever, there will inevitably be new oversight challenges that will require our careful consideration and engagement. However, I have no doubt that my teams at both IPCO and OCDA are well placed and have the tools to deal with whatever 2022 sends our way.

2. Developments in 2021

Overview

- 2.1 This chapter provides an overview of the key policy and operational developments that have had an effect on the Investigatory Powers Commissioner's responsibilities or had an impact on the work of the Investigatory Powers Commissioner's Office (IPCO) or the Office for Communications Data Authorisations (OCDA) in 2021.

Covert Human Intelligence Sources (Criminal Conduct) Act 2021

- 2.2 The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 Act was granted Royal Assent on 1 March 2021. The Act provides an express legal basis for intelligence agencies, law enforcement agencies (LEAs) and other specified public bodies to continue to use authorised undercover officers and covert human intelligence sources (CHIS) to participate in crime for the greater good. The Act introduces a new requirement for all Criminal Conduct Authorisations (CCAs) to be notified to the IPC as soon as reasonably practicable and, in any event, within seven days of being granted.
- 2.3 Ahead of implementation, we agreed, with the law enforcement community and government officials, how the notification procedure would operate and the standards of compliance expected by the Judicial Commissioners who would receive the notifications. This helpful engagement has meant that the introduction of the CCA and notification procedures has been relatively smooth, with only very minor issues identified thus far.
- 2.4 It was agreed that staggered commencement arrangements would allow public authorities, including IPCO, sufficient time to prepare for the introduction of the new statutory regime. For LEAs, this meant that by 15 September 2021, all extant authorisations for "participation in crime" relative to CHIS and undercover officers and any new CCAs for both areas had to be authorised under section 29B of the Regulation of Investigatory Powers Act 2000 (RIPA) and thereafter notified to us no later than within the required seven days.
- 2.5 The Act also gave the IPC oversight of the enhanced safeguards which the Act introduces for juvenile and vulnerable CHIS. The IPC wrote to all relevant authorities in August 2021 asking to be informed within seven days of the authorisation of a juvenile or vulnerable CHIS. The IPC keeps such authorisations under close review, with bespoke inspections taking place as soon as they can be arranged. Additionally, the IPC has requested that a quarterly review of all CCAs is conducted within IPCO, to help inform both Authorising Officers (AOs) and Judicial Commissioners of common themes or issues at an early stage. Early findings from the initial review of CCAs issued by LEAs are set out in Chapter 13 (paragraph 13.18).

Air Traffic Management and Unmanned Aircraft Act 2021

- 2.6 The Air Traffic Management and Unmanned Aircraft Act 2021 amends Part 3 of the Police Act 1997 to extend the property interference regime to certain offences related to the unlawful use of unmanned aircraft (i.e. “drones”). Such offences previously fell below the serious crime threshold and therefore the police lacked powers to combat the use of drones other than in a counter-terrorism or national security context. The amendments fully came into force on 29 June 2021 with Judicial Commissioners being notified of property interference authorisations in the usual way.

The UK-US Data Access Agreement

- 2.7 As reported in our 2020 report, the IPC will oversee use of the UK-US Data Access Agreement which facilitates access by public authorities of electronic data relating to the prevention, detection, investigation and prosecution of serious crime.
- 2.8 Preparations have been made for our oversight of this new function, which will come into force once a date for the entry into force of the agreement has been determined by the UK Government and its US counterparts.⁶

Definition of communications data

- 2.9 An area that caused significant challenge for OCDA throughout 2020 and 2021 is what has become colloquially known as the *IPA versus DPA* (Data Protection Act 2018) issue. This was reported in detail in our last two reports.⁷ The Investigatory Powers Act 2016 (IPA) brought changes to the definitions of communications data (CD) and telecommunications operators (TO). It also prohibited (via the Code of Practice) the use of data protection legislation to circumvent requesting CD under the IPA and introduced a criminal offence of knowingly or recklessly obtaining CD from a TO without lawful authority. This has resulted in public authorities seeking IPA authorisation to acquire information that would previously have been acquired using data protection provisions. In turn, this has presented difficulty for OCDA in that it can only grant authorisation to acquire data that falls within the complex and ambiguous definition of CD under the IPA. At times, this has led to conflict with some public authorities faced with a TO refusing to disclose CD otherwise than by response to an IPA authorisation, and OCDA declining to grant such an authorisation where the information being sought could not clearly be defined as CD.
- 2.10 In early 2021, we conducted a review of the definition of CD and identified many areas of ambiguity arising largely from the Government's decision to adopt a technology neutral drafting style in the IPA. The benefit of this approach is that it aims to ensure that the legislation has longevity by being able to accommodate developments in technology. The trade-off, however, is that the definition has to adopt a degree of ambiguity in order to accommodate those changes in technology. CD is a particularly complex area. It includes data that goes to the heart of how technology systems operate. Determining what constitutes CD under the current definition has found us needing to spend significant time and resources discussing a particular system or service with the Technology Advisory Panel

⁶ See: Data Access Agreement: joint statement by the United States and the UK – GOV.UK (www.gov.uk)

⁷ Annual Report of the Investigatory Powers Commissioner 2019 (page 89). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf and Annual Report of the Investigatory Powers Commissioner 2020 (from paragraph 14.72). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

(TAP), sometimes even down to the packet level; such discussions also often generate multiple legal views.

- 2.11 The outcome of our review was that the IPC is concerned that the current definition of CD is not fit for purpose. He feels that both operational professionals and the public should be able to understand with relative ease what data is CD and what data is not. It cannot be right that only a combination of systems engineers and legal experts poring over the legislation and Code of Practice can reach a tentative conclusion on what is the most widely used investigatory power.
- 2.12 In an attempt to address this, throughout 2021 joint discussions were held between OCDA, IPCO and the Home Office Investigatory Powers Unit to develop additional guidance as to the definition of CD and TO. The guidance explained the IPC's and Home Office's agreed view that the definition of TO is broad, covering many companies which do more than just provide a telecommunications service and which might not be aware that they are a TO within the meaning of the IPA. We consider that the definition is not limited to telephony and internet service providers but is broad enough to include any website owner or operator. This means that social media platforms, online marketplaces, streaming platforms, online dating sites, food delivery services, banks, cloud providers and taxi services booked online are all TOs.
- 2.13 It is important to note, however, that unlike internet service providers which may be exclusively a TO, most of these types of companies will only be a partial TO in respect of certain services. For example, a business which simply provides a telecommunications service is likely to hold all users' account data as CD. With partial TOs, it is, therefore, necessary to determine what data a company holds as a TO rather than for the purposes of other parts of the business as, in general, a CD authorisation will only be available in relation to the data it holds as a TO. For example, the guidance describes how a payment method used for a subscription to an online streaming service would be CD. However, if that company also operates an online marketplace then the payment method used for a transaction would not be CD, as a payment for goods does not relate to the provision or use of the telecommunication service, i.e., the operation of the website.
- 2.14 The challenges for operational practitioners, OCDA and TOs to identify what data is CD and what is not are self-evident, especially if the public authority and OCDA are not familiar with how that business operates. The guidance was formally "launched" by the IPC and the Home Office in November 2021 and will be implemented after a programme of training across public authorities during 2022. We will report on progress on the interpretation and impact on the level of compliance in our 2022 Annual Report. It is the IPC's expectation that the guidance will ultimately be included in the next update of the Code of Practice.
- 2.15 To illustrate one issue with the definition of CD, under old section 21(4)(c) of RIPA, the definition of CD included:
- "any information not falling within [the preceding paragraphs] that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service".*
- 2.16 The definition therefore clearly covered what is often called "subscriber" or "account" data (i.e. "entity data" under the IPA). This is vital for law enforcement as it enables them to identify who is using a particular system or service. It is of note that paragraph (c) of the RIPA definition, in contrast with the preceding paragraphs, did not carve out the content (i.e. the meaning/substance) of a communication. It therefore did not previously matter how a TO held data, i.e., whether it obtained or held data as content. Paragraph (c) could,

however, on its face, include content such as the body of an email. In enacting the IPA, Parliament decided expressly to carve out content from *all* limbs of the definition of CD (see section 261(5) of the IPA). On one view, a large proportion of what is traditionally considered to be subscriber or account data comes from content; for example, your name may be included in an electronic web form when you open an online account and when you click “submit” it is sent to that company’s servers. The “content” or “the meaning” of that communication is the information you have entered in the form. If that is the only record of the subscriber or account data held by the TO then, if that analysis is correct, it places such data beyond the ambit of a CD authorisation. This may therefore pose significant difficulties for law enforcement and other public authorities who rely on this vital information to protect the public. For this reason alone, the IPC considers the case for legislative clarification to be strong.

Operational purposes

- 2.17 The UK intelligence community (UKIC) continues to rely on the full range of operational purposes in the vast majority of its bulk warrants issued under the IPA. We were satisfied, in relation to the bulk warrants we reviewed in 2021, that the operational purposes included in each warrant met the statutory tests: namely, that each purpose was one for which examination of material obtained under the warrant was or might be necessary.
- 2.18 The IPA requires the Prime Minister to review the list of operational purposes annually. This last happened in September 2021.

Inspection findings

- 2.19 During 2021, we reviewed the way our inspection findings are presented in order to provide greater consistency for public authorities and facilitate easier management of required actions. We have replaced “recommendations” with “areas of non-compliance” (with the relevant Act or Code of Practice). These issues require remedial action by the Senior Responsible Officer (SRO) and, to assist with the prioritisation of their response, we grade them as follows:

Areas of non-compliance

Critical: indicates a significant vulnerability and immediate action is required to address the deficiency.

Priority: indicates an area where action must be prioritised to address the deficiency within the timescale highlighted in the report.

Action: indicates an area where action must be taken to address the deficiency before the next inspection.

- 2.20 Observations, highlighting both good and poor practice, continue to be a feature of our reports. These may not necessarily identify compliance concerns (at the stage it is highlighted) but could indicate an inefficient or ineffective process that the SRO may wish to review, or a weakness that, if not addressed, could lead to non-compliance in the future.

- 2.21 Where we identify important systemic or novel issues, these will be shared with the relevant government department or national working groups to ensure both good and poor practice is highlighted appropriately.

Highlighting good practice

- 2.22 During inspections of Councils and other public authorities, Inspectors often encounter well written policy and procedural documents. Where these are seen to be the most helpful, they have been written in an easy to digest format, perhaps with helpful examples of the types of investigative or enforcement scenarios that will be meaningful to their readers. Less helpful are the policies which simply regurgitate large sections from the relevant Codes of Practice or contain legalese.
- 2.23 Where Inspectors identify good examples of these documents, they will often ask if the relevant public authority is willing to share them with others who might be struggling to find the right format. It is always helpful for a public authority to make its internal guidance documents available, where this is possible, on its website. This is in the spirit of openness with local residents or those members of the public who may find themselves under the eye of other, perhaps national, organisations.

Raising concerns with IPCO

- 2.24 In our 2019 report, we set out the process for making a disclosure to IPCO as enabled by the information gateway set out in section 237 of the IPA. This enables both current and former employees of the public authorities which we oversee to raise with us any serious concerns they have. This process is now published on our website.⁸
- 2.25 In 2021, we received two new disclosures, both of which involved allegations concerning the use of investigatory powers by local authorities. Following investigation, the allegations in both cases were not substantiated.
- 2.26 As set out in our 2020 report, we received one new disclosure in 2020 which we were unable to investigate due to the Covid-19 pandemic. This has now been resolved with the allegations against a government department not substantiated.

8 See: <https://www.ipco.org.uk/publications/policy-documents/>

3. Relevant litigation in 2021

Overview

- 3.1 The powers that the Investigatory Powers Commissioner (IPC) oversees and the powers upon which the Office for Communications Data Authorisations (OCDA) takes decisions can all be subject to direct and indirect challenge in the UK courts and the European Court of Human Rights. This chapter sets out the legal developments that have had a bearing on either the Investigatory Powers Commissioner's Office (IPCO) or OCDA in 2021.

Technology Environments (“the MI5 data handling”) case

- 3.2 Since 2019, we have reported on the compliance problems identified in a certain technology environment at MI5, including the response to those problems by MI5, the Home Office and IPCO. In January 2020, Liberty and Privacy International brought a new claim in the Investigatory Powers Tribunal (IPT) against MI5 in relation to this matter (“the MI5 data handling claim”). The claimants alleged (among other things) that MI5 had failed fully and frankly to disclose the absence of certain safeguards within the technology environment to the Secretary of State and to Judicial Commissioners when applying for warrants and that the Secretary of State had failed adequately to investigate the deficiencies within the environment in the context of deciding whether to issue warrants. The claimants also applied to amend and re-open a separate, existing claim regarding MI5's handling of bulk personal datasets (BPD) and bulk communications data (BCD) (“the BPD/BCD claim”) on the basis of the deficiencies that existed within the technology environment during the period at issue. In February 2020, that application was stayed pending determination of the MI5 data handling claim and the issue of remedies in the BPD/BCD claim was adjourned.
- 3.3 In July 2021, the IPT decided to make a statutory request for assistance of the IPC, seeking to confirm whether any further potentially relevant material was held by IPCO. In response to that request, we provided a number of potentially relevant documents to the Tribunal in December 2021. The substantive hearing in the MI5 data handling claim took place in July 2022 with the judgment awaited.

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

- 3.4 In 2018, Mr Eric Kind was offered a post with IPCO subject to obtaining developed vetting (DV) security clearance. On 26 March 2021, the Divisional Court held that while the decision to refuse Mr Kind's application for clearance was rational and respected his human rights, it was unlawful on the grounds that the process had been procedurally unfair. Accordingly, the Court quashed that decision.⁹

9 See: *R (on the Application of Kind) v Secretary of State for the Home Department* [2021] EWHC 710 (Admin)

- 3.5 Although the IPC is confident that the IPCO recruitment and vetting process is independent in practice, following this judgment he wrote to the Home Office to enquire what steps the Government was taking to ensure that others who were offered employment by IPCO could have confidence in the fairness of the process. He also invited the Cabinet Office to conduct a policy review of the arrangements to see if any changes should be made.
- 3.6 In the light of this, the Home Office has conducted a lessons learned exercise and revised its vetting processes to ensure that, should a case raising similar complex and unusual circumstances be encountered again, that process should be procedurally fair. The Cabinet Office has accepted the suggestion that it carry out a policy review of the vetting arrangements for IPCO's staff. We are reassured that the issues have been understood and that options are currently being considered and will report further on this in our next annual report.

Big Brother Watch and others v United Kingdom

- 3.7 On 25 May 2021, the Grand Chamber of the European Court of Human Rights handed down its judgment in *Big Brother Watch and others v United Kingdom*. This consisted of a challenge to the bulk interception regime as operated under the Regulation of Investigatory Powers Act 2000 (RIPA).¹⁰ We had already adapted, and intensified, our approach to the inspection of bulk interception (BI) in the light of the first instance judgment (as set out in our 2020 report)¹¹ and we will continue to adjust our approach to take account of the Grand Chamber's judgment.

Legal principles

- 3.8 The judgment included some important legal principles which will govern our approach to future inspections.
- 3.9 First, the Court held Article 8 ECHR applies at every stage of the BI process, although the degree of interference increases as the process progresses. This underlines the importance of recommendations we have made to the Government Communications Headquarters (GCHQ) about the need to justify the necessity and proportionality of any BI process which increases the likelihood of data being seen by an analyst, even if it does not directly result in selection for examination (see from paragraph 10.14).
- 3.10 Second, the Court held that the six minimum safeguards required for a targeted interception regime to comply with the ECHR set out in *Weber and Savaria* needed to be adapted to reflect the specific features of a BI regime; technology had developed in the 10 years since *Weber* and BI is, in any case, different from targeted interception in several important respects.
- 3.11 Third, as a result of the above findings, the Court set out the eight minimum requirements for a BI regime to comply with ECHR. The legal framework must clearly define:
- i) the grounds on which BI may be authorised;
 - ii) the circumstances in which an individual's communications may be intercepted;
 - iii) the procedure to be followed for granting authorisation (see below);

¹⁰ See: <http://www.bailii.org/eu/cases/ECHR/2021/439.html>

¹¹ Annual Report of the Investigatory Powers Commissioner 2020 (from paragraph 11.24). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

- iv) the procedures for selection for examination of intercepted material;
 - v) the safeguards governing sharing of that material with other parties (see below);
 - vi) the safeguards governing retention, storage and deletion of the material;
 - vii) the supervision by an independent authority (i.e., IPCO) of compliance with i) to vi) above; and
 - viii) the independent *ex post facto* review of that compliance (e.g., by IPCO and the IPT).
- 3.12 Fourth, the Court was not persuaded that what is now called secondary data (metadata) is necessarily less intrusive than content; as such, the above eight principles also applied to the interception, retention and searching of secondary data, although they need not necessarily be applied identically.

Breaches of Article 8 and Article 10 ECHR

- 3.13 Setting aside the lack of judicial approval for BI warrants (which has been rectified as it is now required under the IPA), the Court found two breaches of Article 8 ECHR under condition iii) above.
- 3.14 First, warrant applications did not include an indication of the categories of selectors to be employed, which meant the necessity and proportionality of those selectors could not be assessed at the authorisation stage.
- 3.15 Second, the use of any “strong selector” referable to an identifiable individual (such as an email address or telephone number) must be justified and that justification subject to internal prior approval, providing for separate and objective verification of whether the justification meets the necessity and proportionality tests. The BI regime did not require internal prior approval to use such selectors to examine intercepted material and therefore breached Article 8 ECHR.
- 3.16 The Court also found that the BI regime under RIPA breached Article 10 ECHR, on the basis that the use of selectors to examine confidential journalistic material was not subject to independent prior approval (e.g. by a Judicial Commissioner) and that, when such material was obtained, there was also no independent approval of its retention and examination.

International sharing

- 3.17 For the first time, the Court set out the safeguards which must apply to the sharing of intercepted material with foreign states or international organisations:
- i) the circumstances in which sharing may take place must be clearly set out in domestic law;
 - ii) the transferring state must ensure the receiving state has in place safeguards capable of preventing abuse and disproportionate interference in handling the data, in particular secure storage and a restriction on onward disclosure – although this does not mean the safeguards in the receiving state must be directly equivalent to those in the transferring state;
 - iii) confidential material must be subject to heightened safeguards; and
 - iv) international sharing must be subject to independent control.

- 3.18 The BI regime under RIPA was held to comply with these standards. The Court attached particular weight to the oversight of sharing by the then Interception Commissioner, underlining the importance of our continued work in this area.
- 3.19 We will take the Court's guidance into account when overseeing the sharing of warranted data with overseas partners where this engages our responsibilities.

Implications in the light of the judgment

- 3.20 As of the end of 2021, we were discussing with the Government:
- i) what changes are necessary to GCHQ's regime for justifying the necessity and proportionality of the various stages of the BI process and its approach to warrant applications, in the light of the Article 8 breaches identified above;
 - ii) what changes are necessary to achieve independent prior approval of the use of selectors to examine confidential journalistic material and its subsequent retention; and
 - iii) to what extent those changes will include secondary data as well as content, given the Court's finding that the essential safeguards above also apply to secondary data.
- 3.21 Given the technical complexities of the BI systems and the likely need for legislation, implementing the required change will take some time. However, we anticipate changes will be made before or shortly after the end of 2022.

Privacy International v Investigatory Powers Tribunal

- 3.22 In January 2021, the Divisional Court handed down its judgment in *Privacy International v Investigatory Powers Tribunal* (the "Malware" case),¹² a challenge concerning whether a warrant issued under section 5 of the Intelligence Services Act 1994 (ISA) could permit the authorisation of "thematic" computer network exploitation (i.e. "hacking") in respect of an entire class of people or an entire class of such acts. The challenge related to the law prior to the commencement of the IPA; such activity would now generally be equipment interference and governed by Part 5 of the IPA.
- 3.23 Privacy International had applied for judicial review of the conclusion reached by the IPT on one of the 10 issues of law on which it was asked to rule. The IPT's conclusion had been:
- "A section 5 warrant is lawful if it is as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable, and it need not be defined by reference to named or identified individuals."*
- 3.24 The Divisional Court agreed that the property covered by a section 5 warrant needed to be "objectively ascertainable" but departed from the IPT's reasoning and meaning of this concept.
- 3.25 First, the Court held that the requirement for specificity applied to the warrant itself (i.e. the instrument produced by the Secretary of State), rather than the application for the warrant and therefore could not be intended to inform the Secretary of State's decision making:

12 *Privacy International v Investigatory Powers Tribunal* [2021] EWHC 27 (Admin)

“Section 5 does not lay down requirements about the application for the warrant, but as to the content of the warrant itself, which is the Secretary of State’s document.”

- 3.26 Second, the Court set out the sense in which the property covered by a section 5 warrant should be “objectively ascertainable”. Having reviewed the authorities on the common law’s aversion to “general warrants”, the Court concluded:

“It is a fundamental right of an individual under the common law that he or she should not be apprehended, or have property seized and searched, save by decision of the person legally charged with issuing the warrant. Expressed in modern legal language, a general warrant is one which requires the exercise of judgment or discretion by the official executing the warrant as to which individuals or which property should be targeted. It follows that a general warrant gives rise to an unlawful delegation of authority by the legally entrusted decision-maker to the executing official. This unlawful delegation breaches a fundamental right.”

- 3.27 Section 5 itself requires that the property to be interfered with is “specified” on the face of the warrant. Applying the doctrine of legality,¹³ the Court concluded that Parliament deliberately used the word “specified”, rather than “of a general description” or “described”, and as such the common law presumption that general warrants are unlawful was not overridden by the language of section 5. Therefore, section 5 could not permit the issue of a “general warrant” as defined by the Court.

- 3.28 For that reason, the crucial test to apply when evaluating the lawfulness of section 5 warrants was:

“Whether the warrant is on its face sufficiently specific to indicate to individual officers at GCHQ...whose property, or which property, can be interfered with, rather than leaving it to their discretion.”

- 3.29 Shortly after the judgment was handed down, we conducted a full review of all live section 5 warrants. Our findings are set out in the chapters covering MI5, the Secret Intelligence Service (SIS) and GCHQ. In summary, a number of warrants were identified as potentially inconsistent with the requirements of the judgment, or otherwise requiring improvements to their specificity in the light of the judgment. All such warrants were cancelled by the applicant authority and revised versions submitted to the Secretary of State for approval. (Section 5 warrants are not subject to the double lock, i.e. these are not subject to prior approval by a Judicial Commissioner. However, they do fall within our inspection remit).

- 3.30 The case has since been remitted to the IPT by the Divisional Court to apply the revised test to the Claimants at the material time. In November 2021, the IPT requested our assistance to verify, so far as possible, the accuracy of the searches carried out by GCHQ in relation to search terms provided by Privacy International. The IPC sent two Inspectors to GCHQ to oversee the re-running of all the searches previously carried out in-person. This enabled the Inspectors to confirm to the IPT in December 2021 that the results of the searches in respect of Privacy International, as disclosed to the Tribunal, were accurate. On this basis, the IPT was “satisfied that the complainant, Privacy International, was not at any material time, subject to any conduct which is not permitted to be authorised by a warrant under section 5 of the ISA in accordance with the judgment of the Divisional Court”.¹⁴

¹³ *R v Secretary of State for the Home Department ex p Simms* [1999] UKHL 33

¹⁴ *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ* [2022] UKIPTrib 1

Provision of Material to the Investigatory Powers Tribunal

3.31 In October 2021, the IPT handed down its judgment on the “IPCO issue”.¹⁵ That issue relates to “the mechanisms that the Tribunal should use when it seeks statutory assistance from the IPC under section 232(1) of the IPA”. Section 232(1) of the IPA states:

“A Judicial Commissioner must give the Investigatory Powers Tribunal all such documents, information and other assistance (including the Commissioner’s opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require –

(a) in connection with the investigation of any matter by the Tribunal, or

(b) otherwise for the purposes of the Tribunal’s consideration or determination of any matter.”

3.32 “The IPCO issue” arose following IPCO’s provision of certain documents to the IPT in the context of the proceedings which have become known as “the Third Direction” case concerning MI5’s guidelines on agents who participate in criminality.¹⁶

3.33 “The IPCO issue” concerned the correct approach that should be taken by the IPT and IPCO at three stages relating to a request for statutory assistance:

- Stage 1 – whether there should be notification and/or submissions on the scope/terms of the request;
- Stage 2 – whether there should be an opportunity for HMG to review any material identified by IPCO prior to transmission to the IPT for (i) legal privilege; (ii) sensitivity; and (iii) relevance; and
- Stage 3 – the supply of the material by IPCO to the IPT.

3.34 The IPT declined to issue general guidance as to the approach at Stage 1. However, the IPT confirmed that, although it was under no general legal obligation to do so, on the facts of a particular case fairness may require notification of a request for assistance from IPCO to the parties. The Tribunal also recognised that there may be circumstances where it would be appropriate and desirable to seek the input of parties in relation to the scope of the request.

3.35 We occasionally receive material from public authorities which is subject to legal privilege. For example, this can be included in application paperwork or it may be encountered during an inspection. A public authority may voluntarily provide IPCO with legal privilege material on a limited waiver basis as a means to explain its approach in a matter. Access to such material is of huge benefit to the oversight of investigatory powers. However, it was necessary for the IPT to consider how legal privilege material held by IPCO (but belonging to public authorities) should be treated following a request for statutory assistance from the IPT. In relation to Stage 2, the IPT therefore summarised the procedure it envisaged would usually be followed:

“(1) The Tribunal makes its request to the IPC.

(2) IPCO collates the material that is covered by the request.

15 *Privacy International and others v Secretary of State for Foreign and Commonwealth Affairs and others* [2021] UKIPTrib IPT_17_86_CH.

16 [2021] EWCA Civ 330.

(3) IPCO flags up any material that is arguably subject to the Respondents' LPP.

(4) IPCO discloses the unflagged material to the Tribunal but asks the Tribunal for its directions in relation to the flagged material.

(5) The Tribunal asks IPCO to provide the flagged material to the Respondents to check for LPP.

(6) If the Respondents do assert LPP in relation to any material, it will not be disclosed to the Tribunal but the Respondents must explain in writing on what grounds the claim to LPP is made.

(7) If there remains a dispute about LPP, the Tribunal will adjudicate on it, if necessary with a different panel constituted to consider the issue of LPP. To the extent that this adjudication can take place in OPEN, it will be. To the extent that it cannot be, it will be conducted in CLOSED, with the assistance, as appropriate, of [Counsel to the Tribunal]."

- 3.36 We welcome the clarity provided by the IPT as it should give public authorities confidence that legal privilege material that has been provided to us will be protected.
- 3.37 The IPT confirmed that there would be no review of material by the Government for sensitivity or relevance prior to its receipt.

Operation VENETIC

- 3.38 Operation VENETIC was the National Crime Agency (NCA) operation to penetrate the encrypted and supposedly secure Encrochat communications platform. The NCA applied for a targeted equipment interference (TEI) warrant from IPCO for this purpose. 2021 saw the beginning of significant litigation concerning this operation. A major area of focus has been whether the conduct to penetrate the Encrochat platform constituted or included the interception of "live" or stored communications. While the produce of a TEI warrant can be admitted in evidence, the warrant can only authorise conduct in respect of stored communications. This is in contrast with a targeted interception warrant which could authorise the interception of "live" communications, but its product is subject to a statutory restriction preventing it from being admitted as evidence. In *R v A, B, C, D* the Criminal Division of the Court of Appeal held that the conduct in question was in respect of stored communications.¹⁷ Operation VENETIC and the associated TEI warrants remain the subject of live criminal and civil proceedings. We will provide an update in our next Annual Report.

4. Protecting confidential or privileged information

Overview

- 4.1 The Investigatory Powers Act 2016 (IPA) and its Codes of Practice provide additional safeguards for certain forms of confidential and legally privileged information. Judicial Commissioners have a statutory role in authorising and overseeing the acquisition and retention of such material. Safeguards are also set out in the Police Act 1997, the Regulation of Investigatory Powers Act 2000 (RIPA),¹⁸ the Covert Surveillance and Property Interference Code of Practice and the Covert Human Intelligence Sources Code of Practice to protect confidential and privileged information acquired from the use of surveillance, covert human intelligence sources (CHIS) and property interference.

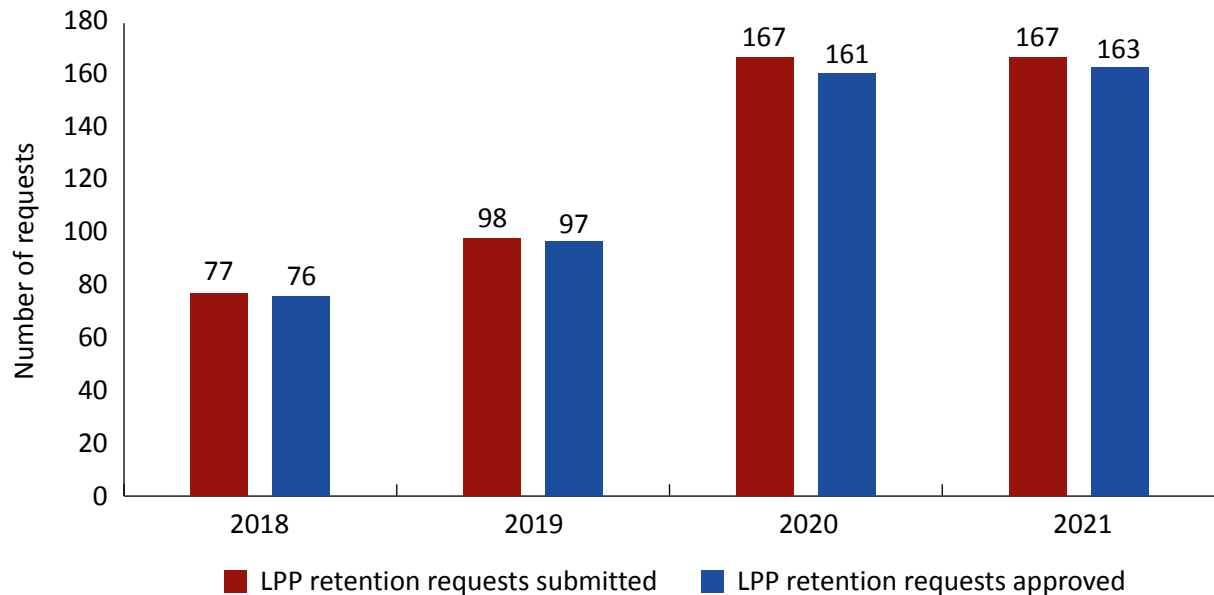
Legal Professional Privilege (LPP)

- 4.2 Legal Professional Privilege (LPP) protects against the disclosure of confidential communications and other material attaching to such communications. It enshrines the right to seek legal advice and conduct litigation in confidence. Material subject to LPP may include conversations and 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 third party.
- 4.3 In all applications, we expect consideration to be given to the likelihood of obtaining material subject to LPP. We expect consideration to be given to the public interest in protecting the confidentiality in privileged communications balanced against the public interest in obtaining the material. We would also expect to see how any material will be handled if it is obtained.
- 4.4 In 2021, we became concerned that law enforcement agencies (LEAs) were not setting out in full their considerations on the likelihood of obtaining material subject to LPP. In some cases, we had concerns that the likelihood of obtaining such material was underestimated within the application. While it was not the purpose of the application to obtain legal privilege material, it was clear the investigation involved situations where legal professionals were likely to be engaged. We have raised this with the relevant LEAs and this has been, and continues to be, an area of focus for Judicial Commissioners and Inspectors.
- 4.5 In the event that public authorities do obtain LPP material in their exercise of investigatory powers, they must inform the Investigatory Powers Commissioner's Office (IPCO) if they wish to retain that material for a purpose other than destruction. When making their decision as to retention, the Judicial Commissioners will take into account the material, its proposed use and the handling conditions in order to determine whether the public interest in retaining it outweighs the public interest in the confidentiality of the material.

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

- 4.6 In 2021, 167 applications were made in relation to the retention of LPP material. Of these, 163 were approved.

Figure 4.1 Number of requests submitted and approved for the retention of LPP material, 2018 to 2021



Confidential journalistic material and sources of journalistic information

- 4.7 Journalistic freedom is protected under Article 10 (freedom of expression) of the European Convention on Human Rights. We would expect all relevant applications to consider the necessity and proportionality of any request in that context. We expect these applications to be rare.
- 4.8 Confidential journalistic material and sources of journalistic information are subject to specific safeguards, which are designed to respect the freedom of the press. All applications made under RIPA and IPA should set out whether the purpose of the application is to obtain confidential journalistic material or identify sources of journalistic information. All applications should also state the likelihood of such material being obtained.
- 4.9 The acquisition of communications data (CD) relating to journalists and sources of journalistic information is covered in Chapter 13.
- 4.10 Looking at the use of other powers, our inspections have not identified any concerns in relation to handling of journalistic material. The number of applications to acquire journalistic material in other powers will always be substantially smaller than those seeking to acquire CD and all warrants 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 is no different. However, we expect additional consideration to be given to the confidential material that may be obtained and to the public interest in safeguarding freedom of the press to satisfy the threshold in this context. We would also expect applications to give some consideration to how confidential material will be handled and the extent to which this material is expected to be relevant to the investigation.

- 4.11 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. The enhanced procedures for obtaining confidential information include requiring the request to be authorised at a more senior level. We would expect any relevant application to include details of how this sensitive material would be protected.
- 4.12 In 2021, 13 applications were made for warrants under the IPA where the purpose was to obtain material which the intercepting agency believed would relate to confidential journalistic material. Applications relating to sources of journalistic information might either be for warrants, which must be considered by a Judicial Commissioner, or for CD, which would also be subject to judicial approval under section 77 of the IPA. Under section 77, the Judicial Commissioner must consider the public interest in protecting a source of journalistic material. There were 13 warrant applications to identify a journalistic source and seven CD applications were considered under section 77 in 2021.

Additional safeguards for health records

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

5. Communications and engagement

Overview

- 5.1 Transparency remains one of the core values of the Investigatory Powers Commissioner (IPC). He is keen to use communications such as this report and engagement with interested parties to enhance understanding of the work of both the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA).
- 5.2 In the spring of 2021, IPCO launched a new, user-friendly website.¹⁹ The website includes information about the work of the organisation, the functions of the Judicial Commissioners and staff, the methodology used by the Inspectorate and an explanation of investigatory powers. The website also serves as a resource for relevant publications, guidance and news items.
- 5.3 Throughout the year, the IPC regularly provided comments and information to media outlets in response to queries about the use and oversight of investigatory powers; in particular, we proactively engaged with the media when publishing our Annual Report. Ahead of publication of the 2020 report, the IPC gave an interview to Joshua Rozenberg for the Law Society Gazette, which was published in November 2021.²⁰
- 5.4 In 2020, we introduced a stakeholder engagement strategy but, with shifting priorities in the light of the pandemic, engagement with those interested in our work was less frequent than we had hoped. Throughout 2021, we therefore refocused our efforts and introduced a more consistent rhythm of engagement. This included regular meetings with non-governmental organisations (NGOs), public authorities, international oversight bodies and other independent bodies.
- 5.5 The full schedule of the IPC's engagements is found at Annex D.

UK engagement

Non-governmental organisations (NGOs)

- 5.6 We began the year with a virtual roundtable event for NGOs. The IPC and our Chief Executive were joined by organisations focused on privacy and security, including Big Brother Watch, Liberty, Privacy International and Reprieve. The IPC outlined our ways of working, reporting processes and objectives for future engagement. A discussion followed with useful contributions from each of the NGOs, providing valuable considerations for how we can further our transparency and enhance our oversight approaches.

¹⁹ See: www.ipco.org.uk

²⁰ "Secrets and spies", The Law Society Gazette, Joshua Rozenberg, 15/11/21. See: <https://www.lawgazette.co.uk/commentary-and-opinion/secrets-and-spies/5110485.article>

- 5.7 Although the roundtable event proved extremely useful, it became clear that each NGO had differing priorities and areas of focus. As such, throughout the rest of the year, the IPC and our Chief Executive met with each organisation individually so that more in-depth conversations on specific issues could be had.

Public authorities and independent bodies

- 5.8 We have continued to send a quarterly newsletter to all organisations that we oversee and regularly receive positive feedback. The newsletter includes an update from the IPC on the activities of IPCO, guidance, case studies and process updates. We have found that this is also a useful tool to share IPCO's official position on specific issues. For example, we have shared an update on our approach to oversight of social media monitoring by local authorities, including offering guidance on what is expected of organisations and encouraging the development of training and policies in this area.
- 5.9 The IPC regularly meets with public authorities and independent bodies that are interested in the work of IPCO. This engagement allows us to hear diverse and challenging views, it enables identification of areas of overlap and it enhances our understanding of the work of others. The IPC has met with representatives from a variety of public authorities and independent bodies throughout the year, such as Her Majesty's Prison and Probation Service (HMPPS), the National Crime Agency (NCA), the Information Commissioner's Office (ICO) and other government departments. Towards the end of the year, the IPC spoke to a group of lawyers from across Government and the UK intelligence community (UKIC), sharing his experience as IPC and offering insight into legal issues linked to the Investigatory Powers Act 2016 (IPA).
- 5.10 In addition to the ongoing engagement that forms their day-to-day activities, we see real value in our Inspectors joining relevant police or Government-led working groups or training events. One such event, organised by the National Police Chiefs' Council, saw a number of our Inspectors delivering a presentation on surveillance and intelligence gathering as part of a CPD accredited training session.

Others

- 5.11 In 2021, the IPC met with Ministers and Members of Parliament with a specific interest in our work, including the Attorney General and Foreign Secretary.
- 5.12 Together with one of our Chief Inspectors, our Chief Executive met with the News Media Association and the Media Lawyers Association following an exchange of correspondence in 2020. The media organisations were particularly interested in better understanding our data on access to information relating to journalistic sources and our level of transparency. They acknowledged that previous Annual Reports had made progress in this regard but thought that more could be explained. Following the meeting, we reviewed how we presented our data in our 2020 report and have followed the same model in this report.

International engagement

- 5.13 In October 2021, the IPC and Chief Executive attended the European Intelligence Oversight Conference. This took place in Rome with representatives from 14 other European countries. Attendees reflected on recent court judgments that have had an impact on oversight activities across Europe. Officials from a smaller number of participating countries, including one of our Inspectors and a member of the Technology Advisory Panel

(TAP), also met separately in 2021 to explore how technology and other influences can have an impact on oversight.

- 5.14 In November 2021, the IPC and Chief Executive joined the virtual Five Eyes International Oversight Review Council (FIORC).²¹ Although this did not carry with it the huge advantages of meeting people in-person, there was still real value in sharing thoughts on how oversight bodies can keep track of technological advances and how the work of each body continues to develop and grow, as well as to hear back from the three working groups set up after the London conference in 2019.

21 See: <https://www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Executive%20Summaries/2022/Executive%20Summary%20-%202021%20FIORC%20Annual%20Meeting.pdf>

6. Technology Advisory Panel

Foreword from Sir Bernard Silverman, Chair of the TAP

The ongoing and changeable nature of the Covid-19 pandemic has continued to provide challenges to how the Technology Advisory Panel (TAP) operates. Nevertheless, the TAP has remained fully active during 2021. The Panel has continued to receive briefings from other organisations in order to remain well informed about the areas on which its advice may be required. Some of these have been remote, others in-person, when safe and practicable to do so. These briefings have been from the UK intelligence community (UKIC), the West Midlands Police and the National Crime Agency (NCA) among others and have involved many fruitful discussions. The Panel has, as always, found such sessions extremely useful, and we would like to thank all those who have willingly shared their time and expertise with us.

As the report indicates, the Panel has found a range of alternative ways of working to mitigate the impact of the pandemic on its activities, to ensure the ongoing provision of technical advice, papers and education for the Investigatory Powers Commissioner's Office (IPCO). Regular meetings and discussions have continued mostly online together with (where feasible and permitted) meetings between secure locations using appropriate remote conferencing technology to allow classified topics to be discussed. I would like to record my thanks to those agencies and organisations which have facilitated such meetings.

It has been good to welcome two new Panel members in the course of the year (Professors Richard Mortier and Sarvapali Ramchurn). Both bring valuable relevant expertise to add to the Panel.

In addition to its work with IPCO itself, the TAP has had ongoing liaison with other jurisdictions and oversight bodies internationally, including the Five Eyes and the European Intelligence Oversight networks, where it has worked alongside IPCO on topics of mutual interest to the UK and other partners.

Overall, the TAP has continued to provide its very important function which is to ensure that the Investigatory Powers Commissioner (IPC) has access to the best possible scientific and technological advice and has done so on very limited resource.

This will be my final report as TAP Chair as I will be standing down from the role in 2022. It has been a great pleasure to establish the TAP and to lead its work, but now is the time to hand over to a successor. I am delighted that the IPC, Sir Brian Leveson, has appointed as my successor Professor Dame Muffy Calder, currently a member of the TAP, and I wish her every success as she takes on the role of Chair. I would also like to record my sincere thanks to the Secretary of the TAP and to all the members for their unfailing enthusiasm and support.

I would again like particularly to highlight my thanks to Sir Brian Leveson, and all the Judicial Commissioners and IPCO staff, for such a positive and constructive relationship. This has given individual Commissioners the facility to ask questions on relevant topics, has enabled the TAP to collaborate with IPCO during inspections and allowed access to IPCO staff meetings to give presentations on technological topics of general interest to them, and in helping the TAP develop its

independent work programme, both on topics (the majority of its work) where it provides advice at the specific request of the Commissioner, and where it initiates advice of its own volition.



Sir Bernard Silverman FRS, Chair of the Technology Advisory Panel

Remit of the Technology Advisory Panel

6.1 The TAP was set up under the Investigatory Powers Act 2016 (IPA – “the Act”) (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 developments of techniques to use investigatory powers while minimising interference with privacy. In the definition of the panel’s remit, “technology” is taken to be interpreted broadly, to include all relevant areas of science and mathematics. The remit of the Panel does not extend to consideration of matters of law, partisan politics or moral philosophy. The TAP is not a decision-making body and its advice cannot constrain any decision of the IPC or of any part of the Government.

Membership of the TAP

- 6.2 The TAP is chaired by Sir Bernard Silverman FRS, formerly Chief Scientific Adviser to the Home Office and Emeritus Professor of Statistics at Oxford University. Panel members during 2021 were:
- Professor Dame Muffy Calder, Vice-Principal and Head of the College of Science and Engineering at Glasgow University, and previously the Chief Scientific Adviser for Scotland;
 - Professor Derek McAuley, Professor of Digital Economy in the School of Computer Science at the University of Nottingham;
 - John Davies, who has an extensive technical background in both government and private industry roles;
 - Daryl Burns, who has worked in cryptography and cyber security for over 30 years and was Deputy Chief Scientific Advisor for National Security; and
 - Professor Niall Adams, Professor of Statistics, Imperial College London whose research interests are in computational statistics, machine learning, and data science (Professor Niall Adams resigned from the Panel in May 2021).
- 6.3 During 2021, Professors Richard Mortier and Sarvapali Ramchurn (Gopal) have joined the panel:
- Richard is Professor of Computing and Human-Data Interaction at Cambridge University, and President of Christ’s College. Current work includes platforms for privacy preserving personal data processing, “Internet-of-things” (IoT) security, smart cities, and machine learning in knowledge management; and
 - Gopal is Professor of Artificial Intelligence, Turing Fellow, and Fellow of the Institution of Engineering and Technology. He is Director of the UKRI Trustworthy Autonomous Systems hub and Co-Director of the Shell-Southampton Centre for Maritime Futures. His research is about the design of Responsible Artificial Intelligence for socio-technical applications

including energy systems and disaster management. This involves applying techniques from Machine Learning, Data Science, and Game Theory.

- 6.4 Sir Bernard Silverman, the inaugural Chair of the TAP, has expressed his intent to step down from the panel during 2022. The IPC has appointed panel member Professor Dame Muffy Calder as the new Chair of the TAP. Sir Bernard has firmly established and populated the Panel since his appointment to the new role in 2017 and is leaving it in a strong position to continue its independent advice and support to the IPC and his team.
- 6.5 TAP members are remunerated at an agreed daily rate. During 2021, members contributed an average of 15 days each to TAP duties. The TAP is supported by a Secretary who is a part-time (50%) civil servant.
- 6.6 In the interests of transparency, the TAP aims to publish as much information openly as possible. The biographies of all TAP members are shown on the IPCO website.²² Furthermore, a Register of Interests of panel members is published on the website and is reviewed on a quarterly basis.²³ Where security considerations allow and subject to the agreement of the IPC, advice and guidance given to the IPC and his staff will also be published openly.

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

23 See: <https://www.ipco.org.uk/publications/technology-advisory-panel/>

TAP Strategy

- 6.7 A TAP Strategy was compiled in April 2021 and has been published on the IPCO website. This is included in full below.

A Strategy for the Technology Advisory Panel

Role of the Technology Advisory Panel

In the context of the use of investigatory powers, the role of the Investigatory Powers Commissioner's Technology Advisory Panel (TAP) is to advise about:

- i) the impact of changing technology;
- ii) the availability and developments of techniques to minimise interference with privacy; and
- iii) the use of technology to support the development and effectiveness of the Commissioner's Office (IPCO).

Strategic workstreams: the six Rs

To fulfil its role the TAP carries out six concurrent strategic workstreams.

1. **Recognise** needs, by ensuring the TAP is collectively well briefed on i), ii), and iii). This involves regular engagement with the public bodies that exercise investigatory powers, as well as attention to the relevant academic research and more general horizon scanning.
2. **Respond** to formal and informal requests from the Commissioner, including those made on the Commissioner's behalf.
3. **Raise** issues proactively that are of concern to us and/or involve areas where we believe the Commissioner needs advice or additional support.
4. **Review** our relative and absolute efforts in the Respond and Raise modes, and between the concerns of i), ii), and iii).
5. **Reflect** on our effectiveness and expertise (including the composition of our membership) and evaluate our processes and outputs.
6. **Reach** out by leading and participating in activities with others interested in aspects of investigatory powers within the TAP's remit. When appropriate, proactively stimulate and coordinate discussions on topics of mutual interest. Publish advice or other documents where security classification permits.

This TAP Strategy complements the published TAP Working Protocol.²⁴ The Working Protocol sets out the broad parameters within which the TAP operates. The Strategy provides more detail and focus. It is not intended in any way to contradict or supersede the Working Protocol.

24 See: <https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Technology-Advisory-Panels-Working-Protocol-with-the-Investigatory-Powers-Commissioner-January-2022.pdf>

Activities undertaken by the TAP and its members during 2021

Coronavirus and lockdown

6.8 Unsurprisingly this has continued to impact the TAP's activities. Though during the year it has become somewhat easier to make in-person visits, there are still several restrictions in particular limitations on numbers. A number of planned activities are still largely postponed including proposed visits to the technical areas of the Government Communications Headquarters (GCHQ), MI5 and the Secret Intelligence Service (SIS). The TAP continues to meet through a mixture of in-person and virtual means and to discuss topics over email, but virtual meetings limit the classification level of any discussions. Occasional in-person participation in IPCO inspections (some by secure video conferencing facilities) resumed in May 2021. It remains to be seen how changing Covid-19 restrictions at the end of 2021 will impact on the Panel in the coming months.

Review of the Investigatory Powers Act 2016

6.9 TAP members participated in discussions in relation to the five-year review of the IPA. This involved working with IPCO and the Home Office on specific sections of the Act including the paragraphs laying out the statutory basis for the TAP and also other paragraphs where the TAP had relevant input based on the Panel's activities. At this stage, no major amendments in regard to the TAP have been identified.

Meetings

- 6.10 Formal panel meetings, mostly online, took place in January, March, April, June (in-person), July, October and November 2021. All meetings and actions were formally recorded. The TAP has been fortunate to be able to use secure video conferencing facilities elsewhere on occasion to permit discussions requiring a higher classification level. We are grateful to Police Scotland and GCHQ for enabling this to happen.
- 6.11 Formal biannual meetings (as laid down in the Working Protocol between the TAP and IPCO) between the IPC and the Chair of the TAP took place in May 2021 and November 2021. The IPC's Chief Executive was also present. Both meetings were formally recorded. The purpose of these meetings is to have a formal set up for ensuring meetings take place, to reflect on the TAP and its past and planned activities.
- 6.12 TAP members attended a panel meeting/discussion on the Ethics of Artificial Intelligence (AI), arranged by GCHQ, for which Dame Muffy Calder was a panel member.
- 6.13 TAP members joined in a discussion with IPCO members on Artificial Intelligence and Machine Learning (AI/ML), as part of IPCO's input to a wider Five Eyes Oversight Intelligence Review Council (FIORC) initiative. TAP members also contributed to a Five Eyes paper on AI which was finalised in March 2021.
- 6.14 The TAP Chair attended an Equities Process inspection by video conference. Currently the Equities Process does not have a specific statutory basis, and the inspection takes place at the request of the Director of GCHQ. However, it is anticipated that the statutory footing of this oversight will be formalised in the future.
- 6.15 TAP members participated in a number of IPCO inspections including at GCHQ, MI5 and West Midlands Police. At the request of the IPCO Inspectorate and Legal Team, TAP

members have also been involved in technical discussions with GCHQ on specific issues arising from inspections.

- 6.16 Members of the TAP attended relevant elements of the Policing and Security conference held online in March 2021.
- 6.17 The National Security and Intelligence Review Agency (NSIRA), the Canadian equivalent of IPCO, held useful discussions with the panel on the TAP's roles and responsibilities to assist with their plans for developing a new internal function to advise on within NSIRA. Other Five Eyes bodies have also expressed an interest in finding out more about the TAP and to this end, a short unclassified document detailing the roles and responsibilities of the TAP was created and made available to these international colleagues.

Publications

- 6.18 The TAP Strategy was published on the IPCO website. Regular checks ensure that all elements of the TAP strategy are being considered at Panel meetings and through the TAP's activities.
- 6.19 The TAP aims to be as transparent as possible and though much of the advice given is at too high a classification level, the TAP will, wherever feasible and with the agreement of the IPC, publish unclassified documents or guidance on the IPCO website. An unclassified paper on Encryption Technologies, redacted from one originally compiled for IPCO, was published on the IPCO website this year. Two shorter entries, on data provenance and a crypt primer, were also made available publicly on the IPCO website. Other papers are to be added to the website in due course.
- 6.20 A paper describing the constitution, role and activities of the TAP was created and shared with the FIORC in advance of the November 2021 online FIORC conference, part of which was attended by the TAP Chair.

Technical support and advice

- 6.21 Technical support was provided to several inspections and other IPCO discussions. TAP members accompanied visits to the West Midlands Regional Organised Crime Unit/ Technical Intelligence Development Unit (ROCU/TIDU), various inspections at GCHQ and MI5. A number of ad hoc queries by Inspectors and Judicial Commissioners were addressed informally. Examples of the queries addressed to the TAP included:
- a request for TAP advice was received from Sir Brian Leveson in relation to some proposed developments in the use of bulk communications data by an intelligence agency. Two members of the TAP joined members of the Inspectorate to discuss the proposals and TAP advice was given to Sir Brian as part of a wider IPCO response;
 - the TAP was asked to advise on a Retention Notice (RN) proposed by an intelligence agency, and in particular on plans for data storage;
 - the TAP was asked to give technical advice in relation to communications data errors being investigated by IPCO;
 - request for TAP advice in relation to a planned change to a UKIC agency's technical environment. Two panel members had been invited to a video conference arranged by a member of UKIC. This was in relation to some previous detailed discussions and inspections relating to technical issues where the TAP had given assistance.

Various options were discussed about how to fix the old issues in relation to the proposed changes;

- the TAP was asked to provide technical support to IPCO in relation to the shift to 5G. Other questions around cellular technology have been posed to the TAP including a request to support IPCO in securing common understanding and approaches across the operational community;
- the TAP provided technical input and advice to IPCO in relation to a variation to a RN;
- to meet a request, the TAP provided IPCO with an explanation on hashing and followed this with a guidance paper for IPCO; and
- following an earlier inspection of bulk powers at an intelligence agency, the IPCO Inspectorate has requested that the TAP pursue a specific topic and provide technical advice to the Inspectorate prior to the next inspection of these powers. Following various discussions, the TAP has created some written advice to IPCO.

6.22 IPCO's Chief Executive has tasked a member of the Panel to research what technical skills are most required for the Inspectorate and whether these can be acquired through training or the recruitment of some specifically technically skilled Inspectors.

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

- a paper on the Cloud which was written as a general guide for IPCO with a version which is due to be published on the IPCO website;
- a proposal for research into Voice Recognition. This topic was raised during TAP participation in an inspection and the TAP considered that it was a topic worthy of further research. As such the TAP has commissioned an academic (Dr Peter Bell, Reader at Edinburgh University) to carry out some unclassified research into the subject. Dr Bell is preparing a formal paper with the findings of his research;
- a paper on Metrics of Intrusion Key Concepts; and
- a letter to the IPC and accompanying paper on Digital Identity, which outlines considerations arising from the recent open consultation issued by the Department for Culture, Media and Sports (DCMS) and the Cabinet Office.

Visits, External Briefings and Liaison

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

- West Midlands Regional Organised Crime Unit (ROCU)/Technical Intelligence Development Unit (TIDU). This followed participation in an IPCO inspection, and the TAP were very pleased to explore further some of the technical work being undertaken by the TIDU;
- the TAP joined other members of IPCO for an informative technical briefing by UKIC;
- the TAP attended a briefing day given by UKIC. Though initially this was billed as a familiarisation day for the newer panel members, all the TAP attended and benefited from receiving up-to-date information and an opportunity to discuss and ask questions;
- TAP members were invited to attend a UKIC briefing on Artificial Intelligence and Machine Learning (AI/ML). This is a topic of increasing interest and likely to involve the TAP in a number of different discussions;

- TAP members were given a fascinating update by the NCA on an ongoing trial of new technology. Following this, a member of the TAP gave a detailed update to a Judicial Commissioner and one of the Chief Inspectors; and
- The TAP had a very useful meeting and discussion with Professor Jennifer Rubin, Chief Scientific Officer for the Home Office, which covered the role and activities of the TAP, focussing on a few current pieces of work.

6.25 A member of the TAP participated in a European oversight group meeting online.

7. The Office for Communications Data Authorisations

Overview

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

Managing the impact of Covid-19

7.2 A key challenge for 2021 remained the ongoing presence of Covid-19 and mitigating its impact on our operations. The revised operational structures we put in place during 2020 had placed us in a strong position to deal with further Covid-19 related restrictions: staff were able to work from home to consider the high volume of applications we received at the low Government Security Classification of OFFICIAL – SENSITIVE and we continued to maintain a safe and secure environment on both our sites to deliver work at a higher classification level.

7.3 Throughout the pandemic, we continued our regular dialogue with the authorities who submit applications to keep them up to date with our operational approach. We agreed that weekday operating hours of 8.00am to 6.00pm (weekend 8.00am to 4.00pm) for most of our higher classification work would be sufficient; this has helped us minimise our office presence and is an operating model which we are going to maintain as we go forward into 2022.

7.4 We responded effectively to the continually changing landscape of Covid-19 restrictions with no impact on our performance. Following the easing of restrictions in July, we began building up the number of staff in our offices and, working within central Home Office guidance, explored a longer-term hybrid working approach, thereby enabling the organisation and our staff to operate in the most efficient manner.

Workflow

7.5 Following the testing of our operating model at the end of 2020 by very high volumes of work, from an operational perspective we began 2021 in a strong position. We had learnt valuable lessons in managing operational workloads and were in the process of implementing tools which would enhance our resilience to deal with increased numbers of applications.

7.6 However, before these processes could fully be implemented, we began to see further increases in applications in February and March 2021. This was particularly attributed to a number of specific national law enforcement operations taking place. This unexpected

increase in applications resulted in breaches of our normal service level expectations (SLEs). We began to apply new operational resilience tools in March which helped clear the outstanding applications and enabled us to return to a position of operating within our usual SLEs.

- 7.7 From April 2021, we saw a more consistent flow of applications being received and we were pleased to deliver decisions within our SLEs for the remainder of the year. During this time, we also continued to work with the law enforcement community to help us better plan ahead and minimise potential spikes in workloads. As shown in table 7.1, by the end of the year we had considered over 240,000 CD applications, an increase of over 8% in comparison to 2020.

Table 7.1: Applications submitted to OCDA, 2019 to 2021

		2019		2020		2021	
Total applications		71,610		226,383		245,272	
Decisions made		71,208	99.4%	223,322	98.6%	242,535	98.9%
Of which	Authorised	63,688	88.9%	199,482	88.1%	222,009	90.5%
	Returned			23,596	10.4%	20,244	8.3%
	Rejected			244	0.1%	282	0.1%
Withdrawn		385	0.5%	3,051	1.3%	2,736	1.1%
Applications with no decision at year end (31 December)		17	0.0%	10	0.0%	1	0.0%

Note: 2019 figures are not wholly comparable as OCDA only became functional in March 2019.

- 7.8 Our key learning points from 2021 included the continuing importance of working closely with law enforcement agencies (LEAs) and wider public authorities (WPAs) to be able to anticipate where and when a surge in application numbers may arise and for how long, so as to align resources accordingly. In addition, our operational model enabled us to focus upon priority work with a corresponding staggering of less high priority applications at times of greatest demand.
- 7.9 The operational pressures also highlighted the importance of improving efficiency wherever possible. With support from the Home Office National Communications Data Service (NCDS), we were able to identify new IT enhancements which could speed up the applications process. This involved moving a number of WPAs away from a reliance on emailing CD applications to us and, instead, using an automated interface with our casework system. This has proved very successful in terms of the time taken to consider applications and a reduction in a number of administrative problems often seen through use of email.

Return for Rework (RfR)

- 7.10 In our 2020 report, we set out the reasons why applications are returned to the requesting authority when the Authorising Individual (AI) is not satisfied that the case for obtaining CD is fully and completely made out. The number of applications we returned for rework during 2021 is an illustration of the level of scrutiny that is applied to each and every application. Despite the ongoing pressures of the pandemic and the high volume of applications received, the data shown below provides assurance that our high quality of case consideration has remained consistent.

- 7.11 Table 7.2 highlights the primary reason for an application not being authorised and subsequently being returned to the submitting authority, namely that an AI does not believe the application meets the necessity requirements. Some of the other reasons given are more technical in nature but all relate in some way to inadequacy or lack of clarity in the information given by requesting authorities. The information on RfRs is shared regularly with law enforcement and public authorities to help them get applications right first time.

Table 7.2: Returns for Rework (RfRs) reasons, 2020 to 2021

Reason	2020		2021	
	Number of Returns for Rework	Proportion of Returns for Rework	Number of Returns for Rework	Proportion of Returns for Rework
Necessity	2,832	12%	4,389	18%
Proportionality	2,832	12%	2,988	12%
Dates/Times	2,596	11%	3,516	15%
Consequential ticked/not ticked	1,888	8%	1,383	6%
Accuracy	1,652	7%	1,922	8%
Consequential Justification	1,652	7%	1,805	8%
Attribution	1,416	6%	1,244	5%
Collateral intrusion	1,180	5%	1,000	4%
Forward facing	944	4%	952	4%
Data Type	944	4%	587	2%
Other (up to 20 categories)	5,663	24%	4,183	17%

Organisational development

- 7.12 Having only become fully operational in January 2020, much of our development has occurred under the restrictions of a global pandemic. However, we have risen to the challenges presented to us and continued to make improvements through enhancements to our systems, improving our resilience for critical functions and investing in our staff to develop their knowledge and skills in the complex and fast-moving field of CD.
- 7.13 We have initiated the next iteration of improvements to our bespoke case management system. These have been developed in conjunction with Home Office technical colleagues who specialise in CD. The changes will help mitigate against potential avoidable errors and will ultimately increase our efficiency.
- 7.14 The pandemic also highlighted the importance of contingency planning. We have now completed an end-to-end review of our existing Business Continuity Plan, refocusing on how we could continue operating in the event of the operational loss of one of our sites. Through some excellent collaboration, we have been able to factor into the plan the option for staff to access another site to complete the most sensitive work. This has increased our operational resilience to continue to fulfil our legal obligations in relation to those sensitive applications.
- 7.15 We circulated our first Operational Digest to submitting authorities in January 2021. The Digest originates in OCDA's internal practice bulletins, which have been produced to provide guidance to our authorising individuals since August 2019. The Digest seeks to

share relevant parts of that internal guidance with the wider community of Single Points of Contact (SPoCs) and Senior Responsible Officers in the public authorities. We have a unique and unprecedented UK-wide role in overseeing large volumes of applications for CD across different jurisdictions. Consequently, we need to insist on some minimum standardisation of practice and the presentation of applications for the acquisition of CD. The Digest is designed to share these expectations with public authorities.

- 7.16 In the latter part of the year, we invited some external analysis and challenge to our decision-making process through a piece of collaborative work with the Human Rights, Big Data and Technology project at the University of Essex. Professor Pete Fussey, Dr Daragh Murray and Dr Amy Stevens undertook a series of semi-structured interviews with OCDA operational staff regarding the organisation and their role. We received the research report in February 2022 and further details will be set out in our 2022 report.
- 7.17 We continued to manage staff turnover during the pandemic by completing two large recruitment campaigns which, when combined with our virtual induction programme, enabled us to onboard staff at varying grades. In addition, we used staff feedback and challenged ourselves to provide a high-quality learning and development offer to staff; this combined upskilling and refresher training on several key aspects across the CD environment and access to cross-government development programmes which helped staff develop wider skills. This important aspect of our work will continue into 2022, ensuring we have a fully staffed organisation equipped to deal with the expected increases next year.

8. MI5

Overview

- 8.1 During 2021, we conducted regular inspections across the range of investigatory powers used by MI5. This included briefings on operations conducted by MI5, detailed reviews of its internal documents and discussions on emerging capabilities and compliance risks.
- 8.2 In our 2020 report, we noted that we would review the use of different IT environments by the UK intelligence community (UKIC) for warranted data. During 2021, we built this into routine inspections in respect of the different powers at all the agencies. We will continue to do this as part of the inspection regime and will only comment specifically if there is an area to be addressed.

Findings

- 8.3 In line with previous years, there continues to be a good level of compliance across MI5 in its use of investigatory powers. However, this is the fifth year we have reported our concerns about particular weaknesses in authorisation by MI5 of directed surveillance. We have flagged this as an issue which requires urgent remedial action.
- 8.4 MI5's introduction of the ambitious "three lines of defence" model (see paragraph 8.30 below) for compliance provides a clear structure for identifying, escalating and managing risk and should be commended. Given our previous investigations into compliance problems at MI5, we are hopeful that, if properly resourced, this proactive approach will ensure that any issues are identified early, if not avoided all together.
- 8.5 We have begun a complex review of the handling of legally privileged material which has no intelligence value but is included within material that does have intelligence value and which needs to be retained. This review will span all three intelligence agencies.
- 8.6 Finally, we raised a concern in 2021 about the level of detail provided to the Home Secretary in MI5's handling arrangements to ensure that all relevant considerations are being taken into account when a decision is taken to issue a warrant. Our concern is that there needs to be more detail available to the Home Secretary as to how MI5 is discharging its obligations under section 53 of the Investigatory Powers Act 2016 (IPA). This is subject to ongoing discussions with MI5.

Covert human intelligence sources (CHIS)

- 8.7 The use by MI5 of CHIS and directed surveillance was inspected in October 2021. A separate review of Criminal Conduct Authorisations (CCAs) was conducted remotely in December 2021.

- 8.8 We found that CHIS compliance remained strong and saw good evidence that MI5 was giving due consideration to the risks involved and the appropriateness of utilising this intrusive activity.
- 8.9 With the assistance and co-operation of MI5, we are seeking a means by which all CHIS records and supporting documentation are more easily accessed by Inspectors. Currently, while all records are made available to inspection teams when requested, this sometimes occurs during an inspection week and can lead to a delay in the record being examined. Our preference is for a more comprehensive range of records being available in the first instance, with any requirement for further records being identified as part of a pre-read examination of CHIS cases. The means by which this will be achieved is being discussed.
- 8.10 We found MI5's use of CCAs for CHIS to be necessary and proportionate. We noted that there could be greater consistency in addressing proportionality in the CCA applications and recommended that this could be rectified by addressing the three points in the draft revised Code of Practice:
- whether what is sought to be achieved by the criminal conduct could reasonably be achieved by other conduct which would not constitute crime;
 - whether the criminal conduct to be authorised is part of efforts to prevent or detect more serious criminality; and
 - whether the potential harm to the public interest from the criminal conduct being authorised would be outweighed by the potential benefit to the public interest and that the potential benefit would be proportionate to the criminal conduct in question.
- 8.11 We are unable to confirm or deny whether MI5 has recruited juvenile CHIS. We are satisfied however, that MI5 has the appropriate policies and practices in place regarding the recruitment and running of juvenile CHIS and the obtaining of confidential material.

Directed surveillance

- 8.12 There continue to be particular weaknesses in MI5's authorisation of directed surveillance. For the fifth year running, we found Authorising Officers (AOs) were not evidencing that they had given sufficient regard to their responsibilities under the Regulation of Investigatory Powers Act 2000 (RIPA); in particular that they were not adding comments to their approvals to demonstrate their personal considerations of necessity and proportionality. It is best practice that AOs record these considerations. Better processes for recording the outcome and value of surveillance are also required. We recommended that MI5 develops an urgent action plan for discussion with us and we will conduct a progress review in mid-2022.
- 8.13 In relation to capability development, MI5 continues to explore new surveillance techniques to respond efficiently to diverse and hard-to-detect threats to UK national security in a manner that is RIPA compliant. This is a complex area and we found that MI5 was taking appropriate measures to expand capabilities while remaining compliant.

Property interference

- 8.14 In the light of the decision in the "Malware" judgment (see from paragraph 3.22), we reviewed all of the property warrants in force at MI5 to identify any compliance issues with the terms of the judgment. Several warrants were amended as a result of that review.

- 8.15 We reviewed a small number of property warrants in the course of routine inspections in 2021 and had no concerns about the necessity and proportionality of the conduct authorised.

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

- 8.16 MI5 continues to make use of combined warrants under Schedule 8 to the IPA. During 2021, we conducted combined inspections looking at targeted interception (TI) and targeted equipment interference (TEI) authorised under the IPA.
- 8.17 Overall we were satisfied that MI5 had achieved a high level of compliance with the IPA in relation to those warrants reviewed.

Thematic warrants

- 8.18 We examined a number of thematic warrants where applications had been made for both major and minor modifications to add new subjects and factors. All of the modifications we reviewed were properly authorised and consistently completed to a very high standard, with a clear rationale for adding or removing factors. Each modification clearly demonstrated the necessity and proportionality case as well as linking the new factor or individual to the subject and purpose of the warrant. If there was any change in potential collateral intrusion as a result of a new factor being added this was clearly addressed. There was good evidence that factors were being deleted promptly when no longer required.

Specificity of thematic warrants

- 8.19 The IPA requires that, where a thematic warrant relates to more than one subject (a group of persons who share a common purpose, for example), the warrant must name or describe as many of those subjects as is reasonably practicable. The Codes of Practice make clear that, in some cases, it may be necessary to use a "general descriptor" covering other individuals who are subject to the warrant whom it has not been reasonably practicable to name or describe at the time of authorisation. Whether it will be appropriate to use a "general descriptor" depends on a number of factors such as the speed and pace of the investigation. It needs to be made clear within the application why use of a general descriptor is justified and this is assessed on a case-by-case basis. This is a particular area of interest for Judicial Commissioners when they consider warrant applications; it also attracts specific attention on inspection.
- 8.20 MI5 has a number of these general descriptor thematic warrants. We examined many of these in detail and we tested the necessity for the general descriptor in accompanying paperwork and briefings from operational teams. We found that MI5 was using this to an appropriate standard and the cases we examined were all justified.

Use of TEI

- 8.21 MI5 informed us in 2020 that it planned to lower its policy threshold for the use of TEI in certain operational contexts. The use of TEI in those contexts enabled MI5 to establish the credibility and seriousness of the intelligence it possessed and to determine the most appropriate resolution (including taking no further action). In some cases, this resulted in a faster resolution of the investigation and less intrusion into privacy overall. We have kept this under review and our inspection provided assurance that the techniques being used were necessary and proportionate to the activities and intelligence being investigated.

Assistance to law enforcement agencies (LEAs)

- 8.22 In line with its statutory functions, MI5 has been providing technical support to some serious crime LEA investigations involving TEI. We received several briefings, both written and in-person, on this process. We have examined the authorisations which supports it as well as the use of the data and the safeguards surrounding the data that is acquired. We were satisfied that, in the cases we examined, all activity was necessary and proportionate and appropriate compliance measures were in place.

Communications data

Bulk communications data (BCD)

- 8.23 In 2021, our inspection focused heavily on amendments made to existing BCD authorisations, the justifications used to retain data for extended periods, the merging of data and the complex searches of BCD.
- 8.24 We reviewed minutes from meetings of MI5's Bulk Oversight Panel, which is tasked with overseeing the justifications used to retain BCD for extended periods. However, due to Covid-19 restrictions, we were unable to examine the work of the internal audit team who assess the justifications made by staff to examine BCD. We plan to do so in 2022.
- 8.25 Overall, we concluded that MI5's recorded justifications for undertaking the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality.

Targeted communications data (CD)

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

Bulk personal datasets (BPD)

- 8.27 The inspection of MI5 was held remotely due to Covid-19 restrictions and concentrated on the work and processes of:
- the Bulk Oversight Panel;
 - the Internal Audit Team, who are responsible for audit and improvement of justifications used to examine bulk data; and
 - the Protective Monitoring Team and the Compliance Investigations Group.
- 8.28 Consistent with our findings in 2020, MI5 continues to achieve a high level of compliance in this area. The systems and processes within MI5 managing the retention and examination of BPD are mature. No areas of non-compliance were identified. We made several observations either to highlight areas of good practice, to fine tune the internal oversight regime or to ensure that we are briefed on developing projects that could have an impact on compliance.

Safeguards

Legally privileged material

- 8.29 Legally privileged material can sometimes be acquired which has no intelligence value but is attached to material that does have intelligence value and which needs to be retained. We have begun an in-depth review of how this material is handled, exploring options for a common, compliant approach with MI5 and the other intelligence agencies.

Implementing the “three lines of defence” model for compliance

- 8.30 MI5 briefed us that it has introduced a “three lines of defence” model to secure compliance on its systems, namely:
- first Line of Defence: MI5 has implemented processes and ensured access to training and guidance within operational, product management and technical development teams to ensure those handling warranted data are aware of and abide by their obligations;
 - second Line of Defence: the aim is to be proactive in identifying and mitigating compliance issues; MI5 has created a new Legal Compliance Centre to create a single structure to set standards, track performance and administer controls; and
 - third Line of Defence: this will focus on internal audit.
- 8.31 We were impressed overall with MI5's ambitious plans to develop an end-to-end approach to risk management. There is a clear structure for identifying, escalating and managing risk, which is all collated through one central point to ensure any issues that cut across branches are not lost. MI5 has carefully considered the internal application of its “three lines of defence” model to ensure it can be consistent across the organisation. It is positive to see a proactive approach to identifying issues early before they escalate into risks, as well as bringing the advantage of improved horizon scanning of potential future issues.
- 8.32 However, it is clear that if MI5's approach is to succeed, it will require significant resourcing over the longer term. We will review the results of the changes introduced by MI5 in 2022.

Compliance investigations

- 8.33 MI5 set up a proactive compliance investigation team this year. The team reviews end-to-end processes where compliance risks have been identified and proposes solutions. We reviewed some early examples of the team's work and were impressed with the level of rigour being brought to this important task. This should ensure that MI5 is able to address compliance risks before they become incidents of non-compliance.

Retention, review and deletion of warranted material

- 8.34 In 2020/21, we asked MI5 to provide us with a full list of systems used to handle material obtained under the covert powers we oversee, setting out how its policy on the review, retention and deletion (RRD) of warranted material applies to each system. We have asked MI5 to ensure that this list of systems is incorporated into a future product catalogue it is producing; this will ensure there is a corporate record of all systems that hold investigatory powers material, including whether the RRD capability is automated, manual or known to be absent.

Handling arrangements

8.35 The programme of work initiated within MI5 in response to the Donnelly Review²⁵ included an initial review of the handling arrangements covering warranted data which the Home Secretary is required to approve under the IPA as a precondition of issuing warrants. This review has not yet been carried out. We are concerned that, as currently drafted, the handling arrangements do not give the Home Secretary a sufficiently detailed insight into how MI5 is handling warranted data in practice. This is an issue to which we shall return in 2022.

25 See: <https://www.gov.uk/government/publications/compliance-improvement-review>

9. Secret Intelligence Service

Overview

- 9.1 In 2021, we conducted regular inspections of the Secret Intelligence Service (SIS). The majority of our investigations related to its work overseas although, for a second year, overseas inspections had to be undertaken remotely due to Covid-19 restrictions.

Findings

- 9.2 Overall, we concluded that SIS continued to achieve a high level of compliance with the statutory requirements governing its use of investigatory powers. SIS has responded positively to recommendations made on previous inspections. However, we investigated two specific compliance incidents during 2021, further details of which are set out below.
- 9.3 SIS identified a number of legacy datasets which, since the introduction of the Investigatory Powers Act 2016 (IPA), now constitute bulk personal datasets (BPD) and which have been retained in error without a warrant in place. We also identified some serious gaps in SIS's capability for monitoring and auditing of systems used to query and analyse BPDs.
- 9.4 Separately, we conducted a special inspection to review an incident in which an SIS agent acted beyond the bounds of the activity permitted under the relevant section 7 authorisation. We reviewed the steps taken by SIS in response and were satisfied that these should significantly reduce the risk of similar incidents occurring in future.

Covert human intelligence sources (CHIS)

- 9.5 We found that the CHIS activity conducted by SIS under the Regulation of Investigatory Powers Act 2000 (RIPA) continues to be necessary and proportionate. The majority of SIS agents overseas are run in reliance on section 1 of the Intelligence Services Act 1994 (ISA) which, as we reported in our 2019 and 2020 reports, are not subject to oversight by the Investigatory Powers Commissioner's Office (IPCO). We observed that while records generally captured the key considerations and basis for a decision, they were not always captured in the comments of Authorising Officers (AOs) who are the key decision makers under RIPA. As we noted in our 2020 report, there should be greater written consideration of necessity and proportionality by AOs in the RIPA paperwork.
- 9.6 We were pleased to see that SIS had responded positively to our previous recommendations and had delivered a mandatory RIPA training course to relevant staff by the time of our inspection in October. This training, alongside other measures, indicated that SIS has embraced and embarked upon a cultural change to ensure that RIPA is better understood across the organisation and is therefore utilised, where appropriate, to authorise CHIS or directed surveillance.

- 9.7 We discussed the SIS approach to the new Criminal Conduct Authorisations (CCA) regime and were satisfied that SIS had adopted a sensible approach. We will look to test this at future inspections.

Directed surveillance

- 9.8 Following on from our inspection in 2020, we selected a number of broadly drawn directed surveillance authorisations for closer scrutiny. We also sought and received detailed briefings about the activity being conducted under these types of authorisations. These authorisations generally relate to activity at the lower end of the intrusion permitted by such an authorisation. We concluded that much of the activity sought to be authorised probably fell short of surveillance or related to activity where there was no UK nexus. However, while the activity conducted in many cases did not require authorisation under RIPA and was much narrower than that authorised, we also concluded that these authorisations were too broadly drawn to be proportionate. It was not that the activity being conducted under these authorisations was disproportionate, but that the wording of the authorisations themselves was simply too broad. This is a novel and complex area which has evolved after the Code of Practice was written. We have asked SIS to address this issue as a matter of priority.
- 9.9 We also noted that, for some categories of subjects of interest, the necessity case should be made out in greater detail rather than simply relying upon either a request from another agency or referencing a high-level intelligence requirement SIS has been tasked to collect against by the UK Government. The necessity case should clearly state how the actions will meet that requirement.
- 9.10 As is the case with CHIS authorisations, we would like to see greater written explanation from AOs showing their ongoing assessment of necessity and proportionality at all key stages in the RIPA authorisation cycle.

Property interference

- 9.11 In the light of the decision in the “Malware” judgment (see from paragraph 3.22) we reviewed all of the property warrants in force at SIS to identify any compliance issues with the terms of the judgment. Several warrants were amended as a result of that review.
- 9.12 We reviewed a small number of property warrants in the course of routine inspections in 2021 and had no concerns about the necessity and proportionality of the conduct authorised.

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

- 9.13 Our TI and TEI inspection of SIS in 2021 found that it was demonstrating a good degree of compliance with the IPA. We were pleased that SIS had responded positively to the recommendations from last year and that changes have been implemented.
- 9.14 We selected a number of thematic warrants for scrutiny and these were shared with us along with the relevant modifications and renewals. Some of these warrants were such that they relied on a “general descriptor” to allow for the adding of new subjects who fall within the activity or investigation described. This type of thematic warrant is underpinned by internal approval documents supporting any operational activity. We examined a number of these internal approval documents and found them to be of a good standard. We also

read and were content with the approach to modifications. In particular, we noted clear reference to any changes in anticipated collateral intrusion.

- 9.15 In addition, we were briefed by several SIS teams on their activities involving TI and TEI material. These helpful briefings provided clear evidence that the teams had a good knowledge of IPA rules and were working with these in mind.
- 9.16 There was a notable reduction in relevant TI errors, from eight in 2020 down to three in 2021. A contributing factor in this is that processes to manage TI activity conducted under warrant and any associated product are now embedded.
- 9.17 Overall, and subject to a number of small areas in which SIS could make amendments to relevant warrants, we were satisfied that SIS's conduct in reliance on the TI and TEI warrants reviewed on this inspection was necessary and proportionate.

Communications data (CD)

- 9.18 SIS has access to certain bulk communications data (BCD) retained by GCHQ and MI5; it does not retain BCD itself in any other format. On other UK intelligence community (UKIC) inspections, we examined the applications made by SIS staff to examine BCD. On our inspection at SIS, we confirmed that these requests were made pursuant to one of SIS's statutory functions, were linked to a valid operational purpose and contained a justifiable necessity and proportionality case.
- 9.19 SIS's use of targeted CD is limited. We were content that the small number of authorisations inspected were compliant.
- 9.20 As in previous years, SIS evidenced a very well maintained and compliant process in this area.

Bulk personal datasets (BPD)

- 9.21 As mentioned in paragraphs 9.2 and 9.3, we conducted an investigation into a compliance incident relating to SIS's use of BPD.

Legacy data

- 9.22 In our previous reports we highlighted that SIS had, when implementing measures to comply with the requirements of the IPA, identified a potential risk regarding the existence of old archived datasets in its systems that, under the IPA, would now constitute BPD. SIS data officers have continued to review historic data throughout 2021 and identified a number of legacy files that may constitute BPD. SIS concluded that the majority of these should have been deleted and were retained in error, a matter which was subsequently reported to us. We intend to undertake a detailed review of this issue during 2022.

Audit arrangements

- 9.23 We conducted a review of the process within SIS for retrospectively auditing the examination by SIS staff of BPDs. The review highlighted several areas of serious concern. Our review identified that there were some BPD systems in operational use where the Compliance Monitoring Team (CMT) had limited or no auditing capability; this means

that, in the case of these systems, the CMT is unable to identify mistakes or procedural deficiencies and put remedial measures in place.

- 9.24 In July 2021, we met with senior members of SIS to be briefed on the measures being adopted to address issues raised in the ongoing review. SIS has kept the IPC and the Foreign Secretary updated throughout.
- 9.25 SIS was early to respond to our observations and recommendations and was quick to set up a Director-led compliance improvement programme. This programme is now addressing, among other things, the resourcing necessary to respond to the issues identified.
- 9.26 We are continuing to work with SIS to monitor its progress and will provide an update to this area of work in our 2022 report.

Section 7 of the Intelligence Services Act 1994 (ISA)

General findings

- 9.27 As we noted in our 2020 report, SIS operates a number of “framework” section 7 ISA authorisations approved by the Foreign Secretary. These allow SIS officers to operate an internal approval regime to authorise individual instances of reliance on the submission. In 2021, we once again found that these “framework” submissions clearly set out the parameters of what conduct was and was not authorised, supported by detailed and appropriate internal policies. The internal records of reliance we reviewed were produced to a high standard. In one case, we noted that the detail as to actions which were or were not authorised was complex and was not entirely straightforward for operational personnel to follow. We therefore suggested SIS might consider whether the authorisation could be simplified.
- 9.28 Separately, we revisited a number of section 7 authorisations relating to a separate class of operations which we had also reviewed in 2020. These involved complex legal issues. As in 2020, the submissions we reviewed set out the analysis on these issues for the Secretary of State with great care and in extensive detail. We were pleased to note that SIS had actioned the recommendations we had previously given on improvements to ensure the Foreign Secretary had as detailed and robust a package of material as possible to satisfy them as to the necessity and reasonableness of the conduct authorised.

Review of section 7 compliance incident

- 9.29 In 2021, SIS reported to us a compliance incident whereby an agent operating online had acted beyond the bounds of the activity permitted under the relevant section 7 authorisation. The incident was thoroughly investigated by SIS and reported to the Police, who concluded that no further action was necessary. The incident was due to a number of factors including difficulties caused by Covid-19 restrictions.
- 9.30 In response to this incident, we undertook a special inspection at SIS in September 2021 to determine: the adequacy of SIS processes in ensuring that agents operating overseas under ISA section 7 authorisations do so within the parameters authorised by the Secretary of State; and the extent to which the Secretary of State could be satisfied that this was the case.
- 9.31 We examined the findings of the SIS internal review into this compliance incident and a second SIS review into aspects of working with liaison partners. We concluded that,

following the implementation by SIS of a mandatory compliance training course in September 2021, adequate measures were in place to minimise the risk of activity beyond that authorised under section 7 of the ISA. This is especially true for the highest risk cases which attract the greatest level of scrutiny and head office oversight. We recommended changes to improve internal processes which should further strengthen the “second line of defence” in lower risk cases, as will the development and implementation of a compliance policy for working with liaison partners. Taken together, these improvements should very much reduce the chances of another compliance incident such as that which occurred in 2021.

Safeguards

- 9.32 This inspection was postponed in 2020 and was conducted virtually in 2021. The safeguards in place for BPD and CD were examined on their respective inspections (see above). We were impressed overall with the agency’s mature and pragmatic approach to safeguarding data.
- 9.33 Legally privileged material can sometimes be acquired which has no intelligence value but is attached to material that does have intelligence value and which needs to be retained. We have begun an in-depth review of how this material is handled, exploring options for a common, compliant approach with SIS and the other intelligence agencies.

10. Government Communications Headquarters

Overview

10.1 During 2021, we conducted a series of inspections at the Government Communications Headquarters (GCHQ) and received briefings on key areas of its work. This included briefings on new capabilities, some of which were also attended by members of the Technology Advisory Panel.

Findings

10.2 Overall, GCHQ continues to achieve a high level of compliance with the relevant statutory requirements governing its use of investigatory powers. We made a relatively small number of recommendations on our inspections in 2021 and were pleased to see that GCHQ had made good progress in addressing recommendations raised in 2020.

10.3 The most significant development in our oversight of GCHQ in 2021 was the judgment in *Big Brother Watch v UK* (see from paragraph 3.7), which has important implications as to how GCHQ operates its bulk interception regime. We continue to adapt our oversight of this technically complex investigatory power in light of the Court's findings.

Covert human intelligence sources (CHIS)

10.4 The inspection planned for December 2021 had to be postponed due to Covid-19 and was carried out in February 2022. Of the previous four recommendations made in our 2020 inspection, only one remained outstanding: that CHIS risk assessments should be more specific and should relate to individual CHIS.

10.5 We were provided with a full range of the records relating to the management of CHIS cases, albeit that those records were maintained in a rather fragmented manner and there was a lack of consistency in their format. A new system is currently being developed that will enable all those records to be housed and viewed in a more coherent manner and require greater consistency of format. However, the records reviewed provided reassurance that all cases were well managed, necessary and proportionate and generally recorded in a compliant manner. The inputs of Authorising Officers (AO) were much improved, although there remains a need for AOs to provide a description of the authorised use and conduct of each CHIS.

10.6 We discussed the use of CHIS Criminal Conduct Authorisations (CCA), following the commencement of the legislation in 2021.²⁶ GCHQ explained that a new policy was being drawn up for implementation in the near future and this will be fully tested at the next annual inspection.

26 See: from paragraph 2.2 for further details on the legislation.

Directed surveillance

- 10.7 We noted a marked improvement in the overall standard of authorisations for directed surveillance. Applicants and AOs are providing greater specificity to the subjects of surveillance and the activity to be conducted as well as better consideration of the necessity and proportionality of the surveillance. There is still a need for AOs to describe the parameters of the covert activity being authorised rather than merely relying on the description provided by an applicant.

Property interference

- 10.8 As with the other agencies, in the light of the decision in the “Malware” judgment (see from paragraph 3.22), we reviewed all of the property warrants in force at GCHQ to identify any compliance issues with the terms of the judgment. Several warrants were amended as a result of that review.
- 10.9 In the course of our routine inspections in 2021, we had no concerns about the necessity and proportionality of the conduct authorised in property interference warrants that we examined.

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

- 10.10 We were satisfied that GCHQ was achieving a high level of compliance with the Investigatory Powers Act 2016 (IPA) and we made no recommendations with regard to TI and TEI. We had access to GCHQ's systems that store necessity and proportionality statements for IPA activity. We examined a number of these and were satisfied that the statements we reviewed justified the activity that they covered in accordance with the IPA.

Use of “descriptive” factors

- 10.11 In our 2020 report,²⁷ we noted that GCHQ was including a description of factors to be intercepted on some of its interception warrants, relying on the provisions in the IPA that such factors may be either specified or described. We reported that we would operate an enhanced oversight regime for GCHQ interception warrants containing these “descriptive” factors. In 2021, we examined a number of these warrants and, in a very small number, we suggested that GCHQ may wish to consider narrowing the scope of the general descriptor to be more consistent with the actual category of individuals the warrant is intended to cover. On the whole, we found that in the warrants we inspected, the use of the general descriptive factors was appropriate. We will continue to monitor this closely in 2022.

Targeted equipment interference (TEI)

- 10.12 We inspected aspects of TEI activity at GCHQ on two occasions in 2021.
- 10.13 We examined one warrant that related to both national security and serious crime. A warrant where one of the purposes is to obtain or select for examination legal professional privilege (LPP) material may only be issued if (among other things) there are exceptional and compelling circumstances. Where the warrant is issued on serious crime grounds, obtaining the LPP material must also be necessary for the purpose of preventing death or

27 Annual Report of the Investigatory Powers Commissioner 2020 (paragraph 11.21). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

significant injury. One of the stated purposes of this warrant was to obtain LPP material but, in discussion with GCHQ, it was unclear in respect of which targets LPP material was being sought and whether this was for national security or serious crime purposes. We recommended that, with respect to this warrant, GCHQ must clarify at the next renewal whether the LPP material sought relates to national security and/or non-national security cases, highlighting the need to prove the exceptional and compelling reasons for obtaining and examining any LPP material.

Bulk Interception (BI)

Findings on our 2021 inspection

- 10.14 We conducted our bulk interception inspection at GCHQ in May 2021, shortly before the Grand Chamber's judgment in *Big Brother Watch v UK* was handed down (see from paragraph 3.7). Our inspection focused on the justifications recorded by GCHQ for several steps in the bulk interception process: decisions as to which bearers would be intercepted; rules (known as "promotion rules") determining what data from those bearers is moved into storage; and the selection for examination of some of that data by analysts, in pursuit of operational requirements.
- 10.15 We identified that the reasons and justification for selecting particular bearers was being recorded formally in some instances but, in others, the decisions were being recorded informally (i.e. in emails). In many instances, there was no consideration of the necessity and proportionality justification for selecting a particular bearer. We therefore recommended GCHQ rectified this as soon as possible. GCHQ took action immediately to ensure that necessity and proportionality justifications were being produced for all bearer selection decisions. By the end of 2021, GCHQ had also made good progress in making the necessary changes to its systems to enable these justifications to be drafted within the relevant systems themselves.
- 10.16 We identified that GCHQ's policy on "promotion rules" required analysts to justify the necessity of rules which moved data into storage but there was no requirement for a proportionality justification to be provided. We therefore recommended that GCHQ's policy be amended to require both necessity and proportionality justifications to be produced for promotion rules. GCHQ has since done so.
- 10.17 We reviewed a sample of statements drafted by analysts at GCHQ to justify the selection for examination of content obtained through bulk interception. We found that 41% of the statements sampled failed to address either necessity or proportionality in sufficient detail and 8% failed to address both. We therefore recommended that GCHQ make improvements to the standard of necessity and proportionality statements used to justify the selection for examination. We will be reviewing a further sample of the selection for examination justifications on our 2022 inspection to test GCHQ's response to this recommendation.
- 10.18 Given the findings of our May 2021 inspection, we had planned a follow up inspection later in the year to review progress against the recommendations made. In the event, it was not possible to conduct this follow up visit. However, GCHQ kept us updated regularly on the action taken against the above recommendations and we expect to see significant improvements on our 2022 inspection.

Bulk equipment interference (BEI)

- 10.19 As in previous years, we continued to conduct an enhanced inspection regime for activity conducted by GCHQ under its more established BEI warrants. We examined a large number of necessity and proportionality cases drafted by analysts to justify the selection for examination of data acquired under BEI warrants.
- 10.20 We were pleased to see that GCHQ had taken action on all the recommendations we made following our 2020 inspection. Overall, we found the standard of record keeping for activity conducted under BEI to be of a high standard. Necessity and proportionality statements relating to action taken under BEI warrants have improved, especially among mission areas that make the most use of these capabilities.
- 10.21 In the context of one BEI warrant, we noted that the warrant instrument listed certain conduct which, when read alongside the warrant application, was not within the scope of the actions authorised or required by the warrant. In discussion with GCHQ, we identified that BEI warrants draw on standardised forms of words to describe the authorised conduct. We recommended that the conduct authorised by all GCHQ BEI warrants should be consistent with the scope and purpose of the conduct described in the warrant applications.
- 10.22 Shortly after our inspection of BEI activity, GCHQ made us aware of two errors in relation to activity authorised under a BEI warrant. GCHQ explained that the team hosting our inspection had been unaware of the internal investigations and so this was not flagged to Inspectors at the time. GCHQ now has a process in place to ensure that the team hosting inspections reviews any errors under investigation to ensure these are raised on inspections as appropriate. We will be seeking detailed briefings from GCHQ about these errors at an early stage in 2022.

Communications data (CD)

Bulk communications data (BCD)

- 10.23 GCHQ's internal compliance team conducts robust retrospective checks of requests made to examine BCD. When justifications are questioned, a policy and compliance lead is responsible for ensuring that the person completing the request is made aware.
- 10.24 The Policy and Compliance Network is a network of staff distributed throughout GCHQ who are responsible for compliance in their areas. Their responsibilities include working with analysts to ensure their justifications are up to standard and providing additional training when audit has found that their requests have fallen below standard.
- 10.25 The compliance team is also able to search the justifications recorded in all GCHQ BCD systems for specific words to identify data examined that relates to individuals who hold sensitive professions or are involved in journalism. From here, the team can assess if the examination was justified.
- 10.26 Overall, we concluded that GCHQ's recorded justifications to undertake the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality.

Targeted communications data (TCD)

10.27 Our inspection in 2021 concluded that processes used by GCHQ to acquire CD were working to a high standard, with applicants' justifications satisfactorily completed and supported by strong internal governance procedures. Overall, we identified positive improvements within GCHQ.

Bulk personal datasets (BPD)

10.28 GCHQ's internal governance process for BPD is overseen by a Bulk Personal Data Panel. The panel meets on a regular basis to consider the necessity and proportionality of the retention and examination of all BPDs.

10.29 The panel maintained its governance role throughout 2021. This was evidenced in the requests made to the panel to retain datasets and we examined the detail at inspection.

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

The Equities Process

10.31 In our 2020 report, we reported on our first inspections of the Equities Process at GCHQ; this is the means through which decisions are taken on the handling of vulnerabilities found in technology. These vulnerabilities may represent a risk to the security of the UK or its allies. In some cases, the same vulnerabilities might provide a means by which the UK intelligence community (UKIC) could obtain intelligence in pursuit of its statutory functions. The term "equity" in this context is used to refer to a vulnerability known to GCHQ.

10.32 On the basis of our inspection in 2021, we remain satisfied that the Equities Process was functioning effectively and that GCHQ was making rational, evidence-based decisions about whether to retain or release vulnerabilities (and thereby enable a patch or other remedy to be implemented).

10.33 In 2020, we recommended that GCHQ should improve the way in which Equities Process decisions are recorded. This recommendation has now been addressed and the records reviewed on our 2021 inspection provided a clear and comprehensive record of decisions taken which provided all of the necessary information for *ex post facto* review.

10.34 Our oversight of the Equities Process at GCHQ continues to take place on a non-statutory basis. We expect our oversight of this area to be put on a statutory footing in 2022.

Section 7 of the Intelligence Services Act 1994 (ISA)

10.35 We reviewed a sample of operations conducted by GCHQ in reliance on section 7 authorisations and were satisfied that these were necessary and proportionate. GCHQ's records of reliance on section 7 authorisations were generally clear and comprehensive, although it is working to introduce changes to one of the systems in which these

records are produced to ensure they are as clear and comprehensible as possible to an external reviewer.

- 10.36 We made recommendations aimed at ensuring submissions to the Secretary of State seeking an authorisation under section 7 were as clear as possible. First, we noted that GCHQ often used terms such as “low” or “medium” to describe the level of risk associated with lines of operational activity; we recommended that, where feasible, GCHQ should define or quantify risk more precisely. Secondly, we recommended that GCHQ includes a clearer description of the operational activities authorised under two of its section 7 authorisations.

Safeguards

- 10.37 Due to Covid-19 restrictions, this inspection was conducted remotely. An in-depth discussion took place across a variety of issues concerning the handling of data obtained under warrant and we were impressed overall with the agency's mature and pragmatic approach to safeguarding data.
- 10.38 GCHQ has a dedicated compliance team that identifies and investigates incidents and is involved in the auditing of systems. In addition, GCHQ has a new automated tool to manage international data sharing which has enhanced the ability to comply with IPA safeguards.
- 10.39 GCHQ reported a systems-related error which had led to the over-retention of IPA material over several systems on a storage area. This is set out in further detail at paragraph 18.8 and is subject to ongoing inspection which will continue into 2022.

Legally privileged material

- 10.40 Legally privileged material can sometimes be acquired which has no intelligence value but is attached to material that does have intelligence value and which needs to be retained. We have begun an in-depth review of how this material is handled, exploring options for a common, compliant approach with GCHQ and the other intelligence agencies.

11. The Ministry of Defence

Overview

11.1 In 2021, we undertook inspections of the Ministry of Defence's (MoD) use of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) in the UK. We also oversee the MoD's agent running and surveillance activities overseas, although this is undertaken on a non-statutory basis. Discussions continue with the MoD about placing our oversight of this area on a statutory footing.

Covert human intelligence sources (CHIS) and directed surveillance

11.2 The MoD's overall level of compliance is very high with excellent and detailed applications alongside well considered inputs from Authorising Officers (AOs). The MoD on occasion errs on the side of caution, obtaining authorisations when possibly none are required.

11.3 The distinction between when conduct takes place overseas or in the UK needs clearer definition in MoD policy to reflect the RIPA Codes of Practice. This has important implications for what approach should be taken and whether an application for a CHIS Criminal Conduct Authorisation (CCA) should ever be needed. CHIS risk assessments were also lacking focus and necessary detail in some cases.

11.4 The MoD is undertaking a review of its RIPA policy and this provides a good opportunity for improvements to be made.

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

11.5 The Army, Royal Navy and Royal Air Force conduct activities on land and in UK territorial waters and airspace which are covered by TI/TEI warrants.

11.6 The MoD has a rigorous internal process for authorising these activities. An assessment is made in each case to take account of any expected collateral intrusion the activity may cause as well as any privacy issues. We observed good practice when training activity is conducted under the warrants in relation to the handling and deletion of data with personnel being made aware of the scope of the activity which is permissible under the warrant. Each application to conduct activity goes into the detail of what equipment will be used and the location and the duration of the activity.

11.7 The warrants are also used to test new equipment and, in limited circumstances, the data may be kept for longer periods to allow analysis of the results. Testing and training is an essential part of the MoD's mission and it is meticulous in ensuring that any data collected is deleted in accordance with the MoD's handling arrangements.

- 11.8 We interviewed representatives from all three services and are satisfied that the MoD has demonstrated a very good level of compliance with the IPA and its Code of Practice in respect of TI and TEI. We also noted that the Secretary of State is briefed on any changes to the Handling Arrangements for data collection.

12. The Principles

Overview

- 12.1 This is the second year 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 force on 1 January 2020.

Findings

- 12.2 Overall, all six public authorities subject to The Principles (known as the “Principles partners”) are achieving high levels of compliance with the policy. We were pleased, in particular, to observe that both the Ministry of Defence (MoD) and the National Crime Agency (NCA) have made significant progress in addressing the problems identified during inspections in 2020. Both organisations have now achieved a much higher improved level of compliance.
- 12.3 The most significant deficiency observed in 2021 concerned the “presumption not to proceed” in cases involving a real risk of torture, set out immediately below. We also identified gaps in SIS’s assessment of two “detention pathways” overseas (see paragraph 12.13).

The “presumption not to proceed”

- 12.4 Paragraph 3 of The Principles says:

“The UK takes great care to assess whether there is a real risk that a detainee will be subject to i) unlawful killing ii) torture iii) cruel, inhuman and degrading treatment iv) extraordinary rendition or rendition or v) unacceptable standards of arrest and detention. The UK investigates whether it is possible to mitigate any such risk. In circumstances where, despite efforts to mitigate the risk, there are grounds for believing there is a real risk of torture, unlawful killing or extraordinary rendition, the presumption would be not to proceed.”

- 12.5 In 2021, we reviewed a number of cases where there was a real risk of torture or unlawful killing which could not be mitigated. These cases arose in our inspections at the Metropolitan Police Service (SO15), the NCA and the Foreign, Commonwealth and Development Office (FCDO) (the latter being an SIS submission reviewed at the FCDO with a focus on the advice provided by officials to the Secretary of State). While the applications presented the risks accurately, the presumption not to proceed was not mentioned in the relevant Ministerial submissions in these cases.
- 12.6 In cases where there is a real risk of torture, unlawful killing or extraordinary rendition that cannot be mitigated, the effect of the “presumption not to proceed” is that the balance is

shifted in favour of refusing the operational proposal. It is therefore crucial that Ministers address their mind to the presumption and are provided with advice to that effect. We have made this clear both to the departments subject to The Principles and to the FCDO and the Home Office, who prepare advice for Ministers on Principles cases. The importance of the “presumption not to proceed” will continue to be a focus for inspections in 2022.

MI5

- 12.7 We inspected MI5's compliance with The Principles by reviewing a sample of cases in which MI5 was sharing intelligence directly with a foreign authority. Overall, we were satisfied that MI5 was maintaining a high level of compliance.
- 12.8 In our 2020 report, we noted that MI5 was not always applying appropriate caveats to intelligence shared with foreign authorities, either because it omitted relevant requirements or they were out of date. On our 2021 inspection, we noted that MI5 has now introduced a standard caveat for use on all intelligence shared with foreign authorities, which may be amended and adjusted as required in specific cases. We were satisfied that all caveats reviewed on our 2021 inspection addressed all of the relevant risks and, where necessary, were being adapted to the operational context.
- 12.9 We also noted in our 2020 report that, where MI5 was acting in reliance on a Principles risk assessment conducted by SIS, MI5 was producing its own, internal risk assessments which tended to be unnecessarily detailed and risked causing duplication or confusion. On our 2021 inspection, we saw examples of MI5's assessments which made much more concise, clear reference to credible and reliable assessments made by SIS. However, we identified one example where an MI5 assessment should have included more detail from the SIS assessment to ensure that the MI5 assessment could be read in isolation.
- 12.10 Finally, we recommended to MI5 that, where appropriate, the officer authorising an internal Principles risk assessment should be given some flexibility in deciding how frequently that assessment should be reviewed in low risk cases, enabling greater focus to be given to higher risk cases.

Secret Intelligence Service (SIS)

- 12.11 Our Principles inspections at SIS continued to focus on SIS as the primary interlocutor between the UK intelligence community (UKIC) and foreign liaison partners overseas, in the context of detention operations. The two inspections we conducted at SIS in 2021 focused on SIS's role as the agency dealing directly with overseas authorities and which is responsible for producing risk assessments under The Principles. However, where relevant, MI5 and GCHQ joined the inspection to explain the operational context to the cases selected for review.
- 12.12 The discussions on our inspection in July 2021 underlined the significant operational and legal challenges posed by conditions in some of the countries in which UKIC is operating. Overall, we were satisfied that UKIC, led by SIS, continued to achieve a high level of compliance with The Principles when contributing to detention operations overseas.
- 12.13 On our inspection in December 2021, we identified two cases in which we concluded SIS had not conducted sufficient “due diligence” as to the treatment of detainees in two particular countries, although in one of those countries SIS was not proactively soliciting detention operations. The term “detention pathway” in this context refers to the route

a typical detainee might take through a country's detention system, from point of arrest through to trial and conviction. We identified that SIS had not considered important details about the way in which detainees might be treated, affecting the reliability of its assessment of risk under The Principles were SIS to contribute to detention operations in future. We judged that these gaps in SIS's assessment were most likely to arise in countries where SIS was not regularly contributing to detention operations and asked SIS to review its assessment of the "detention pathway" in other relevant countries as a priority.

- 12.14 In our 2020 report, we included details of the multi-agency assessment team which is compiling assessments of human rights risks in support of decisions made under The Principles. The team has now proposed a new, more efficient, way of producing its open source analysis work, enabling the team to focus its efforts on assessments requiring reference to classified material. We were content with this approach, given the SIS approach still ensured that a UK Government official continued to make the final decision on the risks highlighted by the assessments.

Government Communication Headquarters (GCHQ)

- 12.15 Consistent with our approach at MI5, at our Principles inspection at GCHQ we reviewed a sample of cases in which GCHQ was sharing intelligence directly with a foreign authority, or authorising the release of its intelligence to a foreign authority.
- 12.16 Overall, GCHQ continued to achieve a high standard of compliance with the requirements of The Principles. In most cases, GCHQ was not disclosing intelligence directly to a foreign authority but, rather, considering requests from UK or foreign partners to disclose GCHQ's intelligence to a third party in circumstances which engage The Principles.
- 12.17 In 2020, we had identified that, on occasion, GCHQ granted permission for its intelligence to be used by third countries to inform the debriefing of a detainee in the custody of a foreign authority overseas. We had recommended to GCHQ that its contribution to detainee interviews in such cases ought to be brought to Ministers' attention, enabling them to consider the causality of UK involvement and the associated legal and policy risks in line with paragraph 14 of The Principles. This recommendation has now been actioned by GCHQ.
- 12.18 On our 2021 inspection, we recommended that GCHQ ensures its internal record included all information relevant to the decision whether or not to proceed under The Principles, including, where necessary, by asking the party requesting GCHQ's permission to disclose the intelligence for further details of the justification for doing so, or by including a cross-reference to any relevant Ministerial submissions.
- 12.19 As of the end of 2021, GCHQ was working on a policy which would apply where a UK government department that was not subject to The Principles was seeking permission to release intelligence owned by a Principles partner to a foreign authority. That policy, on which we will report further in our 2022 report, is likely to rely on the department that is not covered by The Principles producing its own assessment of the relevant risks, e.g. under the Overseas Security and Justice Assistance (OSJA) policy framework.

The Ministry of Defence (MoD)

- 12.20 In our 2020 report, we commented on serious gaps in the MoD's assessment of risk under The Principles in a particular operational context. We said then that the MoD had initiated

a programme of work to revise and refresh its approach. At our 2021 inspection, we were pleased to observe considerable improvement in the consideration of risk and the quality and clarity of ministerial submissions. The MoD had fully addressed all but one of our previous recommendations; this related to developing a greater understanding of the differences in approach to some Principles risks by certain international partners.

- 12.21 We identified one case in which the MoD was not privy to information available to another Principles partner that was relevant to a decision being taken by the MoD under The Principles. We note that the MoD has now become more fully engaged with other Principles partners to ensure that it has access to the most up to date assessments of Principles risks in different countries. This should avoid future instances of the MoD being unaware of information that has a material bearing on the assessment of Principles risks.
- 12.22 Separately, we asked the MOD formally to report an error regarding its failure, on several occasions, to comply with The Principles by notifying Ministers of its receipt of unsolicited intelligence in one operational context. While the MOD has already taken steps to try to prevent similar errors occurring in future, similar steps were taken in 2019 in response to the same error in the same operational context. We will examine the MoD's arrangements for receipt of unsolicited intelligence again on our next inspection.

The National Crime Agency (NCA)

- 12.23 In our 2020 report, we noted that The Principles risk assessments produced by the NCA were of variable quality and that the country assessment documents in use at the time were insufficiently focused on risks under The Principles, thereby risking confusing officers. We reported that the NCA had introduced more focused assessments.
- 12.24 We conducted two inspections of the NCA in 2021. In both inspections, we noted a marked improvement in the NCA's assessment of risk under The Principles compared with our findings in 2020. Overall, we were satisfied that the NCA was achieving a good level of compliance with The Principles and we will be conducting the NCA's inspection once per annum from 2022 onwards.
- 12.25 The NCA has accepted that it needs to move away from assessing all operations on a case-by-case basis, working towards a model where thematic or framework assessments are developed, setting out the risks associated with a particular set of activities in a particular country. This ensures that the risks are assessed comprehensively, having regard to all of the relevant evidence, and reduces the risk of individual officers overseas making errors when producing their own ad hoc risk assessments at short notice. We saw some early signs that these thematic assessments were being produced to a good standard. We noted it was important for officers overseas to be clear on what actions they are and are not authorised to take under thematic assessments and that they record their judgment in each individual case, confirming that their actions fall within the boundaries of that assessment.
- 12.26 On our second inspection of 2021, we reviewed two cases involving a real risk of torture which could not be mitigated, although in the end no intelligence was passed to a foreign authority in either case. We noted the vital importance of Ministers being reminded of the "presumption not to proceed" in such cases (see from paragraph 12.4). In the cases we reviewed, the presumption was not mentioned either in the NCA's internal assessment or in the Home Office's submission to Ministers. We expect this to be addressed in all future submissions.

- 12.27 Finally, we noted a degree of confusion in one case as to whether the risk to a detainee fell to be assessed against the known facts about that particular detainee, or against the background to the detaining authority generally. We recommended that, in cases involving unsolicited intelligence, the NCA should ask whether the available information on the detaining authority suggests detainees are at real risk of mistreatment. If there is, in general, a real risk that detainees in the country may be subject to mistreatment, that risk will apply to the individual detainee unless the NCA can identify specific facts which suggest otherwise.

Metropolitan Police Counter Terrorism Command (SO15)

- 12.28 SO15 has made good progress since the introduction of The Principles. It has developed a strong, knowledgeable central team to oversee compliance and to improve knowledge among its colleagues based overseas who also have an important role to play and has set up robust processes to achieve compliance with The Principles. We were impressed by a new form which, with a few minor changes recommended on our inspection, should guide applicants and senior personnel through all of the necessary considerations under The Principles.
- 12.29 We asked SO15 and the Home Office to work together to ensure Ministers are presented with the clearest possible information upon which to consider whether any proposed sharing of information is consistent with the UK's policy not to condone mistreatment. We also recommended that SO15 must clearly highlight any cases in which the "presumption not to proceed" is engaged (see from paragraph 12.4).
- 12.30 SO15 reported a number of errors under The Principles in 2021, nearly all of which related to a failure to apply The Principles to the receipt of unsolicited intelligence from low risk countries. We have suggested that assessing the risks of receipt from such countries on a thematic basis would help reduce the risk of similar errors occurring in future.
- 12.31 In our 2020 report, we noted that the NCA and SO15 were preparing a policy setting out how they, and the other Principles partners, would proceed in urgent cases. This policy has not yet been received by IPCO. If it is agreed, we will include details in our next report.

13. Law Enforcement Agencies and Police

Overview

- 13.1 During early 2021, we continued to be flexible in how we conducted inspections with decisions driven by the specific needs of the inspection and the prevailing pandemic regulations and guidance. Although towards the latter part of 2021 we were able to return to a position where physical visits were feasible, we have continued to adopt a more flexible approach to our inspection model with a mix of in-person and remote visits; this offers our Inspectors and public authorities more flexibility but ensures that our inspections remain at the same high quality as before.

Findings

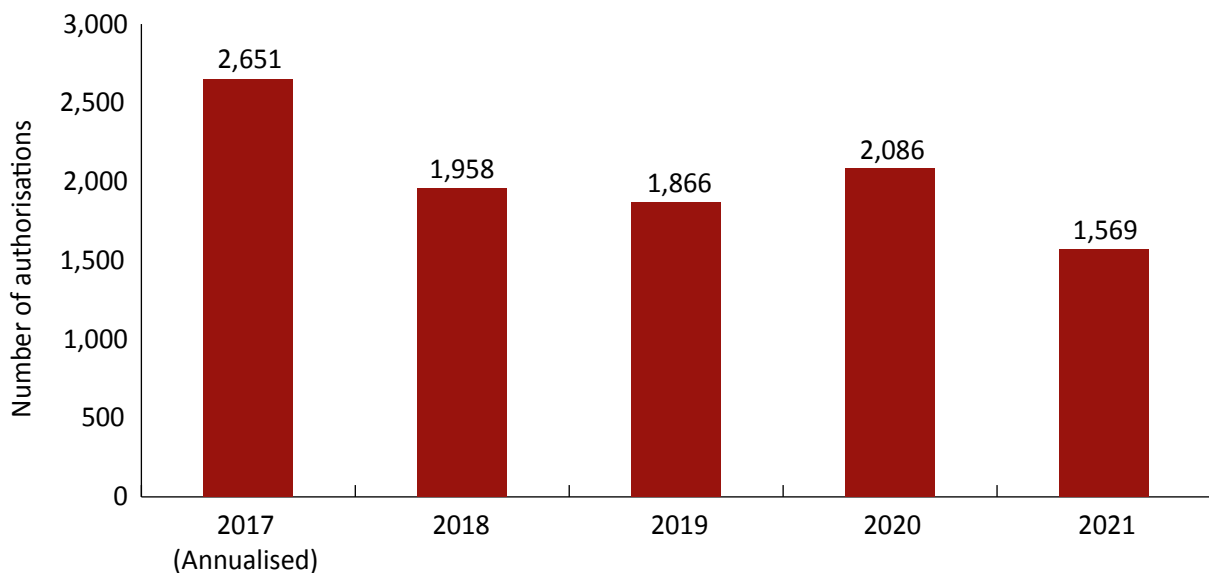
- 13.2 The level of compliance at the forces we have visited has generally been high. It is clear that some law enforcement agencies (LEAs) were still coping with the effects of lockdown, particularly in relation to maintaining good management in place for covert human intelligence sources (CHIS) and the ability to conduct surveillance. However, it is pleasing that, despite dealing with ongoing issues from Covid-19, there has been on the whole, a quick and successful adaption to the CHIS Criminal Conduct Authorisation (CCA) regime by police forces.
- 13.3 At most LEAs we inspect, we continue to highlight data assurance and safeguards as issues of non-compliance. It is recognised that a good deal of work has taken place, or is underway, but it will be a matter of time before all LEAs have implemented regimes compliant with the safeguards in the relevant Codes of Practice. A particular concern identified through this programme of work was in relation to the way Regional Organised Crime Units (ROCUs) were handling and storing targeted intercept (TI) material received from both the National Crime Agency (NCA) and the Metropolitan Police Service (MPS). Although the key issues have now been resolved, this is an area on which we will be focusing in our 2022 inspections.
- 13.4 In our 2020 report, we noted that the IT system used by LEAs to apply for and manage intercepted material was resulting in some compliance issues which caused a number of relevant errors. While an interim solution has been put in place on the current system, this does not detract from the need to find a sustainable longer term replacement.
- 13.5 Since 2019, we have been commenting in our annual reports about LEAs not meeting the criminal threshold for applying for communications data (CD) in internal professional standards investigations. While there remain some legacy issues, we have seen a considerable improvement in applications over 2021.

Covert human intelligence sources (CHIS)

13.6 CHIS intelligence continues to be a vital tool in the fight against a broad range of criminality, particularly conspiratorial crimes such as the supply of class A and B drugs which are notoriously difficult to tackle through more conventional, overt evidence-gathering techniques. All LEAs aim to be proactive in their recruitment of sources, seeking to ensure that those who are authorised report on the priorities set by the LEA and in support of its defined intelligence requirements.

13.7 Figure 13.1 shows the number of CHIS authorisations (excluding relevant sources) from LEAs since 2017.

Figure 13.1: Covert human intelligence source authorisations for LEAs, 2017 to 2021



13.8 Our inspections show a high degree of compliance with the statutory framework in this area. The grounds of necessity and proportionality for CHIS deployments are generally articulated well. However, we continue to identify examples where the risk of interference with the private or family life of persons who are not the subjects of the CHIS activity (collateral intrusion) is not sufficiently addressed. The adoption of templated or formulaic entries by applicants and Authorising Officers (AOs) was highlighted in our 2020 report and this poor practice continues to be encountered during some inspections. The considerations of collateral intrusion should explicitly relate to the individual CHIS, acknowledging the particular ways in which a source may gather intelligence on behalf of the LEA.

13.9 Through our examination of CHIS pre-authorisation records, we have identified a number of LEAs where the engagement with a source extends over a number of months before a decision is reached on whether to seek formal authorisation. During these protracted periods, many sources will continue, whether tasked or not, to provide the LEA with information. Among a small number of LEAs, there remains a misconception that if the prospective source is not formally tasked by the LEA to provide information then an authorisation is unnecessary. This is not the case and a source must be authorised once they meet the statutory definition. We have generally found that those LEAs who adopt a policy of early intervention and robust oversight of the source recruitment process by the AO are the most compliant in this area and we recommend this as good practice for all.

- 13.10 In 2020, we reported how different LEAs had responded with alacrity to the constraints imposed by the pandemic. Inevitably, the number of physical meetings with CHIS had to be reduced and even temporarily suspended during the lockdown periods. As the Government restrictions were relaxed during the year, we were pleased to note that the pre-pandemic rhythm of contacts, particularly with higher risk sources who may suffer from drug or alcohol addictions, had resumed.

Focus on CHIS welfare

We have been pleased to see the efforts of individual LEAs and national working groups to do what they can to ensure that the mental welfare of those authorised as CHIS, be that as professionally trained undercover officers or individuals reporting intelligence to police forces, is given appropriate consideration.

Undercover officers are already well supported and receive ongoing psychological assessment and support. Those members of the public acting as what we might term "crime CHIS" are invariably those individuals who are living less structured lives, often without paid employment or the security of a stable family life. Many will be current or past users of alcohol or drugs and some will be engaged in criminality from which they find it difficult to escape.

It is therefore vital to assess their suitability for the CHIS role before authorisation. This should form part of the proportionality and risk assessment considerations of the AO. We are pleased to learn that some police forces have used medical practitioners to assist them in particular cases, with the necessary anonymity of the CHIS maintained, in their assessments of the CHIS's welfare and handling needs. Such an assessment assists the public authority to discharge the duty of care that it owes to any CHIS providing intelligence for its benefit.

We are also aware that some dedicated Mental Welfare First Aider training has now been rolled out for those managing crime CHIS in a number of forces, with additional input and guidance planned for operational policies and training by the National College of Policing. We will look more closely at this training course during the coming year in order better to understand the tools provided to those managing CHIS. This should also assist in their examination of CHIS documentation and ensure they are able to identify the mental wellbeing triggers those records might indicate to enable early intervention and support for the CHIS.

We will continue to ask the appropriate questions during our oversight of CHIS management units, to ensure that CHIS welfare and mental wellbeing is being given the relevant investment and appropriate consideration by those statutorily responsible for their use and conduct.

- 13.11 We continue to send representatives to the National Source Working Group (NSWG) meetings to share the good practice we have encountered during our inspections, not only in relation to the management of mental health but also wider CHIS related issues. This includes matters such as the implementation of the Covert Human Intelligence Sources (Criminal Conduct) Act 2021²⁸ and the safeguarding of material acquired through CHIS activity.

Juvenile CHIS

- 13.12 In 2021, we inspected the records relating to four authorisations that had been granted for the use of a juvenile CHIS (anyone aged below 18). Some of the records spanned the period

28 See: paragraphs 2.2-2.5.

2020/21, as the pandemic had disrupted our usual inspection timings. Understandably, this covert tactic remains a rarity.

- 13.13 While it would be imprudent to give too much detail, those juveniles had been used variously to assist with investigations into matters such as terrorist groups and criminal gangs involved in serious criminality including murder and firearms. In one police force, the use of a juvenile had been seriously contemplated but was deferred until such time as the individual had reached maturity and could be authorised as an adult. On our inspections of CHIS records, we look to see that clear parameters have been set for tasking and debriefs and that steps are taken to ensure individuals clearly understand what is required of them. We also expect to see enhanced risk management plans, which may need to include suitable control measures, including limiting the nature and extent of contact between the source and subjects upon whom they are reporting; the submission of monthly reviews; and ensuring their Handlers had a good understanding of any issues that could impact the welfare of a child.
- 13.14 In August 2021, the Investigatory Powers Commissioner (IPC) wrote to the relevant public authorities asking that he should be notified within seven days of the authorisation of any juvenile (or vulnerable) CHIS. This ensures an early review by our Inspectors rather than waiting for the next inspection, which could be several months away. The impact of and the results from these early inspections will be reported on in our next report.
- 13.15 We worked closely with the Home Office during the passage of the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 and the associated consultation on a revised CHIS Code of Practice to ensure that the paragraphs relating to the use of juvenile or vulnerable CHIS are consistent with these developments.

Covert Human Intelligence Sources (Criminal Conduct) Act 2021

- 13.16 As set out in Chapter 2,²⁹ the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 put on a specific statutory footing authorisations which permit elements of criminal conduct on the part of CHIS and relevant sources. The focused attention of LEAs as the legislation was introduced has created some momentum to achieving consistency of approach across the LEA community. Evidence of this is already being seen.
- 13.17 In addition to the requirement for LEAs to notify a Judicial Commissioner of each CCA within seven days of authorisation, we review these during our inspections. The IPC has also instigated a quarterly review process, conducted by the Inspectorate, to examine the effectiveness of the notification processes, the standard of submissions to IPCO and that relevant comments by Judicial Commissioners are taken into account by the authorising body.
- 13.18 The first quarterly review revealed that, in spite of some early teething issues when the process was first introduced, the standard of submissions was generally quite high. Some of the general findings included evidence that:
- most CCA applications are well constructed with appropriate and relevant considerations around necessity, proportionality and collateral intrusion;
 - as time progressed, authorisations improved in quality, with most dealing well with the three distinct elements attached to proportionality;

29 See: paragraphs 2.2-2.5.

- collateral intrusion considerations were specific to the nature of the criminal conduct being authorised, with most articulating the risk appropriately;
- AO considerations were, in the main, specific to the criminal conduct they were authorising although early in the process some relied on considerations they had for the section 29 authorisation;
- in some applications, comments provided by the senior officer giving concurrence drifted towards those considerations reserved for the AO;
- details provided around the risk to the CHIS or relevant source engaging in the conduct were generally of good quality. Some good examples provided a vivid picture of the risks and measures being introduced to manage them;
- in most cases, a very detailed description of the conduct being authorised was articulated. This ensures the CHIS or relevant source will understand the parameters they were required to work within; and
- the cases that resulted in comment from a Judicial Commissioner following statutory notification produced a positive response with the LEA either addressing queries via return email or the submission of reviews and/or cancellations.

13.19 It is accepted that there are still some learning and administrative issues to overcome. However, it is worth noting the significant work undertaken by the NSWG and National Undercover Working Group (NUWG)³⁰ in delivering the appropriate training and guidance to LEAs to ensure the notification process is complied with. Our ongoing liaison with these groups ensures that any potential non-compliance issues are addressed speedily and robustly.

Relevant sources

13.20 The examination of operations using relevant sources (or undercover operatives) continues to be a major aspect of inspections for any LEAs that utilise this covert technique.

13.21 Table 13.1 sets out the authorisations and applications for relevant sources since 2020.

30 The National Undercover Working Group (NUWG) is the group which formulates national policy. It is led by a Chief Constable, and its membership includes representatives from IPCO, each region of the UK, national law enforcement agencies, the Crown Prosecution Service, College of Policing, Home Office and the National Police Chiefs' Council (NPCC) liaison team to the Undercover Policing Inquiry.

Table 13.1: Relevant source authorisations and applications, 2020 to 2021¹

	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

Notes:

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

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

³ Refusals relate to applications to renew only.

13.22 There continues to be an increase in the number of online operatives authorised. This is targeting a wider range of criminal activity and threats to national security as law enforcement recognises that virtually all forms of organised criminality and extremism will utilise the internet and social media to varying degrees.

13.23 A number of recurring failings were noted in 2021 and brought to the attention of the relevant LEA and the NUWG:

- a failure to notify us of newly granted authorisations, particularly where an operative(s) was added to an ongoing undercover operation;
- applications for long-term renewals sent to us at short notice, despite the LEA being notified of the impending date in sufficient time; and
- an ongoing tendency, particularly at the periodic reviews that are conducted, to provide a lot of unnecessary and repetitious detail. While this is not wrong, it is not best practice as it carries the danger that important factors can be buried among the extraneous detail.

13.24 It has been noted that there has been a marked improvement in risk assessments, which are now more specific to individual operatives and dynamically updated as any issues emerge.

13.25 Undercover operatives continue to offer highly effective information in the prevention and detection of crime and protection of national security. Notwithstanding that there are often learning points and areas for improvement found during most inspections, the reality is that the oversight, governance and management of this technique is much improved on the regime that was extant 10 years ago. That is not to say that our oversight can be relaxed in any way; this will remain a key area of our inspections.

Police Scotland

13.26 In early 2021, following a change in management structures and an internal review, we were alerted by Police Scotland to the discovery of several significant failings in relation to the use of undercover operatives. The majority of issues identified by the Force concerned poor supervision resulting in, in some cases, non-adherence to internal standard operating procedures (SOPs). These matters were raised with us as potential compliance failings in some areas which, if not addressed immediately, would likely lead to future compliance issues. We worked with Police Scotland to offer guidance and develop both immediate and

longer-term solutions. In our inspection in May 2021, we paid particular attention to the issues that had been brought to our attention.

13.27 Several areas requiring action were identified, including:

- the management of risk during operational deployments was questionable, leaving practitioners concerned for their personal safety;
- the oversight required by the Covert Operations Manager (COM-UC) was lacking, with no regular contact with operational staff;
- operational security measures, necessary for the development of these specific covert tactics, had been undermined, with several standard operating procedures not followed;
- there had been limited engagement with the Covert Authorities Bureau (CAB), responsible for the compliant construction of necessary authorisations. This has led to a lack of understanding and limited assessment of legislative requirements; and
- there had been a failure properly to develop, deploy, store and audit necessary technical equipment, and a failure properly to retain, review and destroy (RRD) covertly obtained material, leading to non-adherence to the safeguarding responsibilities outlined within the relevant Code of Practice.

13.28 Following the inspection, the IPC directed that an interim inspection of the Special Operations Unit (SOU) should take place to assess progress.

13.29 In August 2021, a further inspection was undertaken with members of the Force's senior management team. Between the annual and interim inspections, we held regular meetings with the Head of the SOU to monitor compliance improvements and to mentor the officer who, while experienced, was relatively new to the role. This helped to assure that those procedures being developed would meet good practice standards and assist in future proofing the use of these covert tactics.

13.30 The Chief Constable and Deputy Chief Constable (as Senior Responsible Officer (SRO)) were strong advocates for developing the required improvements and were commended by the IPC in this regard. We have continued to hold follow up conversations with the Head of SOU, with this covert tactic identified as an area for further, specific focus during the 2022 inspection.

13.31 The IPC was grateful for the manner in which senior officers from Police Scotland felt able to engage candidly with us, to highlight compliance issues and to take on board the advice and guidance offered. This is an excellent example of how we can work with public authorities to encourage the development of good practice and promote improvements in compliance standards, particularly when deploying the highest level of intrusive covert tactics available.

Daniel Morgan Independent Panel

13.32 On 15 June 2021, the Daniel Morgan Independent Panel published its report.³¹ While recognising that considerable changes had been made to the rules concerning the management of informants since the death of Mr Morgan in 1987, the panel made the following recommendation:

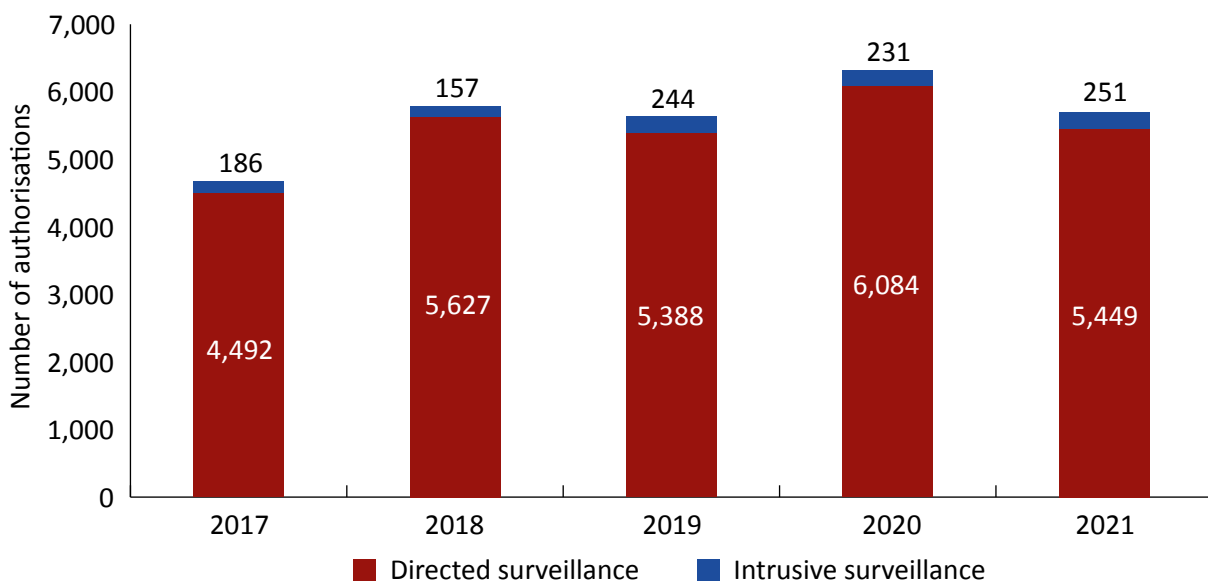
Recommendation 79: The Panel is concerned that the policies and procedures relating to the use of informants by law enforcement agencies still allow scope for corrupt practices, and it recommends that the Investigatory Powers Commissioner takes this into consideration during inspections.

13.33 As set out above, handling the risks associated with the use of CHIS and undercover officers is a key focus for us. Our inspections include interviews with those in handler and controller roles and detailed scrutiny of the paperwork around the authorisation and management of CHIS, to ensure that risks are properly understood and mitigated by individual agencies. We carry out ad hoc inspections as required, should particular concerns arise, and overall findings are set out in our annual reports. This is, and will remain, a core focus of our inspections.

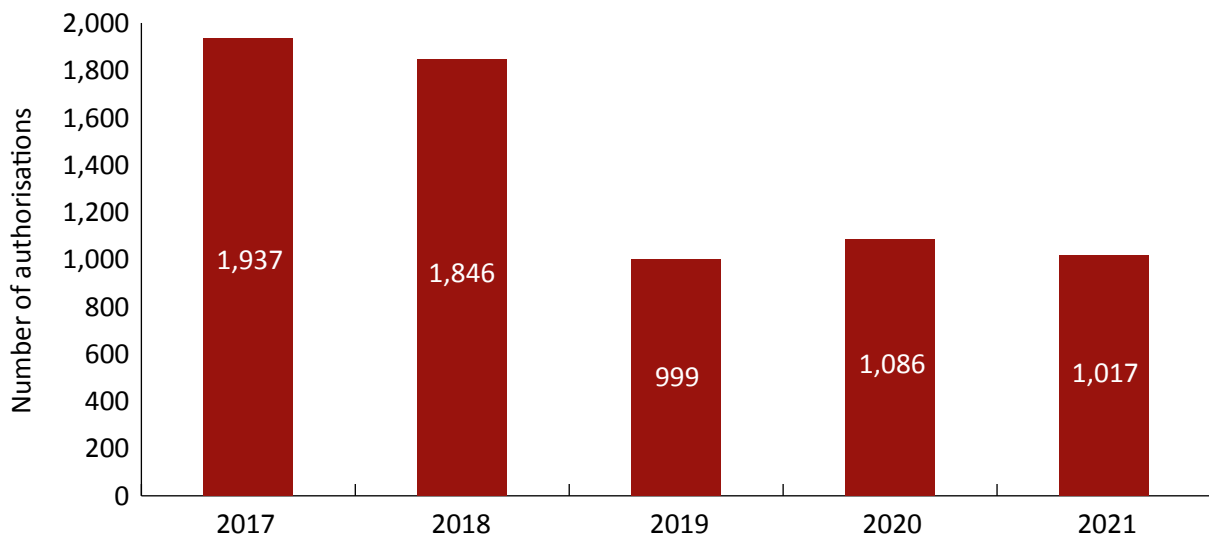
Surveillance and property interference

13.34 There continues to be a good standard of compliance across the LEA community in respect of covert surveillance and property interference authorisations. In our 2020 report, we observed that the administration of urgent oral applications fell below the expected standard. We have continued to include a selection of urgent authorisations in our dip sample reviews during inspections; overall, there have been improvements to the contemporaneous recording of key decisions by applicants and AOs where this had been identified as a matter requiring greater attention to detail.

Figure 13.2: Intrusive surveillance authorisations and directed surveillance authorisations for LEAs, 2017 to 2021



31 See: <https://www.danielmorganpanel.independent.gov.uk/the-report/>

Figure 13.3: Property interference authorisations for LEAs, 2017 to 2021

Legal professional privilege (LPP) material

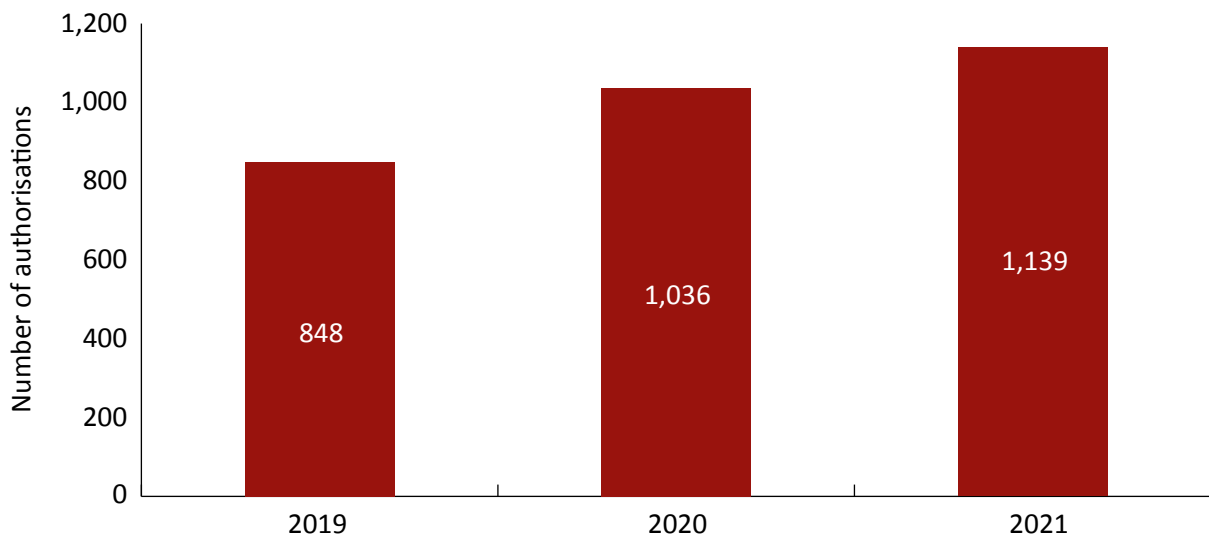
13.35 We continue to identify cases where applications do not properly address the likelihood that LPP material may be obtained as a result of activity authorised. Paragraph 9.54 in the Covert Surveillance and Property Interference Code of Practice directs applicants to include an assessment of how likely it is that information which is subject to legal privilege will be obtained. Many of the cases we identified related to activity conducted after a subject had been released from custody pending further investigation and after they had been in receipt of legal representation. In those cases, applicants dismissed discussion of legal advice in the absence of one of the parties being a qualified legal advisor as not being subject to legal privilege. With some support from *R v Turner* 2013,³² Judicial Commissioners are of the view that where a suspect discusses legal advice in the absence of a qualified legal advisor (such as with an associate), it is necessary to consider the circumstances of that discussion in order to determine if privilege is waived. If waiver is ambiguous, public authorities should err on the side of caution and treat the product as potentially privileged; the retention of such material (for a purpose other than destruction) requires approval from IPCO. In such cases, AOs often fail to identify the shortcoming in the application and consequently do not fully acknowledge the likelihood of acquiring material subject to legal privilege.

13.36 This point has been highlighted as an area of non-compliance and raised as an observation for several organisations and will continue to be an area of focus for Inspectors and Judicial Commissioners. Despite this issue, we remain confident that organisations continue to handle sensitive material appropriately and in line with the legislative requirements.

Targeted equipment interference (TEI)

13.37 As shown in figure 13.4, there were 1,139 TEI authorisations in 2021. Of these, 277 were urgent authorisations.

32 *R v Turner* (Elliot Vincent) [2013] EWCA Crim 642.

Figure 13.4: Targeted equipment interference authorisations for LEAs, 2019 to 2021

13.38 In our 2020 report, we set out the challenges faced by public authorities in applying for TEI warrants.³³ To address these challenges, we revised our inspection model in 2021 to give a greater depth of scrutiny to the use of TEI warrants and associated powers. Because the use of TEI requires specialist equipment and a high degree of training, many LEAs have developed these capabilities within the regional collaboration structures for serious crime and counter-terrorism and, as a result, our revised inspection model has been developed around these regional structures. By way of example, in the East Midlands region the police forces of Leicestershire, Derbyshire, Nottinghamshire, Lincolnshire and Northamptonshire have collectively developed and manage TEI tactics through the East Midlands Special Operations Unit. In addition to the inspection of each of these regional policing units, our revised inspection model includes standalone inspections of those larger LEAs (e.g., the NCA and MPS), where the use of TEI warrants is seen in greater numbers.

13.39 Given the wide variety of techniques to acquire digital data and communications, we have established a multi-specialist team that includes Inspectors experienced in TEI, TI and the acquisition of CD. This allows us fully to explore the boundaries and interdependencies between the disciplines and, in particular, to determine whether or not less intrusive powers can or could have been used to achieve the same objective. For example, in a fast-moving, high-risk operation, the use of a TEI technique may be justified, whereas in a lower-risk, slower-time investigation the acquisition of CD from a telecommunications operator, using the powers under Part 3 of the Investigatory Powers Act 2016 (IPA), could achieve the same result. In circumstances where more specialised technical knowledge is required to establish exactly how a TEI tactic works in practice, members of the Technology Advisory Panel (TAP) have accompanied the inspection team on their visits.

13.40 In 2021, we completed inspections of around a third of the LEAs empowered to use TEI and will complete the remainder during 2022. Early inspections findings are described below:

- some authorities have struggled to adapt to the TEI warrant regime, failing to recognise that the process for TEI has more in common with a search warrant issued by a court than the process to sanction powers under the Regulation of Investigatory Powers

33 Annual Report of the Investigatory Powers Commissioner 2020 (from paragraph 14.49). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

Act 2000 (RIPA) and the Police Act 1997 that were used for these techniques prior to the IPA. Consequently, some authorities have tried to adapt the previous descriptions and principles used for property interference into the TEI regime. This can mean they miss key details required in the application process or omit to submit relevant documentation, resulting in returns for additional work and/or adverse comment by Judicial Commissioners;

- perhaps unsurprisingly, those organisations that utilise TEI warrants in greater numbers and which have developed specialised teams to manage and co-ordinate applications, demonstrate higher levels of compliance than those that only engage the powers infrequently and rely on more generalist staff; and
- there is a significant lack of consistency within regional police units in terms of the application process where, in general, each police force within the collaboration has its own way of doing things. This results in regional teams needing widely to vary their submissions according to the particular requirements set by the force processing the application. This is exacerbated by the individual expectations and requirements set by law enforcement chiefs issuing TEI warrants. In the worst cases we have seen, this results in five completely different ways of doing the same thing and achieving the same objective.

13.41 In 2019, we conducted a thematic inspection of some TEI techniques to benchmark standards of compliance (TEI was brought into effect in December 2018) and look for national consistency. As this was an initial benchmarking exercise, this was not reported on. However, that inspection identified a disparate range of knowledge and understanding when it came to the assessment of collateral intrusion or, in other words, unavoidable interference to equipment other than the targeted devices. It has been pleasing to see in the inspections conducted so far that this situation is much improved. Operators have a good understanding of the risks involved and are able clearly to explain and demonstrate the steps that are taken during deployments to reduce such risks.

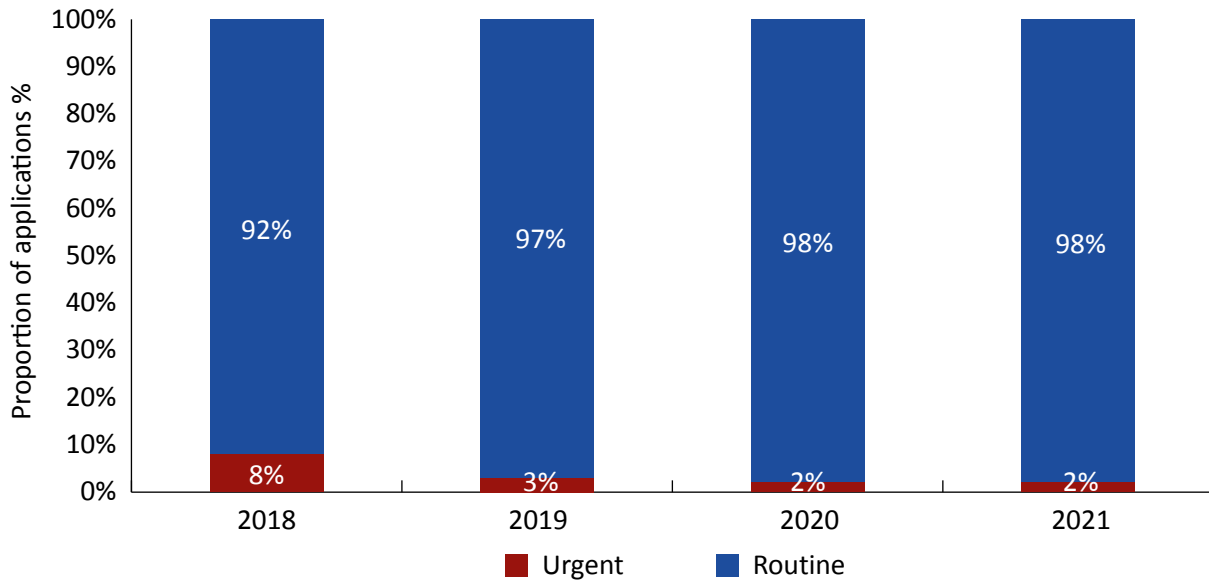
13.42 A key focus of the 2020 inspections was to examine how any data collected through collateral intrusion was being managed. We were concerned in 2019 that data was being kept on a “just in case basis” yet was rarely if ever required for disclosure. The IPC set out clear expectations in this regard and, again, it has been pleasing to see that, in most cases, collateral intrusion data is now deleted as soon as a warrant is cancelled.

13.43 In order to keep up to date and ensure we are sighted on emerging and developing TEI capabilities, as well as to emphasise during such development the core principles of necessity and proportionality that run throughout the IPA, we continue to sit on national TEI working groups.

Targeted interception

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

Figure 13.5: Proportion of urgent and routine applications by LEAs for targeted interception, 2018 to 2021



Law enforcement systems

13.45 Last year, we reported we had started to see some compliance issues on the IT system used by LEAs to manage intercepted material. We indicated that this was an old system and that plans were well underway to develop a replacement. It is disappointing that it has been necessary to reset that project, with a new expected delivery date some three to four years from now. Given the sensitivity of the information involved, it is vital that no more time is lost in taking this forward. It is, however, helpful that we are now regularly briefed on the project plans and we will ensure that compliance with both the IPA and the Data Protection Act 2018 (DPA) remains a critical success factor for the new system.

13.46 In the meantime, we have worked with the Home Office to ensure that the most serious performance and compliance issues on the current system have been addressed. Our concerns remain that others will emerge given the age of the system and we will keep this under close review.

National Crime Agency (NCA)

13.47 We inspected the NCA twice in 2021. The first inspection focussed on a small number of large thematic warrants and the second covered a much wider selection of material. In both inspections, we were given briefings from operational teams and subject matter experts on the NCA's use of TI. Over 2021, we saw good evidence that the NCA uses TI warrants in a way that is compliant with the IPA and the Code of Practice. Some warrants had a high number of modifications; those we reviewed were all presented to a good standard with respect to necessity, proportionality and attribution.

13.48 In our 2020 report, we highlighted a relevant error that had been reported to us by the NCA in relation to the handling of TI material by police Regional Organised Crime Units (ROCU). This error led to a wider review of compliance with the IPA safeguards, which found a number of issues with the way ROCUs were handling and storing TI material received from both the NCA and the MPS. The IPC directed a managed investigation by the NCA and MPS in relation to this and immediate remedial action was taken to make the process compliant

with the relevant safeguards. As a result, a number of relevant errors were reported by both the NCA and the MPS. The compliance issues were around retention and security of TI material. These have now been resolved and new processes are in place. We will be enhancing our inspections of the ROCUs in 2022.

- 13.49 Our 2021 inspection highlighted a difference in the way the NCA distributes TI material to the MPS when compared to the way it distributes to other police forces. While both processes are compliant with the IPA, there was some ambiguity in defining areas of responsibility and a potential weakness in the lack of a clearly defined process or ownership. We have asked the NCA to review the end-to-end processes, to ensure both are consistent with the measures set out in the NCA section 53 safeguards and its own handling arrangements and also to define areas of responsibility for compliance. We will report further on this next year.

HM Revenue and Customs (HMRC)

- 13.50 HMRC's remit includes tobacco and alcohol excise fraud, money laundering, Construction Industry Scheme tax fraud, hydrocarbon oils excise fraud, misconduct in public office, tax evasion and self-assessment fraud. We examined warrants covering all these areas and were satisfied that HMRC has a very good level of compliance with the IPA and the Code of Practice. Warrant applications are clear, concise and well drafted.
- 13.51 HMRC is making good use of thematic warrants and great care is taken to ensure additions are counterbalanced by appropriate deletions of factors when they are no longer necessary and proportionate. Thematics allow HMRC to work at pace and react quickly in fast moving situations. The results have been impressive and the seizures under various operations have clearly demonstrated the value of the interception.

Metropolitan Police Service (MPS)

- 13.52 Our inspection in September 2021 found that MPS (SO15) continues its good track record of compliance with the requirements of the Act and Code of Practice for TI. The inspection was focused on modifications, renewals and cancellations following the approval of a warrant by a Judicial Commissioner and the arrangements in place to safeguard intercept product. Where warrants were modified, this was done within the foreseeable scope of what had been authorised and approved, with the necessity and proportionality fully justified. Individual warrants, including thematic warrants, were well managed to ensure that the interception being undertaken remained proportionate.
- 13.53 As indicated above, we have previously highlighted a relevant error in relation to the handling of warranted TI data by the police ROCUs. While the NCA is the main supplier of TI warranted data to the ROCUs, the MPS also carries out this function. The error led to a wider investigation of compliance with the handling arrangements for both the NCA and the MPS and the reporting of a number of relevant errors by the MPS. We recommended that a memorandum of understanding be developed between the MPS, the NCA and the ROCUs to ensure TI material supplied to ROCUs was always handled in accordance with the supplying agency's (MPS or NCA) policies. We intend to enhance our inspection of the ROCUs in 2022 to check on compliance.

Police Scotland

13.54 Our inspection in June 2021 found that Police Scotland continues its good track record of compliance with the requirements of the Act and Code of Practice. Where warrants were modified, the necessity and proportionality of the conduct authorised was fully justified. Warrants were being kept under constant review. We saw some particularly thorough reviews, renewals and cancellations which detailed the value of the interception to date and, where relevant, the continuing need to undertake interception. Police Scotland demonstrated a clear understanding of the geographical limits of interception warrants granted by a Scottish Minister and the Home Secretary. The safeguarding of intercept product was being diligently managed by Police Scotland, although we recommended the handling arrangements document should be reviewed annually to ensure it remained current.

Police Service of Northern Ireland (PSNI)

- 13.55 Overall, we were satisfied that PSNI had achieved a high level of compliance with the IPA. We examined a number of applications, renewals and cancellations and were satisfied that necessity and proportionality considerations were properly being articulated. We saw good examples of assessments of collateral intrusion.
- 13.56 We examined whether the appropriate amount of detail was being included in minor and major modifications which are not subject to prior approval by Judicial Commissioners. We were satisfied that modifications were being used appropriately and provided the necessary operational flexibility foreseen by the Act. In our view, the modifications fell within the foreseeable scope of the application and renewal documentation set out the scale and scope of operations clearly. We also saw good early use of modifications to remove factors that were no longer deemed necessary.
- 13.57 PSNI has resolved the two compliance matters we referred to in our 2020 report and which related to the retention of IPA data. We have been in correspondence throughout the year, have inspected the areas concerned and we are satisfied that PSNI is now fully compliant.

Communications data (CD)

- 13.58 From our 2021 inspections, we found that, with the exception of the two areas of concern set out below (from paragraph 13.60), the general standard of compliance across LEAs has remained high. The safeguards provided by the Office for Communications Data Authorisations (OCDA) provides through its robust scrutiny and independent authorisation of the necessity and proportionality for all the routine applications (see Chapter 7 for further details) are clear from our inspections. It is also reassuring to see that a positive attitude towards the reduction and elimination of errors prevails (see Chapter 18 for further details).
- 13.59 In 2021, 273,193 CD authorisations were made. These include: authorisations made under section 60A, as authorised by OCDA; warrants authorised under section 61 in the interests of national security (which are not authorised through OCDA); and those made under the urgent provisions.

Figure 13.6: Communications data applications and authorisations for LEAs, 2020 to 2021

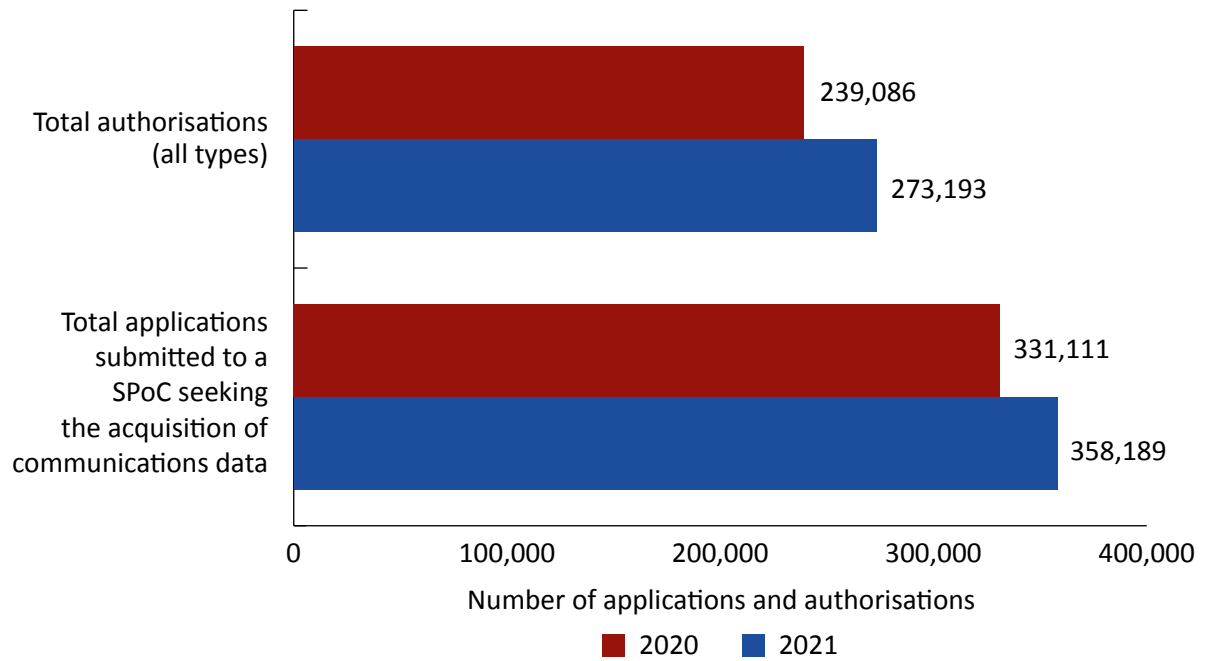
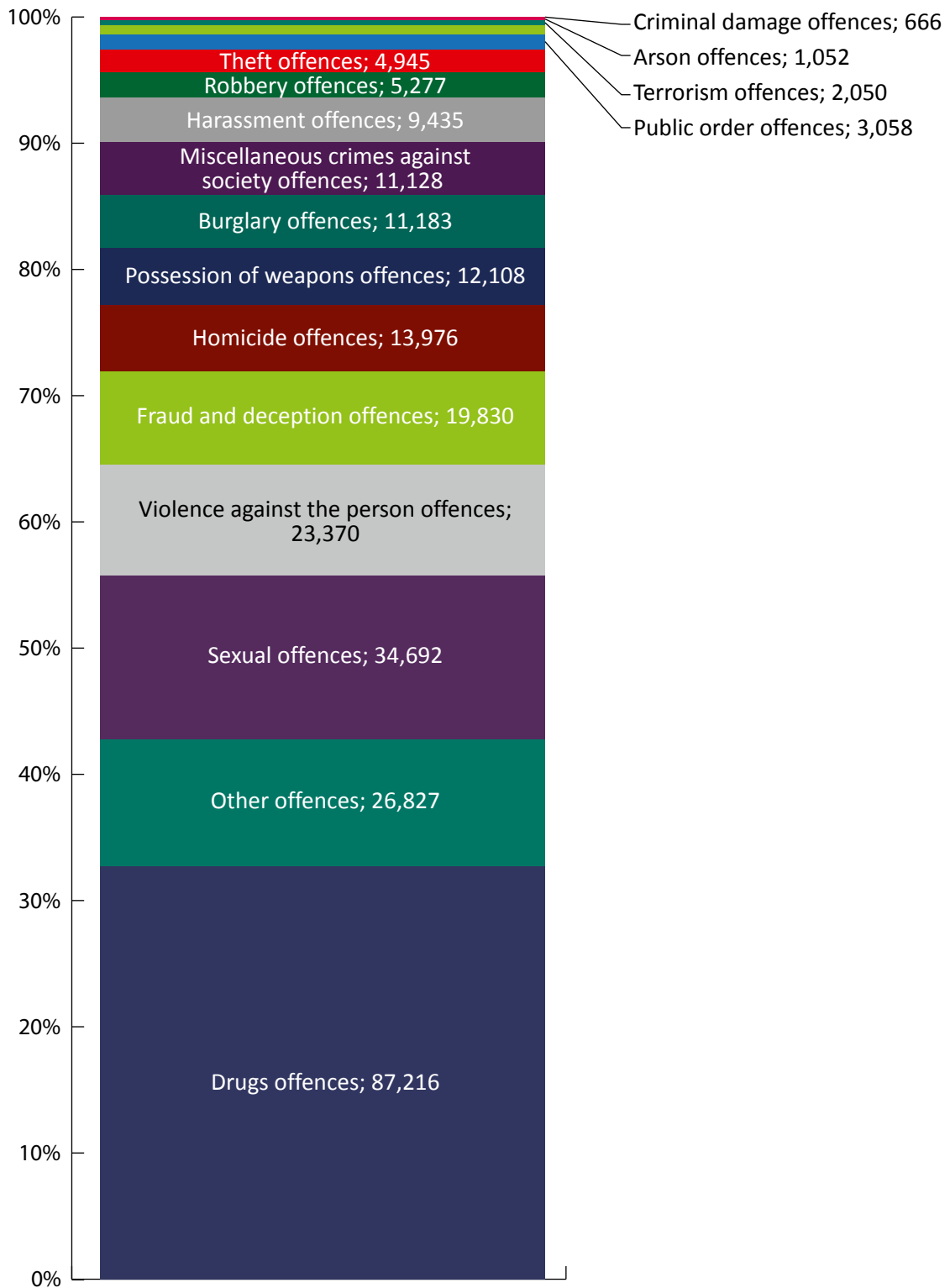


Figure 13.7: Communications data authorisations by offence, 2021



Note: The total number of authorisations shown here exceeds the figure shown in figure 13.6 as an authorisation may relate to more than one offence.

Internal misconduct investigations

- 13.60 We first raised concerns about the acquisition of CD in connection with misconduct investigations in our 2019 report and in 2020 we reported that we had seen little improvement. All too often our inspections had identified cases where aspects of criminal conduct had been conflated with simple non-compliance with police misconduct regulations. While clearly demonstrating bad behaviour or breaches of internal discipline, applications did not sufficiently explain why the conduct was of such a degree to amount to an abuse of the public's trust in the office holder.
- 13.61 We set out in our 2020 report a number of steps to address these concerns,³⁴ all of which we have now completed.
- 13.62 The close scrutiny applied by OCDA has seen a higher number of applications being returned for rework or rejected and, alongside our probing inspections, has made a significant contribution to an overall improvement in the standard of applications. In May 2021, IPCO and OCDA issued guidance to public authorities setting out the minimum expectations that all applications citing Misconduct in a Public Office or related offences would need to satisfy before being considered for authorisation by OCDA. While our inspections in 2021 still encountered some historic examples where we considered the case for acquiring CD had not been satisfactorily made out, it is pleasing to report that, since the circulation of the minimum expectations, we have seen a marked improvement.
- 13.63 The message from the IPC remains clear: all applications to acquire CD must reach the criminal threshold and the reasons for why that criminal threshold has been met must sufficiently be described within an application. This will mean that OCDA can give the request due consideration. Internal misconduct investigations will therefore remain a primary focus of our inspections in 2022.

Freedom of Expression

- 13.64 A further recurring area of concern relates to cases of malicious communications or minor offences under the Public Order Act 1986. In this connected world where so many people live their lives across the myriad of social media platforms, the number of complaints and allegations being dealt with by police about what is said and posted on those platforms has increased. While in many cases the criminal conduct is clear, increasingly we are seeing cases where the material posted may be unpleasant, rude, even offensive, but ultimately falls short of being a criminal offence. The pressure on police to "do something" often results in CD being sought for what could be described as little more than a public falling out or name calling.
- 13.65 We expect applicants in these cases fully to understand the requirements of the offences that are being investigated and ensure that, when providing their reasoning of proportionality, they have not only considered the impact on privacy that comes with the acquisition of CD but have also balanced the impact of what has been said or done against a person's Right to Freedom of Expression under Article 10 of the European Convention on Human Rights (ECHR).
- 13.66 We will set this expectation and raise awareness of the concern during our inspections, through presentations to national CD forums and when assisting public authorities with training events. The theme will be a focus of our inspections during 2022.

34 Annual Report of the Investigatory Powers Commissioner 2020 (from paragraph 14.78). See: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

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

- 13.67 Journalistic freedom is protected under Article 10 (freedom of expression) of the ECHR and we would expect all relevant applications to consider the necessity and proportionality of any request in that context. Most applications relating to journalists fall into the sensitive profession category where a journalist has been a victim of crime.³⁵ However, 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 CD Code of Practice.
- 13.68 Under section 77 of the IPA, authorisations for CD seeking to identify a journalistic source require authorisation by OCDA and the prior approval of a Judicial Commissioner who must consider the public interest in protecting a source of journalistic information. The annual returns provided by public authorities indicated that LEAs had made seven such applications in 2020, although one (the second case listed below) was refused by OCDA before it reached a Judicial Commissioner. All of these were investigated further as part of IPCO's *ex post facto* oversight and details are set out below.
- 13.69 The first case (two applications) involved a police officer suspected of leaking sensitive police information concerning high-profile incidents to a freelance journalist for financial gain. Through the acquisition of CD on the police officer's mobile phone, the application sought to identify contact between them and the journalist around the time of the incidents. Both applications were approved by OCDA and a Judicial Commissioner.
- 13.70 The second case (one application) concerned an anonymous call made to a newspaper reporting the location of a bomb. Incoming call data on the newspaper's landline phone was sought to identify the caller. The application was declined by OCDA as the circumstances of the case did not require the additional considerations required and, after amendment, was authorised as a standard application without the need for Judicial Commissioner approval. As outlined in our 2020 report, it is our view that a statute should not be interpreted as giving any protection to the furtherance of crime in the absence of express words to that effect and that Parliament must have intended to provide a consistent and coherent regime for the protection of journalistic freedoms. Accordingly, we consider that the exclusion of such conduct from the definition of journalistic material in section 264(5) of the IPA should be read into the definition of a source of journalistic information in section 263(1) of the IPA. This application for CD was therefore not to identify a journalistic source as the person's contact with the newspaper was in the furtherance of crime (i.e. to make a hoax bomb threat).
- 13.71 The third case (one application) involved a news editor who reported receiving a communication from a person claiming responsibility for the commission of a serious crime. On an assumption this would have been received via telephone, an application was made to acquire incoming call data for a narrow timeframe. A further application was submitted in relation to such numbers identified through the call data in the hope of identifying the suspect. On the basis that any or all numbers might feasibly relate to legitimate journalistic sources in contact with the editor around the same time, the Judicial Commissioner approved the application.
- 13.72 The fourth case (two applications) concerned an investigation into misconduct in public office where police staff were suspected of leaking information to the media. Both authorisations were approved by a Judicial Commissioner as they portrayed the level of

35 See: figure 19.6.

harm created by the leak; this, in turn, forms part of the necessity case in satisfying the criminal threshold for this offence. The information provided to the media resulted in the victim being contacted by the journalist and the journalist being aware of certain details that had not been made public.

- 13.73 The fifth case (one application) also related to a misconduct in public office investigation involving information suspected of being leaked to a journalist. The information was the name of an officer who was facing a misconduct hearing. In this instance, the Judicial Commissioner did not approve the authorisation. This was due to there being no evidence the allegations had been leaked, nor had they appeared in the public domain several weeks following the suspected leak. As no harm to the public had been caused, the application fell short of the criminal threshold required to acquire CD under the IPA. Such applications have provided clarity that submissions of a similar nature must be clear as to the exact nature of the information supposedly leaked, as well as what the journalist has done with it.

Data assurance

- 13.74 In 2020, we reported on the steps we had taken to benchmark levels of compliance across LEAs with the additional safeguards on the handling of material obtained through the use of covert investigatory powers that were introduced in the 2018 Codes of Practice. We also reported that assessing compliance with these requirements would remain a primary focus of our inspections throughout 2021.
- 13.75 In 2020, initial inspections had been based on a triage of risk, with those authorities deemed to be higher risk prioritised for inspection. The triage considered the nature of the public authority, the covert powers available to it, the extent of use of the available powers and the amount of material likely to have been obtained. Alongside a continuing assessment of compliance, one of our key aims throughout 2021 was to manage the integration of this oversight within the existing inspection regime. The exception to this for 2022 will be the MPS where, given its size and complexity, a further standalone inspection will take place.
- 13.76 At the start of this work, we developed a set of principles for use by public authorities. These were used as an inspection framework during our 2021 assessments. By the end of 2021 we concluded that, while all LEAs were actively working towards full compliance with safeguarding requirements, progress had been mixed. In some forces we saw limited progress due to a lack of priority placed on the extent of work required, coupled with an expectation of national policies being issued by the National Police Chiefs' Council (NPCC) and upgrades required to common IT covert management systems.
- 13.77 Those LEAs that have made significant progress have:
- appointed senior oversight in the form of a management board level SRO;
 - instigated a clear reporting structure such as working groups, steering groups, and compliance boards to escalate compliance risk;
 - taken an organisational approach and included records management leads, legal teams and investigation teams, rather than limit involvement exclusively to covert teams;
 - undertaken the data pathway mapping exercise across the entire organisation; and
 - found additional resource to undertake some of the work, such as project managers, business analysts, or staff to review physical documents.

13.78 Those who have made less progress have:

- left any data assurance work to the relevant covert teams to manage;
- decided to wait for NPCC guidance to be released (issued in February 2022); and
- failed to see the bigger picture and focused on one area of business. An example of this would be a CD SPoC unit ensuring they were fully compliant with all safeguarding requirements and therefore not completing any further work, without understanding that those same requirements extend to material held throughout the force.

13.79 Compliance with the requirements to safeguard material obtained through the exercise of covert investigatory powers will remain a priority theme for us during 2022.

14. Wider Public Authorities

Overview

- 14.1 In addition to law enforcement agencies (LEAs), local authorities and the UK intelligence community (UKIC), a number of other organisations, referred to as wider public authorities (WPAs), have the statutory power to use certain covert tactics. A full list of these is set out in Annex A. The nature and extent of the powers used across the WPAs varies depending on their specific functions. Several are empowered to authorise the use of directed surveillance and the acquisition of communications data (CD), whereas property interference and intrusive surveillance powers, which require a higher level of authorisation, are limited to a smaller number of organisations.

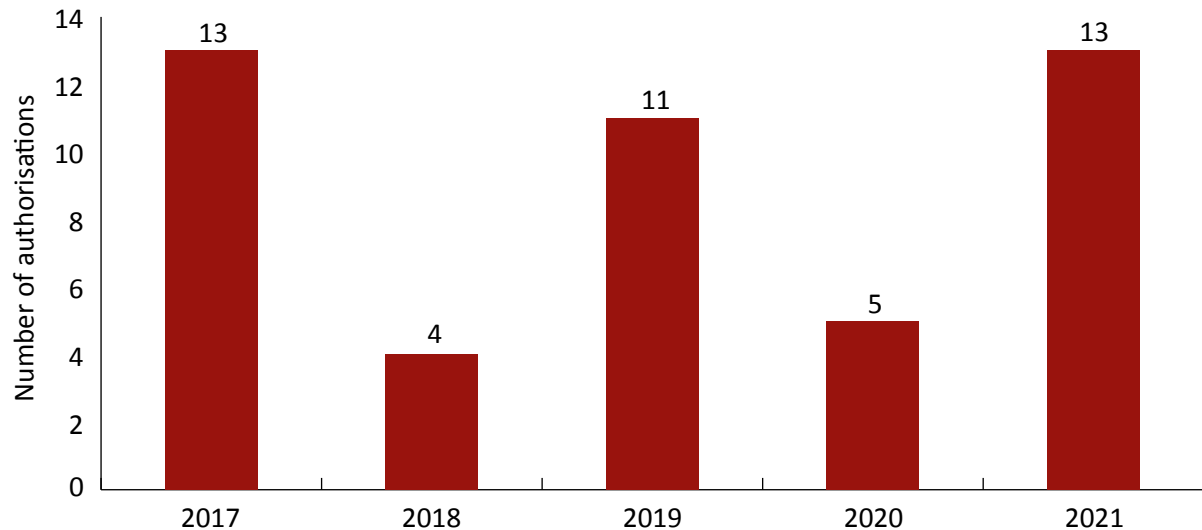
Findings

- 14.2 In 2021, we conducted 52 inspections of WPAs. In line with our new hybrid inspection model, several of the WPA inspections were conducted remotely.
- 14.3 Many WPAs are responsible for investigating discrete types of criminality, such as fraud or environmental crimes, and may have certain thresholds to reach before a prosecution can be brought. Many of those we meet as part of our inspections have investigative skills honed over their time with these specialist organisations and many have come to them following careers in LEAs. The above factors have a bearing on the number and types of covert activities across a given year, as well as the general compliance standards found during inspections.

Covert human intelligence sources (CHIS)

- 14.4 The use of CHIS powers among WPAs remains relatively low, with many authorities choosing not to exercise their powers.

Figure 14.1: Covert human intelligence source authorisations for WPAs, 2017 to 2021



14.5 During our inspections, we found that non-users of directed surveillance and CHIS focused on the procedures in place to ensure that Authorising Officers (AOs), applicants, investigators and intelligence officers were aware of the most recent guidance, good practice and legislation to guard against any inadvertent drift into territory for which an authorisation should be in place. Inspectors review policies to ensure that they represent the most recent Codes of Practice and that refresher training on the Regulation of Investigatory Powers Act 2000 (RIPA) is provided. Examples of where authorities operate such policies and procedures include:

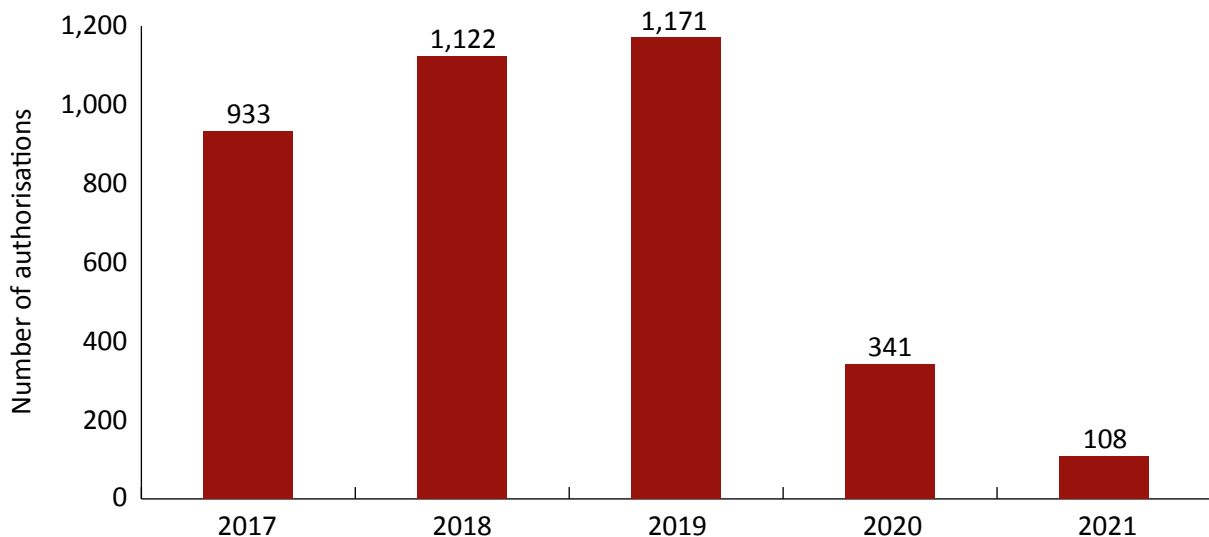
- at the Environment Agency, members of the public who are willing to provide intelligence about environmental crimes are treated as “Confidential Sources” and are often advised that any further information should be provided via Crimestoppers. In these circumstances, we have highlighted the importance of taking account of the potential risks to that individual from their reporting, regardless of whether individuals go on to become registered CHIS or not;
- at OFSTED, we found that the guidance provided to staff outlining the key principles underpinning the tactic was of a high standard and should enable staff to be aware of situations where potential considerations of CHIS may be necessary. This helps to guard against unauthorised activity and should benefit staff who may interact with members of the public offering information, particularly those who may do so repeatedly; and
- while the Department for Work and Pensions (DWP) no longer retains the power to authorise the use and conduct of CHIS, it does receive approximately 800,000 allegations annually from both members of the public and its own staff. To mitigate the risk of unauthorised CHIS activity and status drift, DWP has created a referral process in which all named sources who potentially meet the definition of a CHIS are assessed by a member of staff with the relevant experience.

Directed surveillance and property interference

14.6 The use of directed surveillance varies across WPAs and overall use of the tactic has decreased in the last two years. For example, the DWP had to refocus its workforce onto other areas during the Covid-19 pandemic and, as a result, its use of the powers decreased

significantly. Additionally, changes in external and internal practices in some organisations have resulted in less requirement for covert tactics. For example, although the Driver and Vehicle Standards Agency still made use of the powers, work had been carried out to limit the opportunities to commit fraud relating to vehicle and driver testing, which therefore reduces the need regularly to employ covert surveillance tactics.

Figure 14.2: Directed surveillance authorisations for WPAs, 2017 to 2021



14.7 Across our inspections, we saw on the whole a good standard of applications and authorisations. Some of the areas of good practice we identified include:

- the application process employed by the Environment Agency which included the requirement to submit applications via a small group of trained gatekeepers. This ensured that an accurate record was made of activity within the central record of authorisations and that high standard documentation was submitted to AOs for consideration; and
- following observations made on previous inspections, we were pleased to see that the Serious Fraud Office's applications included more succinct intelligence cases rather than the unnecessarily detailed descriptions of the type we had previously seen.

14.8 At the DWP, we found there continued to be a protracted delay between the receipt of an allegation to trigger an investigation and the authorisation of directed surveillance. It was not uncommon for these delays to extend to 14-16 months. The failure to act on this information timely potentially undermines the necessity and proportionality grounds of the deployment.

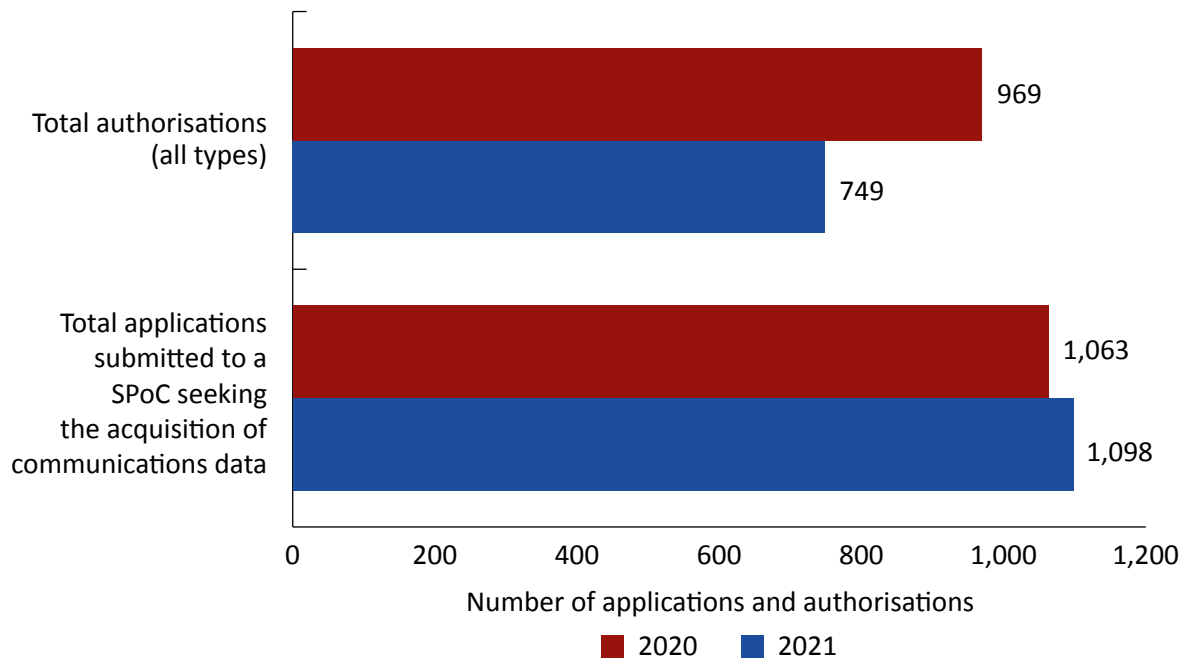
14.9 In 2021, none of the WPAs who are authorised to use property interference or intrusive surveillance powers made any applications to use them.

Communications data

14.10 The volume of CD acquired by WPAs is low but, despite the infrequent use, our inspections of WPAs during 2021 identified a generally good standard of compliance. We were satisfied overall that the documentation justified the principles of necessity, proportionality and collateral intrusion and provided a sufficient outline of what can, in many cases, be quite

complex investigations. We made a small number of recommendations, most of which related to administrative procedures.

Figure 14.3: Communications data applications and authorisations for WPAs, 2020 to 2021



- 14.11 While a small number of WPAs can call on internal authorisation in cases of life at risk urgency (for example the Maritime and Coastguard Agency), we rarely see this option being exercised. All routine applications must be submitted to the Office for Communications Data Authorisations (ODCA) for independent consideration.
- 14.12 In 2020, five additional authorities were added to the IPA schedule and given powers to authorise the acquisition of CD. In October 2021, we undertook our first inspection of the UK National Authority for Counter Eavesdropping (UK NACE) which provides guidance and operational support to the UK Government and friendly foreign governments on detecting and protecting against technical espionage. The findings from this inspection were reported to the IPC in early 2022 and we will cover them in our 2022 report. In addition, we carried out preliminary inspections of the Pensions Regulator, the Insolvency Service and the Environment Agency, all of whom are low users of the power and where we found no issue regarding their use. The inspection of the Civil Nuclear Constabulary will take place in 2022.

Data assurance

- 14.13 During our data assurance programme, all WPAs were contacted and asked to complete a self-assessment which was triaged by our data assurance team. Her Majesty's Revenue and Customs (HMRC) and Home Office Immigration Enforcement (HOIE) were selected for follow up inspection, with the remainder offered early guidance on the steps required to achieve compliance and the level of scrutiny and validation to expect at their next routine inspection. Both HMRC and HOIE have made good progress against the requirements since their inspections.

15. Local Authorities

Overview

- 15.1 Local authorities can make use of a limited range of investigatory powers: directed surveillance, covert human intelligence sources (CHIS) and the acquisition of communications data (CD).
- 15.2 During the pandemic, we switched to remote inspections of local authorities to minimise physical visits. Experience shows that, for normally minimal users of the powers, this is a productive and efficient way of monitoring compliance within local authorities, both for us and for them. We will, of course, continue to arrange site visits where necessary, for example where powers have been used at a significant level or poor performance has previously been demonstrated.

Findings

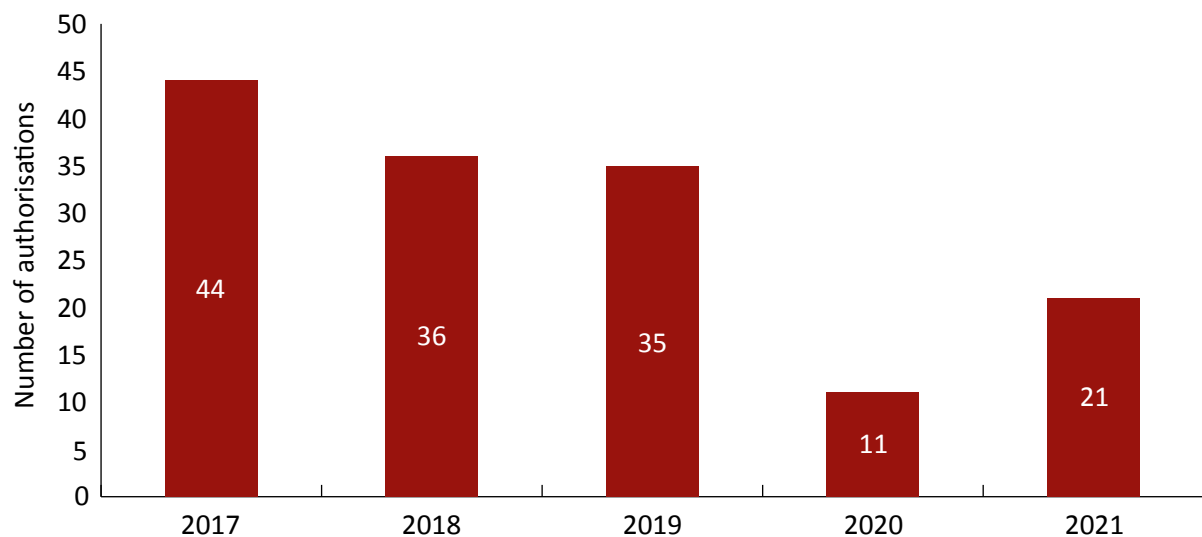
- 15.3 Local authorities are inspected every three years. We carried out 105 inspections in 2021.
- 15.4 Although local authorities continue to be low users of investigatory powers, a small number account for a significant proportion of authorisations. In part, this appears to be due to familiarity with how the powers may be used for positive effect, together with confidence derived from successful use. For active users of the powers, we look for evidence of the maintenance and documentation of internal processes for the management of authorisation requests and the regular training of key personnel, particularly Authorising Officers (AOs). We often find that corporate policies and procedures have not been updated in line with legislative changes, or to reflect changes in key personnel, and the requirement that elected members are provided with an update (as required by the Codes of Practice) has often fallen by the wayside. These matters are often identified only when the inspection is announced, although we encourage local authorities to maintain ongoing internal governance in between our visits. Similarly, while we understand that awareness training for the Regulation of Investigatory Powers Act 2000 (RIPA) has been impacted by the pandemic, some councils have taken the opportunity to introduce online learning modules. A number of councils were reassuringly compliant in several regards, notably, although not exhaustively: Dover District Council; Stirling Council; Basingstoke and Deane Borough Council; Maidstone Borough Council; Neath Port Talbot County Borough Council; Cardiff Council; Huntingdonshire District Council; Mid Sussex District Council; and Bournemouth, Christchurch and Poole Borough Council.
- 15.5 RIPA powers continued to be used to investigate a range of crime types, including the sale of dangerous and counterfeit goods, significant fly tipping events/hotspots and housing related matters such as subletting combined with right-to-buy fraud. Powers are most often used by individual authorities but we do see examples of success by partner investigation units where more than one authority or agency work together to achieve operational outcomes. An example of this was seen in our inspection of Hampshire County

Council, which collaborated with the National Trading Standards and the Federation against Copyright Theft (FACT) to use its powers in relation to unlawful TV streaming with an international reach and for which, in March 2022, the perpetrators were imprisoned. The applications and authorisations in this case were of an excellent standard.

Covert human intelligence sources (CHIS)

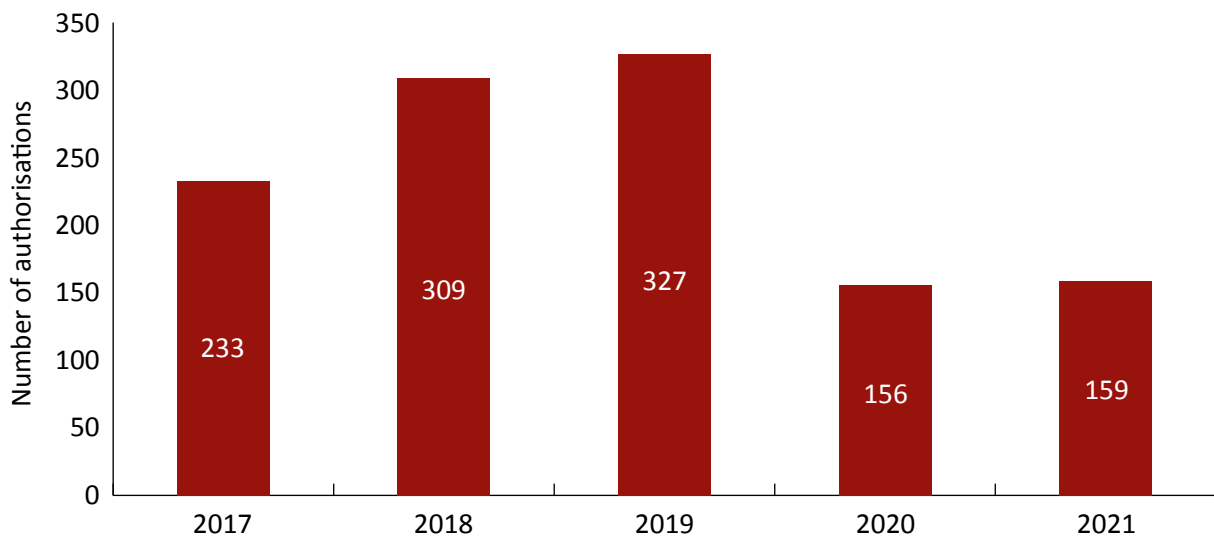
15.6 As shown in figure 15.1, local authorities continue to utilise CHIS authorisations in low numbers. During 2021, examples were seen of test purchase activity using suitably authorised members of staff who engaged with online sellers, most commonly on online selling pages, to arrange a physical meeting to secure and evidence the sale of counterfeit items. It is extremely rare for local authorities to use external CHIS in the context seen by other RIPA users. Where the use of a CHIS is identified as necessary, it is more common for councils to work in partnership with other agencies, such as the police, who have the required skills and infrastructure required to manage the risks associated with CHIS.

Figure 15.1: Covert human intelligence source authorisations for local authorities, 2017 to 2021



Surveillance

15.7 Figure 15.2 shows that the use of directed surveillance across local authorities has remained broadly consistent in the last two years. While there is no direct analysis to rely upon, it seems highly likely that the pandemic, with the increase in working from home, has had a bearing on the reduction in usage over the past two years.

Figure 15.2: Directed surveillance authorisations for local authorities, 2017 to 2021

- 15.8 Physical surveillance continues to be conducted mostly through the use of remote static observation posts. We have seen examples of this tactic being used to identify who is residing within a defined domestic premises to confirm or refute allegations such as council tax fraud arising from undeclared joint occupation. In these cases, Inspectors expect that AOs limit the scope of observations to minimise collateral intrusion, for example by restricting the location of a static camera to a position that only captures images of occupants entering and leaving the relevant address, rather than a wider view where passing members of the public may be seen.
- 15.9 Similar considerations are relevant to observations conducted within locations known to be hotspots for fly tipping or the large-scale dumping of hazardous waste. These are often isolated rural or industrial locations. In such cases, the intention is to capture images of vehicles used in order to further investigations. Our expectation is that any surveillance is sufficient to capture the required information only and not excessive in terms of overlooking neighbouring premises.
- 15.10 Three elements arise most often in the feedback given to local councils following our inspections. These are:
- the articulation of proportionality cases in surveillance applications. Paragraph 4.6 of the Covert Surveillance and Property Interference Code of Practice requires that applicants address four distinct elements of proportionality in sufficient detail that the AO can make a meaningful assessment of the suitability of covert surveillance. We often find that proportionality arguments rely overly on the seriousness of the activity, or on somewhat bland assertions that the covert activity is the only way in which the criminality can be tackled. As the Codes set out, more detail is needed from both the applicant and AO to demonstrate whether other methods of investigation have been tried or ruled out, as well as whether the planned covert activity is justifiable in its scale and potential impact on both the subject of interest and those who might be affected through collateral intrusion;
 - the need for the AO to articulate in their own words why they are authorising directed surveillance and clearly to state what has been authorised. Authorising an application for covert surveillance must not be seen as a purely bureaucratic sign off or rubber stamp exercise: the AO has been given the personal responsibility, through legislation,

of acting in a quasi-judicial capacity (in England and Wales) prior to the approval of the magistrate; and

- the processes that underpin the authorisation function, such as the date and time of authorisation, duration and prompt cancellation. We often see examples of cases where directed surveillance is authorised for an incorrect duration (less than three months), where regular reviews are not undertaken or where authorisations have been allowed to expire or have lapsed purely because they have reached their expiry date. In the latter case, this fails to comply with the requirement to cancel an authorisation when it is deemed no longer necessary.

Internet and social media

15.11 We continue to scrutinise local authorities' use of the internet as part of their investigations or enforcement responsibilities. We seek to ensure that inadvertent covert surveillance has not been conducted via the repeated and sustained observation of social media profiles or other online information, or a CHIS relationship engaged through meaningful contact with another individual online. This risk is most effectively managed when councils take steps to define clearly what conduct their staff are permitted to undertake without engaging RIPA considerations. This can include undertaking a brief initial assessment of a person's online presence to identify if such material might be of relevance to an existing investigation.

15.12 Where a local authority identifies that the monitoring or recording of a person's online content, such as a social media profile, is necessary and proportionate and has been suitably authorised, we suggest that an auditable record is maintained of:

- the means that are used to facilitate the surveillance;
- who can use those means, when they are used and for which investigation; and
- what searches and monitoring are undertaken. These should then be reviewed by the relevant AO to ensure that they have been conducted within the limitations of the authorisation.

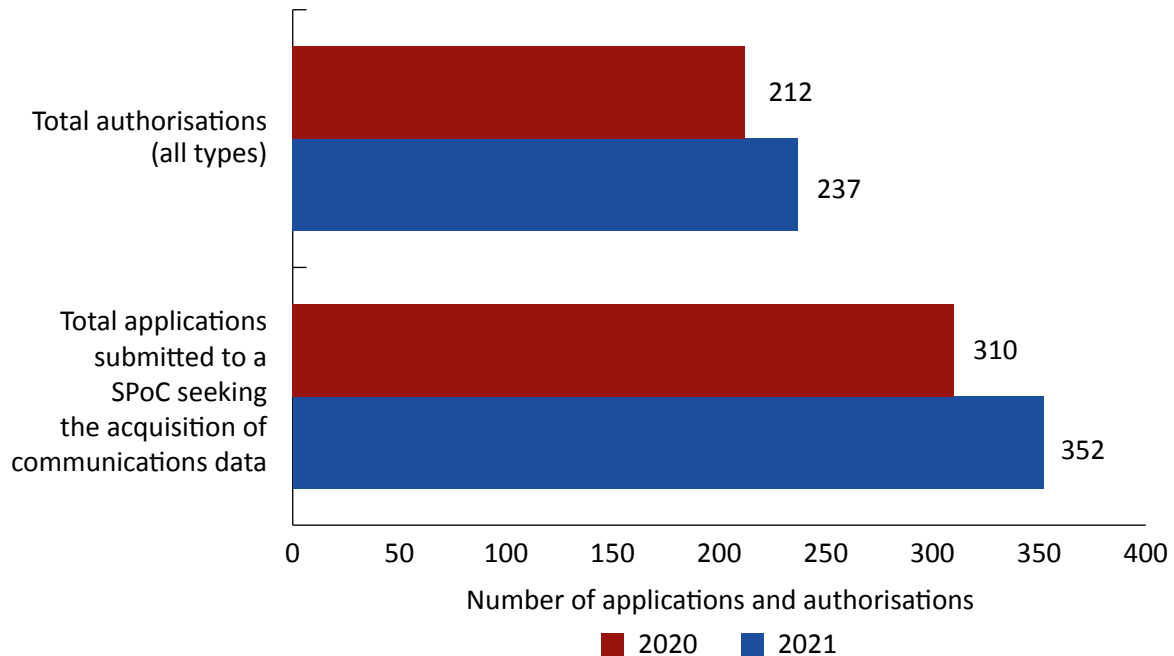
15.13 Some local authorities choose regularly to audit online activity undertaken by staff. This can be a useful way of identifying training needs or where more detailed guidance needs to be provided.

Communications data (CD)

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

15.15 We have highlighted our support for this sound and well established process in previous reports, not only for the national consistency and legally compliant applications that result but also for the excellent CD and Investigatory Powers Act 2016 (IPA) training packages offered to local authority investigators and senior managers. Our 2021 inspection of the NAFN identified a continuing regime of good compliance and raised no areas of concern; once again we were impressed by the level of knowledge and professionalism of the staff at the NAFN.

Figure 15.3: Communications data applications and authorisations for local authorities, 2020 to 2021



Data assurance

- 15.16 Every local authority in England and Wales has been notified in writing by the Investigatory Powers Commissioner (IPC) of the requirement to comply with the data safeguards contained within Chapter 9 of the Covert Surveillance and Property Interference Code of Practice and Chapter 8 of the CHIS Code of Practice. Consequently, our Inspectors have been tasked with assessing compliance with these safeguards during their routine inspection activity.
- 15.17 Most local authorities have in place an internal policy concerning the retention, review and deletion of material obtained during investigations, although it is unusual for RIPA material to be categorised separately within retention schedules. It is important that information obtained in the course of surveillance or CHIS operations is subject to regular review to ensure that its retention can be justified. On our inspections, we ask local authorities to confirm if they hold any RIPA material that does not comply with their internal retention schedule. In some cases, this has resulted in the immediate review of the central record of authorisations and destruction of associated records.
- 15.18 We encourage local authorities to maintain good document management practice to ensure that all RIPA material is retained within a structured format; material should easily be identifiable and only one copy of relevant records should be kept. It is the responsibility of the Senior Responsible Officer for RIPA matters to provide assurance that data safeguarding considerations have been complied with and this should be reflected within the regular reports made to council members.

16. Prisons

Overview

- 16.1 We inspect Her Majesty's Prison and Probation Service (HMPPS), the Northern Ireland Prison Service (NIPS) and the Scottish Prison Service (SPS), along with a selection of prisons across England, Wales, Northern Ireland and Scotland.
- 16.2 We carry out inspections of prisons to ensure that communications monitoring is conducted adequately and that any use of surveillance techniques or covert human intelligence sources (CHIS) is compliant with legislation and the Codes of Practice. On our inspections of the use of the interception of communications we also assess compliance against the relevant guidance in England and Wales, Northern Ireland and Scotland.

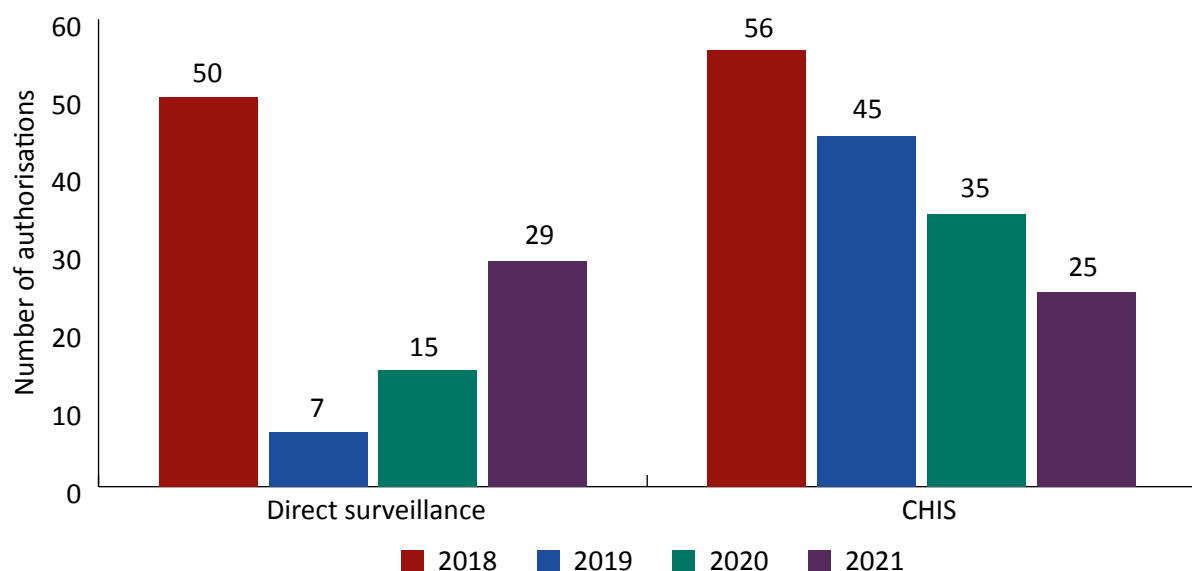
Findings

- 16.3 Our inspections of prisons were largely disrupted during 2020 and we are grateful to HMPPS for assisting a return to onsite inspections in 2021. We conducted 76 inspections in 2021.
- 16.4 We continue to be concerned about the arrangements in place regarding the interception of communications and, as we set out in our 2020 report, we are working with HMPPS to resolve this. We are grateful for the constructive engagement on this matter. We recognise the challenging environment in which HMPPS is trying to bring about change and acknowledge that progress has been made. However, it remains the position that the legislative and policy framework is insufficiently robust and we expect to see significant progress with the implementation of a new Prison Service Instruction (PSI) in 2022.
- 16.5 We see considerable variations in compliance levels across the prison estate. We continue to identify in our reports training issues and emphasise the importance of embedding awareness and understanding of the relevant policies when people are appointed to security roles. The holistic approach now being taken by HMPPS to look at the level of compliance across the estate should enable greater consistency in the future and we hope to see further improvements over the next year.
- 16.6 During the summer of 2021, we undertook a thematic investigation into the safeguards in place to protect intercept material on the PIN phone system. We visited a representative sample of six prisons and we identified a number of issues (see paragraph 16.20 for further details). In some of the prisons visited, we found that an unacceptably high proportion of monitored calls either lacked authorisation or the record of the authorisation was not in accordance with the PSI; this meant that no assurance could be given that a significant proportion of monitoring was necessary and proportionate. We will continue to monitor how HMPPS takes forward our recommendations.

Covert human intelligence sources (CHIS) and surveillance

16.7 As shown in figure 16.1, the number of directed surveillance authorisations has increased and the number of CHIS authorisations has decreased. We have noted an obvious improvement in the standard of applications and authorisations particularly regarding directed surveillance. The use of Prison Rule 50A has continually been highlighted as a concern in previous reports but HMPPS has taken the positive step of rewriting the guidance for when it should be used. Once the consultation process has been carried out, Rule 50A will be used for the purpose of prisoner safety and, in limited circumstances, to support investigative activity.

Figure 16.1: Covert human intelligence sources and directed surveillance activity at Her Majesty's Prison and Probation Service, the Scottish Prison Service and the Northern Ireland Prison Service, 2018 to 2021



16.8 Since our last report, HMPPS has embedded its overarching “Policy Framework” and “Operational Guidance” across the wider estate for the authorisation, management and delivery of CHIS and surveillance. This year’s inspection demonstrated continued progress in compliance with the legislation and Codes of Practice.

16.9 The introduction of an internally developed IT solution is assisting with the challenge of managing all authorised activity. Once the new system is completely tested and fully operational across all aspects of surveillance and CHIS, any compliance concerns should be eased. The Covert Authorities Bureau (CAB) has undergone a restructure, increased its level of vetting for staff and introduced tighter control and management of authorisations.

16.10 Our 2021 inspection incorporated a focus on the new regional operating model and the Long-Term High Security Estate (LTHSE). All regions are now resourced and operating in some capacity. A cadre of regional and national Authorising Officers (AOs) has been recruited and accredited and there is already an obvious improvement in compliance. Regional staff are developing strong relationships with trained and vetted staff within prison establishments to ensure the safety and security of both CHIS and handling teams remain a priority throughout.

- 16.11 At the time of our last inspection, the LTHSE had not moved to the regional operating model. While we acknowledge that managing covert activity across the LTHSE presents unique challenges and risks, using a consistent operating model would be beneficial. Our concerns were raised directly with the SRO and their team and actions are already advanced to bring the management of covert activity across the LTHSE in line with the wider HMPPS estate. Its incorporation into the new Directorate of Security will no doubt help standardise the HMPPS approach.
- 16.12 HMPPS continues to work closely with its partners to improve the awareness and management of CHIS managed in prisons by other agencies. The structure of the Prison Source Working Group is currently under review, but HMPPS is fully involved in that review and will continue to co-chair the group going forward.
- 16.13 HMPPS has made little progress in relation to the management of surveillance product, largely due to the impact of the pandemic. We have agreed to conduct a further inspection during the next year which will focus specifically on the arrangements and compliance with the safeguarding measures outlined in the relevant Home Office Code of Practice.

Interception

- 16.14 Section 49 of the Investigatory Powers Act 2016 (IPA) provides for the lawful interception of communications in prisons if carried out in the exercise of any power conferred by or under the Prison Rules. The arrangements for the interception of communications in prisons exist to prevent inappropriate use of telephones and letters, for example, to harass victims or witnesses or facilitate criminal conduct.
- 16.15 Prisoners' communications with their lawyers, Members of Parliament (MPs) and several other organisations are privileged, or confidential, and should not be read or listened to other than in the most exceptional circumstances. We have reported previously that there is a lack of safeguards for the handling of the inadvertent interception of such material and we continue to work with HMPPS, the Ministry of Justice and the Home Office to explore how this vulnerability can be addressed.
- 16.16 While we have described in previous reports how the arrangements for the monitoring of communications have, in general, been in accordance with Prison Rules, we have become increasingly concerned with the inconsistency of compliance we see from our inspections and the need repeatedly to highlight the same areas of vulnerability or failure. We believe one of the primary reasons for this inconsistency is the PSI that regulates such activity. This is, in our view, overly complex, often contradictory and conflates the principle of an interception regime based on necessity, proportionality and the recognition of human rights, alongside general directions to ensure safety and good order.
- 16.17 Common findings have included a failure of AOs to provide sufficient reasoning of necessity and proportionality, a lack of justification when an authorisation is reviewed or extended, incomplete authorised monitoring, therefore undermining any grounds of necessity and proportionality given at the outset, and an inconsistent approach to record keeping.
- 16.18 We have worked with HMPPS throughout 2021 to address these concerns and we have been encouraged by the positive response. At the end of 2021 we were provided with a first sight of some draft proposals and, after providing our feedback, we expect the revised PSI to be implemented in the summer of 2022. We will monitor the progress and impact of these revisions and report our findings.

- 16.19 For a number of years now, it has been our view that the reliance upon the prisoner to inform the recipient of a telephone call that their discussion is being recorded and may be monitored, is not satisfactory. Taking these concerns on board, HMPPS ran a pilot across a number of prisons using an overt announcement during 2021. We are pleased to learn that, after some further evaluation and refinement, this announcement will formally be rolled out in 2022. This will bring England and Wales into line with the approach in Scotland, Northern Ireland and in many other foreign jurisdictions.
- 16.20 In the latter half of 2021, with the full co-operation and support of HMPPS, we conducted a thematic inspection of the system used to record (intercept) and monitor telephone calls on the PIN phone system. We visited a representative sample of six prisons where authorisation records were compared against the monitoring that was known to have taken place. In some of the prisons visited, we found insufficient controls on who can access the system, what can be accessed, and a lack of training and guidance for staff using the system. We were most concerned that, for a significant proportion of the calls monitored, no authorisation records could be produced. While HMPPS has sought to reassure us that monitoring would have been justified, for example in urgent cases or where an immediate response was required, rather than any nefarious reason, in the absence of such records we can give no assurance that all monitoring was necessary and proportionate. We also identified that improvements could be made to the control measures in place for protecting legal calls.
- 16.21 The IPC has since discussed these findings with HMPPS who has welcomed the report and committed to use the detail to inform the revision of the PSI. Safeguarding advice will also be used to assist with building "compliance by design" into the specification for the renewal of the monitoring system that is now due. We will monitor this progress and report in due course.

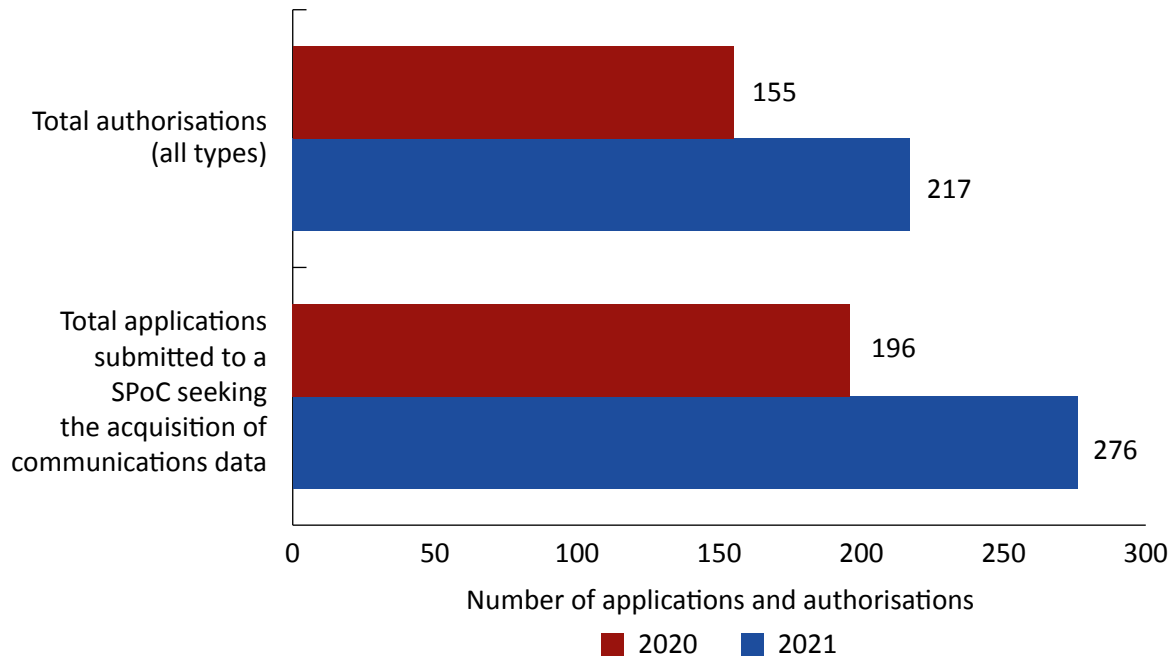
Prison Interception: Northern Ireland and Scotland

- 16.22 As a result of restrictions brought about by the pandemic and numerous outbreaks of Covid-19 across the prison estate, our plans to conduct inspections of prisons in Northern Ireland and Scotland had to be postponed. As a result, completing inspections of all prisons in these jurisdictions will be a priority in 2022.

Communications data

- 16.23 The acquisition and disclosure of CD is undertaken by the HMPPS Digital Media Investigation Unit and, unless a case meets the urgency criteria, all applications for CD are considered independently by the Office for Communications Data Authorisations (OCDA). There were no areas of non-compliance identified in our 2021 inspection. A good standard of applications was evident and our observations were limited to minor areas of administration and suggestions on how the efficiency of the process could be improved.

Figure 16.2: Communications data applications and authorisations in prisons, 2020 to 2021



Data assurance

- 16.24 Although the safeguarding of records and material derived from prison interception is governed by the PSI, rather than the IPA Codes of Practice, our inspections adopt the same process of audit that we apply to material obtained through the use of other covert powers. This is to ensure that such material is held securely, reviewed and deleted in line with those requirements.
- 16.25 The findings from our inspections to date are mixed. In some prisons, staff are aware fully of the requirements to ensure that the content of intercepted communications (mail, email or telephone calls) is deleted after 90 days and that, in general, authorisation records should be retained for six years; in other prisons we have found a lack of consistency and understanding. Problems include, for example, uncertainty as to who is responsible or how and where material should be stored, reviewed and ultimately disposed. On occasions, we have identified material that has been held beyond the 90-day limit and have required its immediate destruction. We have been working with HMPPS to strengthen the safeguarding procedures within the expected revisions to the PSI and this area will remain a focus for our inspections during 2022.

17. Warrant Granting Departments

Overview

17.1 Our inspections vary across the Warrant Granting Departments (WGDs) depending on which intelligence agencies or law enforcement bodies use them and the powers available to them. We conduct annual inspections at each department, reviewing casework across the powers they authorise. At the Home Office and the Foreign, Commonwealth and Development Office (FCDO), inspections cover interception, equipment interference and bulk powers under the Investigatory Powers Act 2016 (IPA), as well as property interference and overseas powers under the Intelligence Services Act 1994 (ISA) and intrusive surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA). At the Northern Ireland Office (NIO), we inspect interception, equipment interference, property interference and intrusive surveillance. At the Scottish Government, which is not involved in national security authorisations, we inspect interception.

Findings

Home Office

- 17.2 The Home Office is providing robust quality control and good advice to the Secretary of State about reviews and the specificity and breadth of thematic warrants. It should continue to adopt a proactive approach with agencies to ensure that new technical developments are fully compliant with the relevant safeguard policies and that the Secretary of State is aware of these when exercising necessity and proportionality judgements.
- 17.3 The Home Office reported an error to us in the autumn of 2021 in relation to the signing of out-of-hours IPA warrants. Although the matter was immediately drawn to our attention, it reflects an approach that has been applied to out-of-hours urgent warrants over several years. The Home Office immediately put in place arrangements, with which the IPC was content, to rectify the problem. The Home Office is investigating the full extent of the issue and we expect a detailed report during 2022.
- 17.4 As a result of being made aware of this issue, the IPC wrote to all intercepting agencies asking them to review their out-of-hours processes alongside the IPA and the Codes of Practice to ensure they were compliant. We will follow up on the responses and any action taken in our 2022 inspections.

Foreign, Commonwealth and Development Office (FCDO)

- 17.5 Overall, consistent with our findings in our 2020 report, we were satisfied that FCDO officials continued to provide high quality advice to the Foreign Secretary, enabling them to discharge their functions both when approving warrants and authorisations and when ensuring appropriate arrangements were in place at the Secret Intelligence Service (SIS)

and the Government Communications Headquarters (GCHQ) for handling warranted data. This includes the proactive and rigorous response by officials to compliance issues as and when they arise.

- 17.6 In our 2020 report, we noted that the then Foreign Secretary had imposed conditions on some authorisations issued under section 7 of the Intelligence Services Act 1994 (ISA). Some of these conditions could cause uncertainty as to what was and was not authorised. The FCDO now has a process in place to clarify what the scope of the authorisation ought to be where the Foreign Secretary has imposed conditions, consulting as necessary with their private office before issuing a minute with the authorisation giving a clear statement of the conditions imposed.
- 17.7 We reviewed two submissions engaging The Principles which, respectively, involved a real risk of torture and unlawful killing. The Principles make clear that, where there is a real risk of torture, extraordinary rendition or unlawful killing, “the presumption would be not to proceed”. While the application and the FCDO’s covering advice presented the risks accurately, they made no reference to this presumption. The lack of clear references to this presumption is not unique to the FCDO, as we have identified a similar issue in Home Office advice as well as in submissions prepared by some of the Principles partners (see paragraphs 12.5 and 12.6). We repeat our conclusion that it is crucial that, where the presumption arises, Ministers are specifically asked to turn their minds to it as it shifts the balance in favour of refusing the authorisation sought.

Northern Ireland Office (NIO)

- 17.8 We were satisfied that the NIO is discharging its function as a gateway for advice to the Secretary of State to a very high standard. Officials carefully examine submissions, the vast majority of which are from MI5 and Police Service of Northern Ireland (PSNI), challenging them where appropriate and producing objective and balanced advice for the Secretary of State. We identified some good practice during the inspection, particularly the processes developed for keeping intercepting agency handling arrangements under review.

Scottish Government

- 17.9 The Scottish Government adopts a proactive approach with agencies and provides good quality control of warrant applications and advice to the Minister for Justice and Veterans about reviews and the specificity and breadth of thematic warrants. It has demonstrated a good level of compliance with the IPA and the Code of Practice and has asked for reviews to be done before some warrants expire to check on the continuing necessity and proportionality of the warrants and, in particular, to assess the collateral intrusion and the impact on privacy.
- 17.10 The WGD continued to provide a service throughout the various lockdowns, ensuring that the authorisations process was not disrupted and that law enforcement could carry out their activity lawfully. We were also impressed with the WGD’s out-of-hours authorisations procedures and consider them to be robust and thorough.

18. Errors and Breaches

Overview

18.1 Investigation of errors and breaches reported to us by the authorities we oversee is an important part of our work. We may also discover potential errors during our inspections. These 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.³⁶

UK intelligence community (UKIC) errors

18.2 In 2021, the errors reported to us did not suggest systematic failures of safeguards or an attempt to act unlawfully or circumvent safeguards. The tables and graphs below show the relevant errors reported to the Investigatory Powers Commissioner (IPC) by UKIC.

Table 18.1: UK intelligence community (UKIC) errors, 2021

	Agency			Total
	MI5	SIS	GCHQ	
Covert human intelligence sources (CHIS)	0	6	0	6
Directed surveillance (DSA)	4	1	0	5
Property interference and intrusive surveillance (PI/IS)	6	0	0	6
Bulk personal data (BPD)	11	18	0	29
Section 7 Intelligence Services Act 1994 (s7 ISA)	0	1	0	1
Interception	30	3	30	63
Systems	0	1	9	10
Bulk/targeted equipment interference (EI)	1	0	8	9
Communications data (reportable) (CD)	19	0	7	26
The Principles	0	2	1	3
Total	71	32	55	158

36 See: <https://www.ipco.org.uk/what-we-do/errors/>

Figure 18.1: UKIC errors (excluding systems and communications data), 2017 to 2021

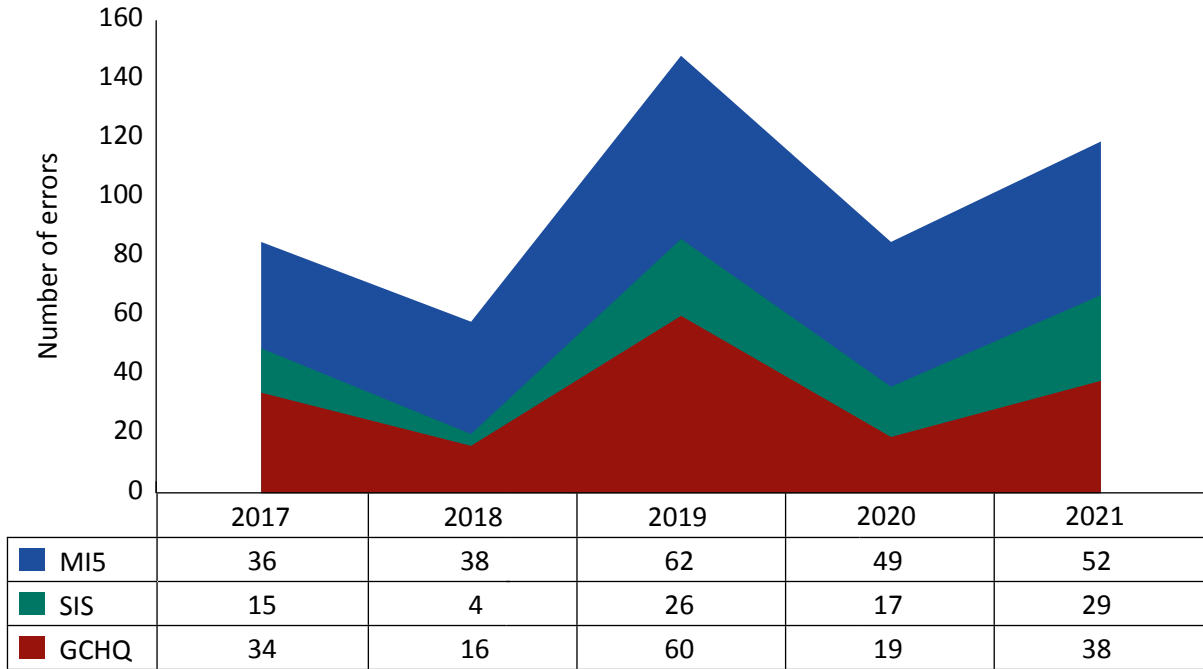


Figure 18.2: Reportable UKIC communications data errors, 2018 to 2021

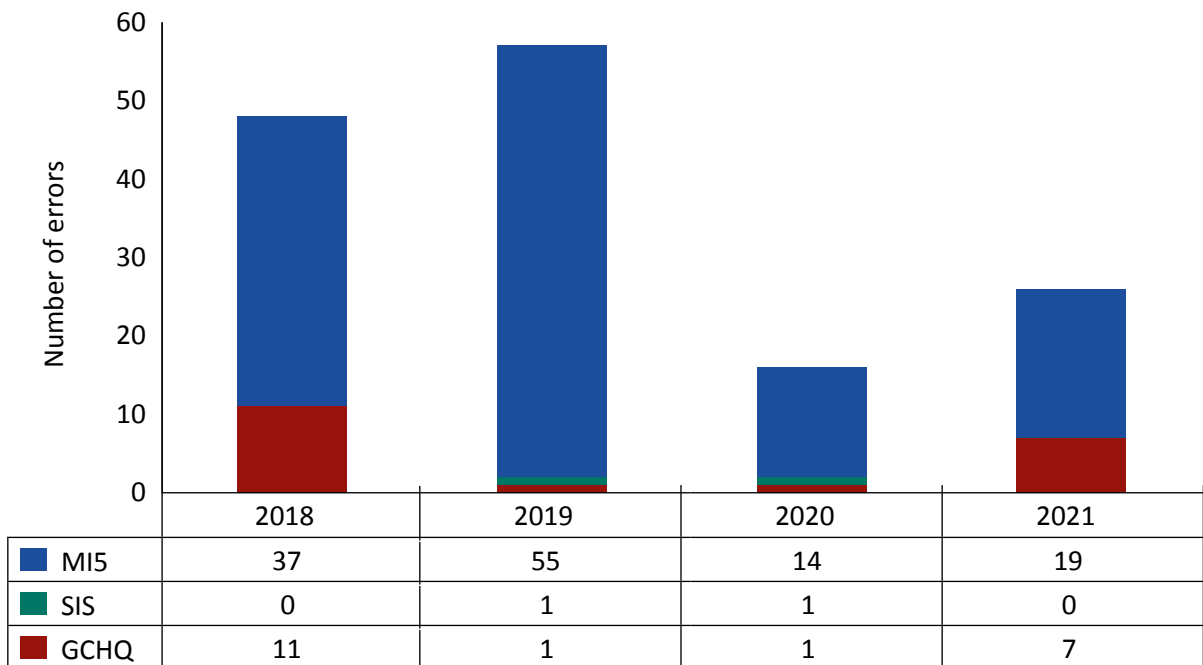


Figure 18.3: MI5 errors (excluding systems), 2017 to 2021

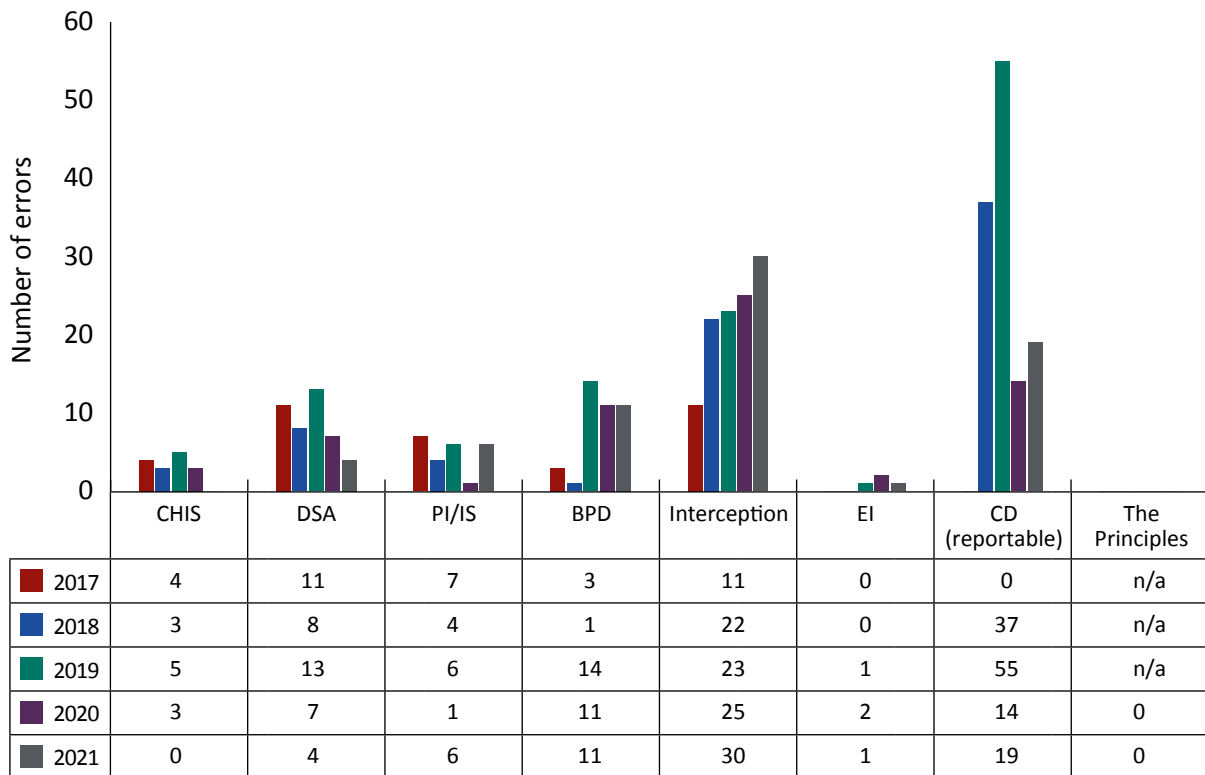


Figure 18.4: Secret Intelligence Service (SIS) errors (excluding systems), 2017 to 2021

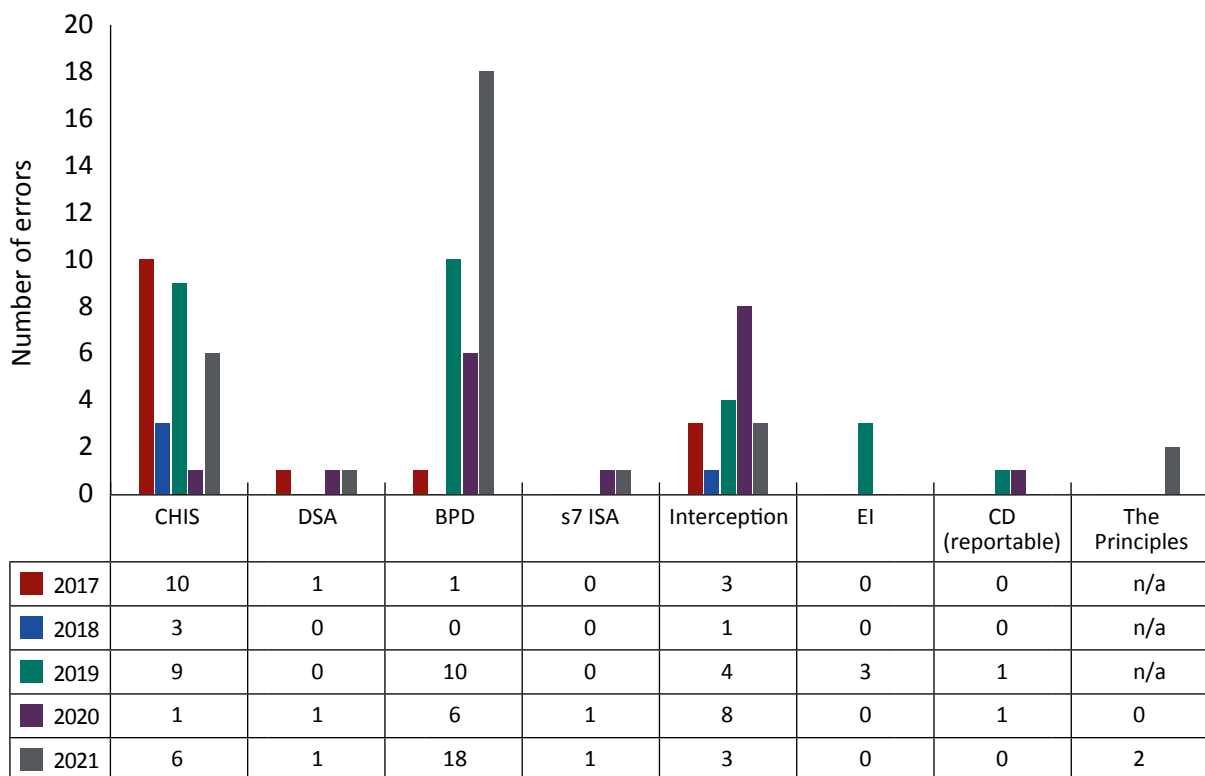
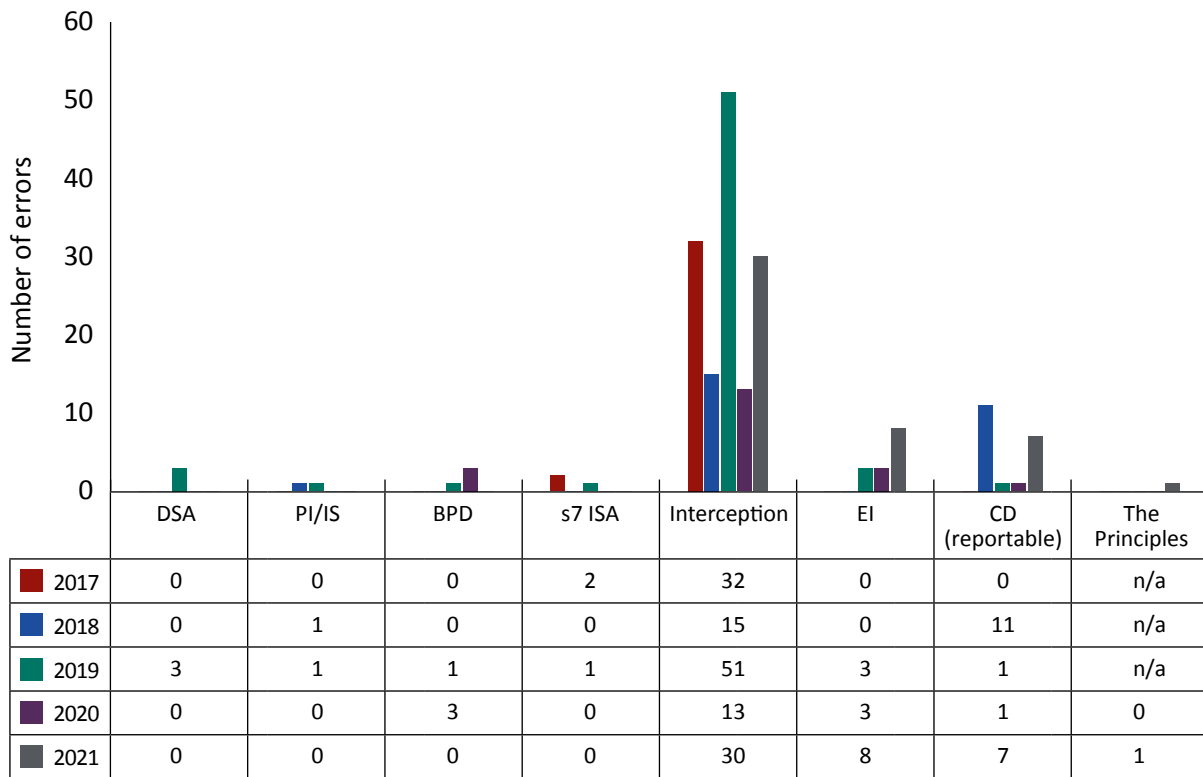


Figure 18.5: Government Communications Headquarters (GCHQ) errors (excluding systems), 2017 to 2021



- 18.3 In 2021, there were 158 relevant errors reported to us by UKIC. This was an increase from the 121 reported last year but still substantially lower than 218 in 2019.
- 18.4 Given the impact of Covid-19 restrictions throughout 2020 and for much of 2021, it is not possible to conduct a meaningful year-on-year comparison of errors statistics. The absence of UKIC staff during 2020 meant that error investigations were taking longer than usual to complete, leading to a reduction in errors reported in that year and this position may have continued into 2021. Nevertheless, it is notable that the total number of errors reported in 2021 was significantly lower than 2019 and therefore, despite the caveats in conducting year-on-year comparisons, our assessment is that the figures for 2021 represent an overall reduction.
- 18.5 In 2021, MI5 reported 71 relevant errors which is broadly consistent with 2020. MI5 now operates a practice where it reports some emerging compliance issues to us before a final determination is made about whether a relevant error has occurred. We welcome this approach as it enables us to follow up on the issue on inspection. MI5 formed a proactive compliance investigation team this year and we have seen some of its work on inspection. This team will proactively look at areas where MI5 believes there is a risk of non-compliance and highlight issues for addressing them before they might escalate to errors. We commented favourably on this team in our inspection report.
- 18.6 The increase in SIS errors is largely due to the increase in bulk personal data (BPD) errors. This has been subject to thematic inspection and continues to be monitored. More details on the BPD issues are contained in the SIS chapter.³⁷

³⁷ See: paragraphs 9.21-9.25.

- 18.7 GCHQ reported 55 relevant errors, a marked increase from 33 in 2020 but broadly consistent with the 61 errors reported in 2019. The lower volume of errors reported in 2020 is likely to have been caused by staff absence arising from Covid-19.
- 18.8 One error that we are continuing to investigate is in relation to over retention of Investigatory Powers Act 2016 (IPA) material in a particular file storage area. This was identified by GCHQ and reported to us earlier in the year. Since then, GCHQ has set up a compliance group and reporting structure to identify fully all the areas of over retention and resolve any issues. Due to the complex nature of some of the systems involved, GCHQ's programme of mitigation took time to implement fully. At the end of 2021, data that had gone past the authorised retention period was in the process of being deleted. The file storage area is now subject to regular review by GCHQ to ensure retention periods are being complied with.

Interception: law enforcement

- 18.9 In 2021, there were 24 relevant errors reported by the five law enforcement agencies (LEAs) that are permitted to carry out interception under the IPA. This is an increase from the number reported in 2020 (15) and back to the same level as reported in 2019.
- 18.10 The National Crime Agency (NCA) reported 16 interception errors, broadly consistent with the 13 errors reported in 2020. The most significant NCA error was in relation to the use by Regional Organised Crime Units (ROCU) of intercept material and non-compliance with NCA safeguards. This became a managed investigation and resulted in the process for distribution and storage of targeted intercept (TI) material in the ROCU changing. While the error was closed, there remains an outstanding required action of a letter or memorandum of understanding (MoU) around the supply of TI material to National Police Chiefs' Council (NPCC) forces.
- 18.11 The NCA has set up a compliance board which reports to a strategic board and can escalate issues. It meets monthly and looks across all IPA and Regulation of Investigatory Powers Act 2000 (RIPA) powers. We see the minutes on inspection. We see this as best practice and a good way of managing compliance matters and reducing errors.
- 18.12 The Metropolitan Police Service (MPS) reported six interception errors, in comparison to three in 2020. The MPS also supplies intercept material to the ROCU but on a smaller scale than the NCA, and were subject to a similar investigative process as the NCA. Like the NCA, the MPS intercept material was being kept within ROCU contrary to IPA safeguards. This was rectified and they are now compliant but there remains the outstanding action, as with the NCA, to provide an MoU between the NCA, the MPS and the NPCC setting out clarity on the rules to be followed for TI material and ownership.
- 18.13 The other two errors were unconnected instances committed by two of the other LEA intercepting agencies.

The Principles: law enforcement

- 18.14 In 2021, the MPS reported eight errors in relation to The Principles, in comparison to one in 2020. Nearly all of the errors reported related to a failure to apply The Principles to the receipt of unsolicited intelligence from low risk countries (see: paragraph 12.30).

Warrant Granting Departments

18.15 The Home Office reported two errors in 2021. As set out in paragraph 17.3, our main concerns related to long-standing arrangements for signing out-of-hours warrants which, on close examination, were determined to be contrary to the IPA. Despite the administrative nature of this error, it has potential to impact on several years of out-of-hours warrants. The Home Office are still investigating the extent of the issue and we will report our findings on this next year.

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

18.16 As set out in table 18.2, there were 80 errors relating to surveillance, property interference and CHIS reported during 2021. This is a slight improvement compared to 2020 when 92 errors were recorded. While each error in its own right is regrettable and viewed seriously, none of the errors constituted a serious error as defined under section 231 of the IPA; this means that no significant prejudice or serious harm was suffered by any individual as a result of these errors.

Table 18.2: Total surveillance, property interference, CHIS and equipment interference errors for LEAs, public and local authorities and prisons, 2021

Investigatory power	Number of errors
Directed surveillance	53
Property interference	15
Intrusive surveillance	0
Covert human intelligence sources (including relevant sources)	12
Equipment interference	0
Total	80

18.17 While the largest proportion of errors were in relation to surveillance and property interference, their number continues to be reassuringly small when viewed in the context of the total number of such authorisations. In line with previous years, the most common types of surveillance and property interference errors are recorded as follows:

- starting the surveillance before the authorisation has come into effect;
- continuing the activity or leaving the equipment *in situ* after the authorisation has been cancelled; and
- exceeding the parameters of the authorised activity.

18.18 Key to reducing the frequency of these types of error is improving communications between the Technical Surveillance Units (TSUs) and Surveillance Teams who are charged with installing and monitoring the equipment, and the investigation and intelligence teams who are responsible for obtaining the relevant authorisations. Accordingly, Inspectors will often scrutinise the policies and procedures for ensuring that the TSU and Surveillance Officers have sight of the authorisation prior to deployment and that they clearly understand the parameters within which they have to operate.

- 18.19 Errors have also arisen when the need for an authorisation has either not been identified or, in connection with CHIS, authorisations have been unnecessarily delayed while the source is assessed for their suitability for recruitment. Surveillance errors are often caused by a lack of awareness of the law, or an overly narrow interpretation of what constitutes private information. Inspectors therefore encourage Covert Authorities Bureau (CAB) managers to provide regular refresher training to those officers who are most likely to engage the powers and to publish guidance on the use of covert investigatory powers on their intranet sites.
- 18.20 Similarly, a lack of awareness, rather than a deliberate attempt to circumvent the law, is the root cause of most of the CHIS errors identified. Some public authorities have developed overly bureaucratic procedures for assessing the suitability of a source for authorisation as a CHIS. Inevitably, this has caused delays in seeking an authorisation, during which time the source has continued covertly to provide the public authority with information and intelligence. A failure to authorise a CHIS once the statutory definition is met is non-compliant with the CHIS Code of Practice and constitutes a relevant error. Public authorities are therefore encouraged to introduce robust oversight arrangements to reduce the risk of such errors occurring.

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

- 18.21 Unsurprisingly, considering that the acquisition of CD is by far the most frequently used covert investigation power, this accounts for highest proportion of errors. There are two categories of error for CD: recordable, where the mistake has not resulted in the acquisition of CD; and reportable, where the mistake did result in the disclosure of CD and there is a duty on the public authority to notify the IPC.
- 18.22 The statistical breakdown of errors for 2021 is shown in table 18.3. The data displays a similar pattern to previous years and does not cause us any specific concern or highlight any increasing trend or systemic failures.

Table 18.3: Reportable communications data errors, 2018 to 2021

Cause of errors	Number of errors			
	2018	2019	2020	2021
Law enforcement agencies	758	755	741	899
Telecommunications operator	127	230	253	332
Postal	0	0	0	6
Other public authorities	13	14	10	15
Workflow	5	12	1	7
Total	903	1,011	1,005	1,259

- 18.23 Table 18.4 shows that the biggest single cause of errors continues to be when an applicant seeks CD on an incorrect identifier. This equates to 31% of all LEA errors, which is in line with figures we have reported in the last two years.

Table 18.4: Breakdown of communications data errors by error type and responsibility, 2021

	Applicant ¹	Single Point of Contact	Telecoms/ postal operator	Authorising Individual	Workflow
Incorrect Identifier	391 (12 IP) ²	93 (15 IP)	101 (5 IP)	0	0
Time/Date	32 (10 IP)	254 (92 IP)	36 (6 IP)	0	0
Excess/No Data	0	0	196	0	0
System Error	0	0	7	0	7
No IPA authority	26 ³	114 ⁴	0	4	0
Total	449 (22 IP)	461 (107 IP)	340 (11 IP)	4	7

Notes:

¹ Includes data provided to an authority by a 3rd party (33)

² Internet protocol address

³ CD obtained via a Data Protection request

⁴ Additional data types obtained in error

- 18.24 It remains that case that the vast majority of errors do not result in any significant harm or prejudice. Most are the result of human error where there has been a simple transposition of a number or letter in a communications identifier and are noticed at a very early stage. Sometimes this type of mistake is made by an applicant or the Single Point of Contact (SPoC) officer processing the application and sometimes the error is present from the outset, for example the telephone number provided to the police by the victim or witness is incorrect, and this not ascertained until the anomaly is recognised in the data returned.
- 18.25 The national Error Reduction Strategy (ERS) is now well embedded and has undoubtedly led to a significant reduction in the number of errors that have the potential to result in serious consequences. It is encouraging that, while originally developed to reduce the risks associated with the resolution of internet protocol addresses (a process that can be very complex), many public authorities now apply the ERS to all applications to acquire CD. This is a practice we encourage and endorse.
- 18.26 All errors reported to us are reviewed for any rising trends or patterns where we could take early remedial action to prevent recurrence. This may take the form of guidance and direction provided to public authorities or working with telecommunications operators (TOs) to identify potential system errors. The same principles apply to recordable errors, collated by the public authority responsible for the error and reviewed by us in detail during our inspections. Any error that we assess could have resulted in significant harm or prejudice is subject of a thorough investigation by IPCO and the subsequent report is provided to the IPC.
- 18.27 In our 2020 report, we noted the intention to initiate a single reporting process with the Information Commissioner's Office in respect to TO errors. This was delayed in 2021 and we will provide an update in our 2022 report.

Serious errors

- 18.28 Section 231(1) of the IPA requires the IPC to inform a person of any relevant error if deemed serious and in the public interest to inform them. A relevant error is defined as an error made by a public authority not a TO itself. If once a relevant error has been established, the IPC must then consider the seriousness.
- 18.29 In 2021, we investigated 24 potential relevant errors that may have resulted in serious harm. Following investigation, the IPC did not notify any of the affected persons in any of these cases. In those determined to constitute a relevant error, the outcome did not reach the seriousness threshold. In the other investigations, although serious harm was clearly apparent, the IPC was unable to inform the affected person. This was because the established cause was not the result of a relevant error. In such cases, victims may nevertheless have a right of remedy through civil redress.
- 18.30 Table 18.5 sets out the breakdown of the cause of each error. A summary of these investigations is set out in Annex C.

Table 18.5: Serious errors by cause, 2021

Error Type	Relevant Public Authorities	Telecoms Operator
Incorrect Data (Human)	6	6
Incorrect Data (System)	0	4
Transposition	3	0
Hacking	3	0
Intelligence	1	0
Breach of Code	1	0
Total	14	10

19. Statistics

Overview

- 19.1 Section 234 of the Investigatory Powers Act 2016 (IPA) sets out a requirement for the Investigatory Powers Commissioner (IPC) annually to publish key statistics, including the number of warrants and authorisations issued during the year. Our approach to the collection of statistics is broader than that specified by the Act as we consider it important to gather, and where appropriate publish, data that helps to inform our understanding of how the powers are being used and to be able to track their use over time.
- 19.2 To that end, we have selected statistics for publication which we believe will give an accurate picture of the extent to which the different categories of authority that we oversee are using their powers. This selection is carried out with two objectives in mind; first, to reflect the ongoing challenge we receive on the value of statistics and the level of transparency they provide; and secondly, as always, the commitment to ensuring that we do not provide statistics which would be partial or misleading or those which could cause any damage to the ongoing operations of the authorities we oversee and to national security.
- 19.3 Throughout the report, we have included statistics alongside our findings to provide the context in which they are being used. Where possible, we have sought to present statistics in the same format as our previous reports.³⁸

Warrants and authorisations

- 19.4 In 2021, 303,831 warrants and authorisations were issued across all powers. Table 19.1 sets out how these break down across the different public authorities. As in previous years, the large number of authorisations by law enforcement agencies (LEAs) is a result of their high use of communications data (CD) powers.

Table 19.1: Investigative and other powers authorised by public authority sector, 2020 to 2021

	UKIC	LEAs	WPAs	Local authorities	Prison services	Total
2020	18,119	251,674	1,130	588	181	271,692 ³⁹
2021	17,458	284,815	870	417	271	303,831

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

39 The total figure was incorrectly published as 271,712 in the 2020 report.

- 19.5 Table 19.2 provides the total numbers for warrants and authorisations issued, considered and approved for 2021. It also provides the total number of certain notifications made to IPCO during this period and the number of applications refused by Judicial Commissioners (18). In addition to these refusals, one authorisation (for property interference) was quashed.
- 19.6 Judicial Commissioners have the option to seek clarification on the detail of an application. This could involve internal discussions with the IPCO Legal Team but in most cases requires further detail to be provided by the applicant. In 2021, Judicial Commissioners requested further information in 125 cases. The majority of these saw explanations provided or the application revised to enable a decision to be made. Four applications were subsequently withdrawn (or no decision required). Judicial Commissioners went on to refuse one application with instructions to destroy legally professional privileged (LPP) material. Additionally, eight Criminal Conduct Authorisations (CCA) applications were cancelled and resubmitted appropriately.

Table 19.2: Breakdown of authorisations, notifications and refusals, including those considered by a Judicial Commissioner, 2021

	Considered by a Judicial Commissioner	Approved, issued or given	Refused by a Judicial Commissioner
Covert human intelligence sources (CHIS) including juveniles and relevant sources	N/A	2,860	N/A
Directed surveillance	N/A	6,847	N/A
Intrusive surveillance	490	489	1
Property interference under section 5 of the Intelligence Services Act 1994	N/A	434	N/A
Property interference under the Police Act 1997	N/A	1,033	0
Bulk personal datasets – class warrant	111	111	0
Bulk personal datasets – specific warrant	66	66	0
Directions under section 219 of the Investigatory Powers Act 2016	0	0	0
Directions under section 225 of the Investigatory Powers Act 2016	5	5	0
Bulk communications data acquisition warrant	14	14	0
Communications data authorisation	N/A	284,932	N/A
Bulk interception warrant	33	33	0
Targeted examination of interception warrant	63	63	0
Targeted interception warrant	3,634	3,630	4
Bulk equipment interference warrant	13	13	0
Targeted examination of equipment interference warrant	63	63	0
Targeted equipment interference warrant	3,175	3,167	8
Mutual assistance warrant	0	0	0
Relevant source notifications ¹	-	554	0
Request to retain legal professional privileged material	167	163	4
Notification under section 77 of the Investigatory Powers Act 2016	7	6	1

Notes:

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

Statutory purpose of authorisations

19.7 Table 19.3 shows the statutory purposes used for authorisations across the different investigatory powers from our statistical returns. It should be noted that more than one statutory purpose could be applicable for a single authorisation.

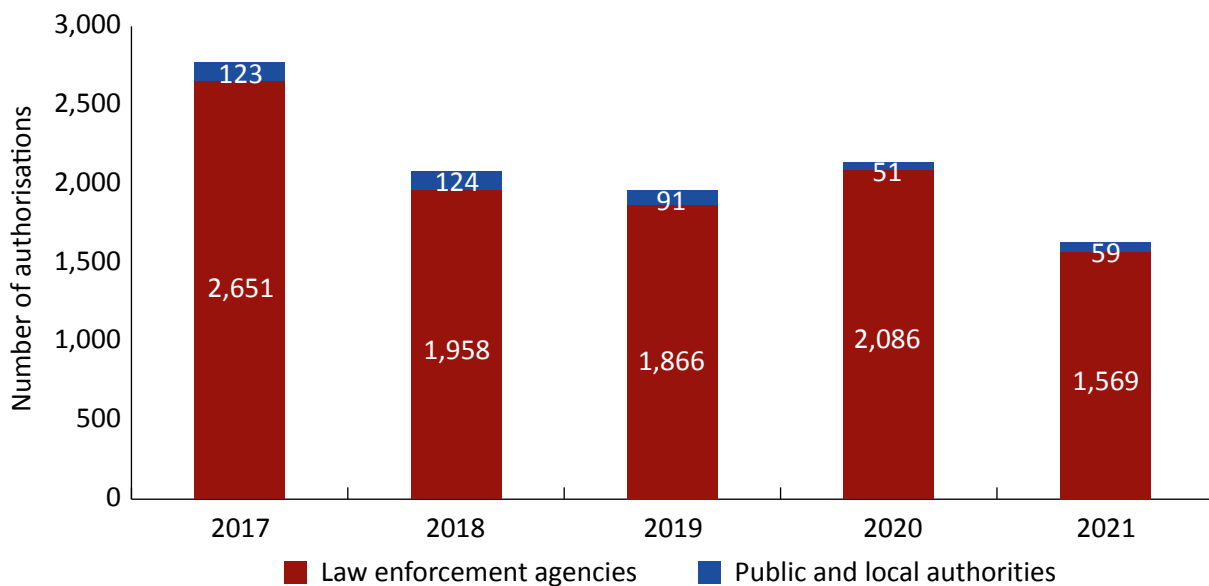
Table 19.3: Authorisations by statutory purpose, 2021

Statutory purpose	Number of authorisations
Prevent/detect crime	268,697
Preventing death or injury	36,663
National security	13,772
Identify person	814
Interests of public safety	418
Economic well-being	360
Other	142

Covert human intelligence sources (CHIS)

19.8 As shown in figure 19.1, a total of 1,628 covert human intelligence sources (CHIS) authorisations were made in 2021 across LEAs, the wider public authorities (WPAs), local authorities and prisons. Of these, nine were urgent and two authorisations related to cases where knowledge of privileged or confidential information may be acquired.

Figure 19.1: Covert human intelligence sources across law enforcement agencies, public and local authorities, 2017 to 2021



Note:

– These figures relate to any authorisation to use a person as a CHIS but do not include authorisations for relevant source authorisations for law enforcement undercover officers.

Criminal Conduct Authorisations

19.9 As set out in Chapters 2 and 13, provisions under the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 were commenced from June 2021, with authorisations being made from August 2021.⁴⁰ Since the commencement of the Act, Judicial Commissioners have been notified of 555 operatives being authorised under the new statute. Due to the potential conflation with CCAs, participation in crime figures have not been included for 2021.

Juvenile CHIS

19.10 In 2021, one new CHIS authorisation was granted which related to a juvenile, who was not under the age of 16 at the time the authorisation was granted.

Relevant sources

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

Table 19.4: Relevant sources authorisations and applications, 2020 to 2021¹

	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

Notes:

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

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

³ Refusals relate to applications to renew only.

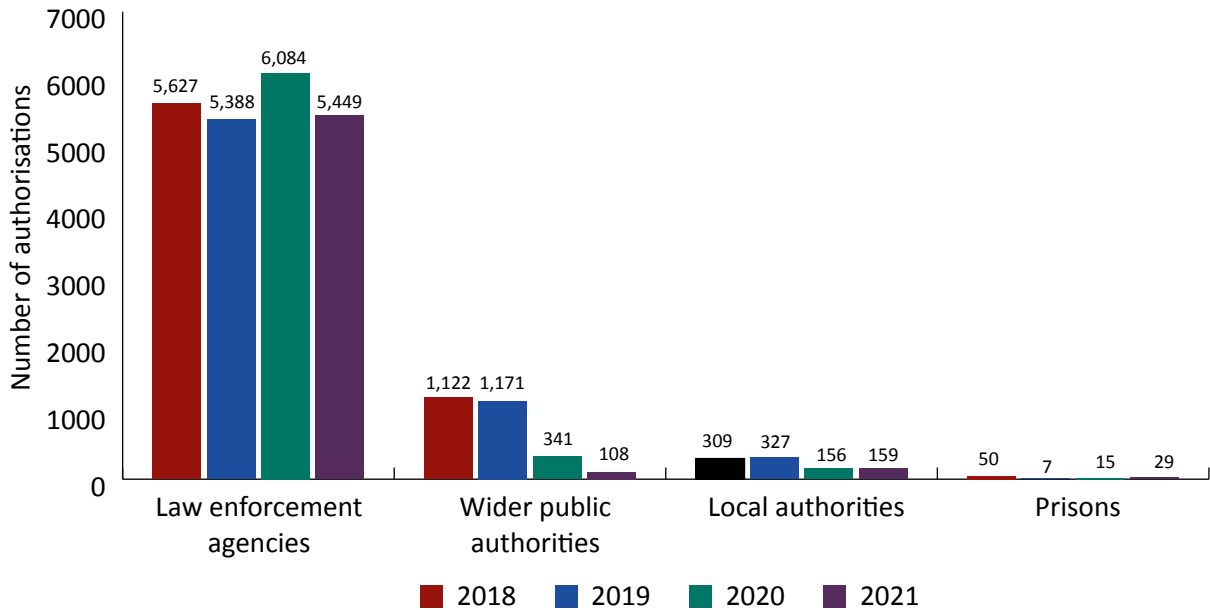
Directed surveillance

19.12 Figure 19.2 shows that a total of 5,745 directed surveillance authorisations (DSA) were made in 2021 across LEAs, WPAs, local authorities and prisons. Of these authorisations, 416 were made under the urgent provisions.

19.13 In 2021, one DSA was granted which either sought or was likely to obtain confidential or privileged material (other than LPP) and 34 DSAs were granted where LPP was sought or likely to be obtained.

40 See: paragraphs 2.2-2.5.

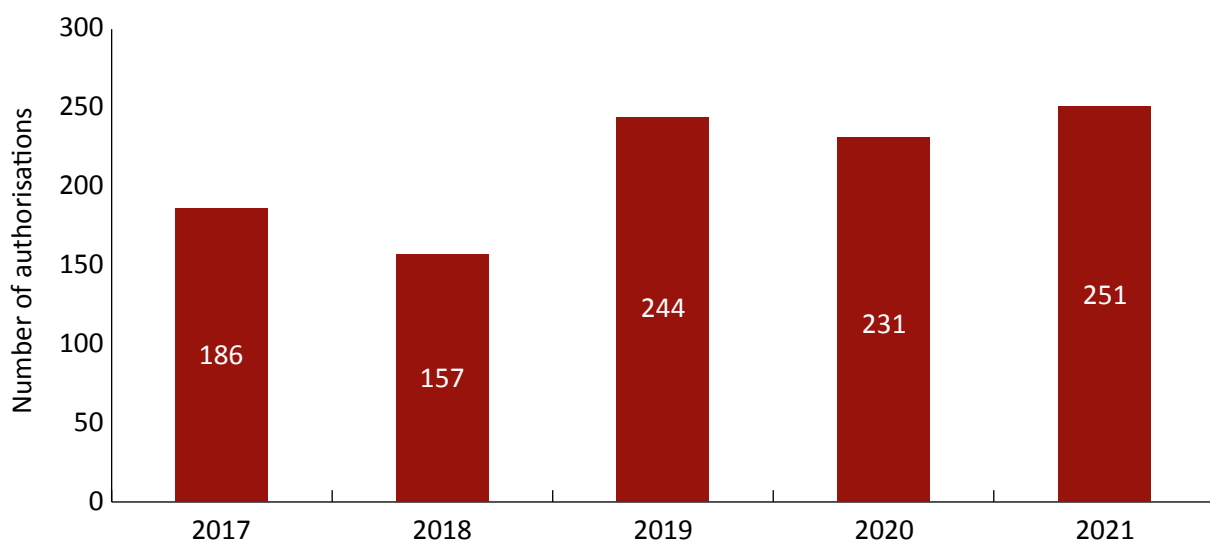
Figure 19.2: Directed surveillance authorisations across law enforcement agencies, wider public authorities, local authorities and prisons, 2018 to 2021



Intrusive surveillance

19.14 In 2021, 251 intrusive surveillance authorisations were granted to LEAs. Of these, 19 were urgent authorisations. One of the authorisations either sought or was likely to obtain confidential or privileged information (other than LPP) and a further 20 were granted where LPP was either sought or likely to be obtained.

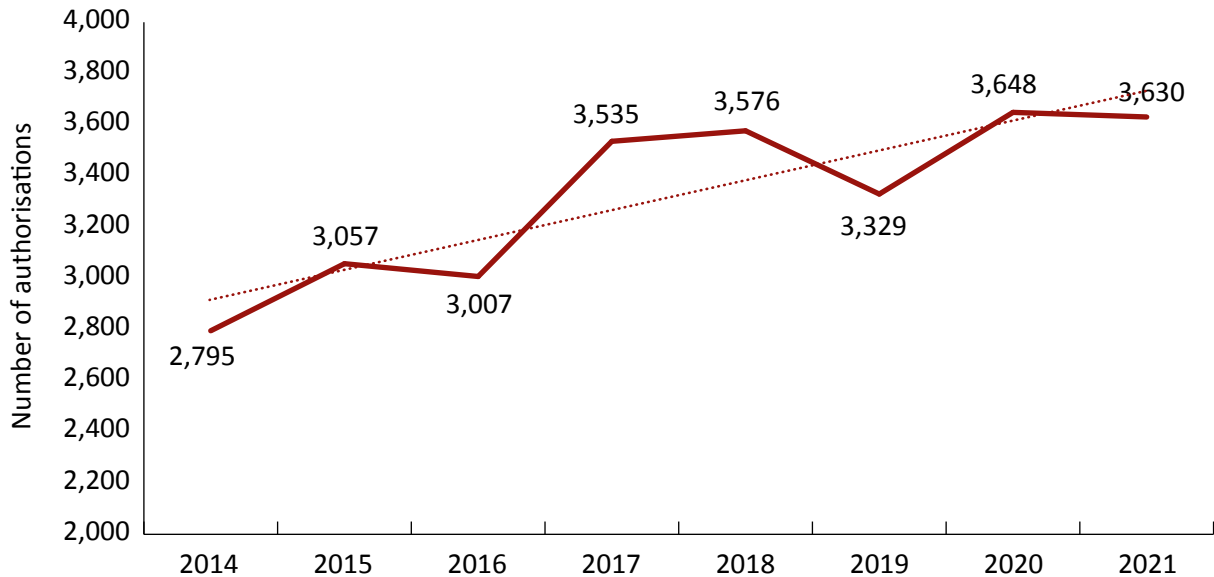
Figure 19.3: Intrusive surveillance authorisations from law enforcement agencies, 2017 to 2021



Targeted interception

19.15 As shown in figure 19.4, the number of targeted interception (TI) warrants has remained steady over the last two years following a slight decrease in 2019. Of the 3,630 authorisations made in 2021, 39 were urgent applications.

Figure 19.4: Targeted interception authorisations by the UK intelligence community and law enforcement agencies, 2014 to 2021



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

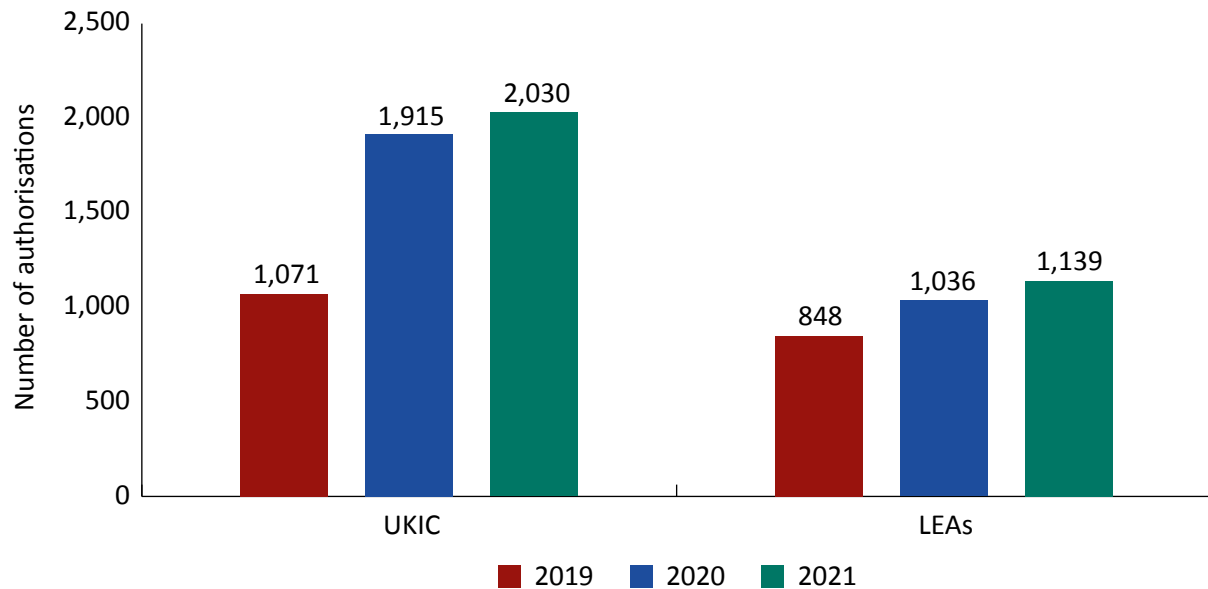
Table 19.5: Targeted intercept warrants involving confidential material, 2020 to 2021

	LPP – sought	LPP – possible	Sensitive professions
2020	12	359	35
2021	11	187	11

Targeted equipment interference

19.17 In 2021, 3,169 authorisations were granted to use targeted equipment interference (TEI) powers, of which 282 were made under the urgent provisions. As was the case in 2020, the three WPAs who have access to TEI powers made no use of them in 2021.

Figure 19.5: Targeted equipment interference authorisations for the UK intelligence community and law enforcement agencies, 2019 to 2021



19.18 As shown in table 19.6, confidential material was only sought or likely to be obtained in a small number of warrants.

Table 19.6: Targeted equipment interference warrants involving confidential material, 2020 to 2021

	LPP – sought	LPP – possible	Sensitive professions
2020	14	207	66
2021	15	64	14

Communications data

19.19 As shown in table 19.7, 284,932 CD authorisations were made in 2021. These include: authorisations made under section 60A, as authorised by the Office for Communications Data Authorisations (OCDA); warrants authorised under section 61 in the interests of national security (which are not authorised through OCDA); and those made under the urgent provisions. LEAs remain the greatest user of the power with 95.9% of all authorisations made.

Table 19.7: Communications data authorisations, 2020 to 2021

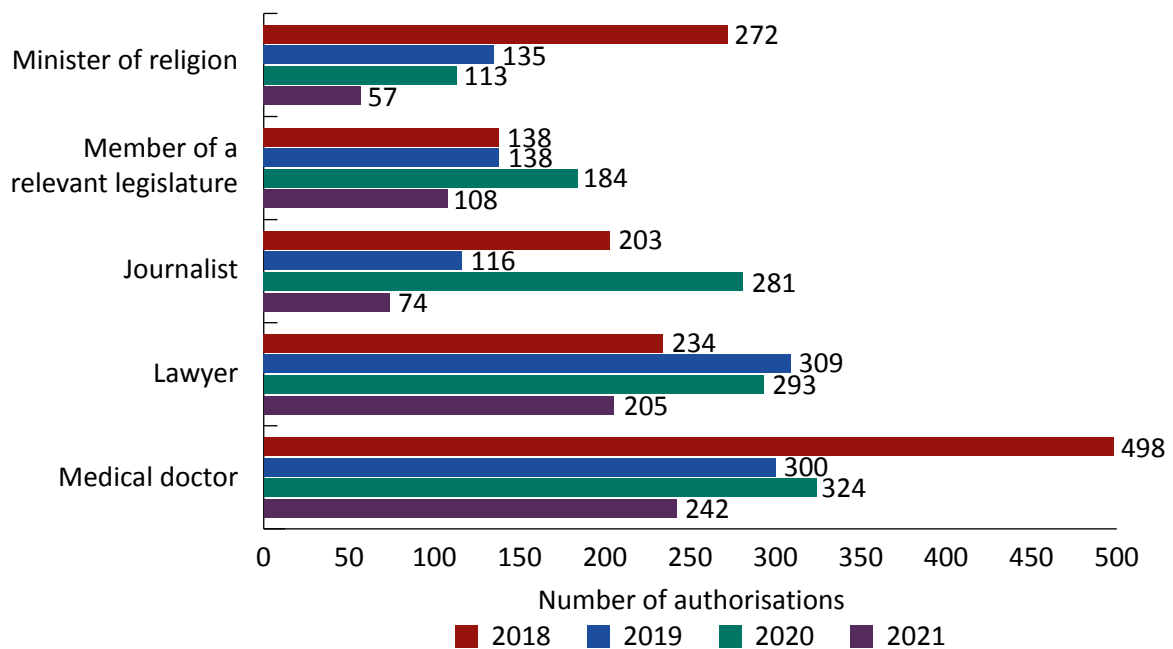
	UKIC	LEAs	WPAs	Local authorities	Prison services	Total
2020	11,444	239,086	969	212	155	251,866
2021	10,536	273,193	749	237	217	284,932

19.20 CD applications are used to request one or more data items. Unfortunately, the systems used to process that data are not able to provide precise statistics and we believe that there is a margin of error of around 10% on the number of data items obtained. However,

the nature of our oversight means that this does not reduce the level of confidence that we have in the compliance of those authorities. In 2021, in the region of one million CD items were obtained.

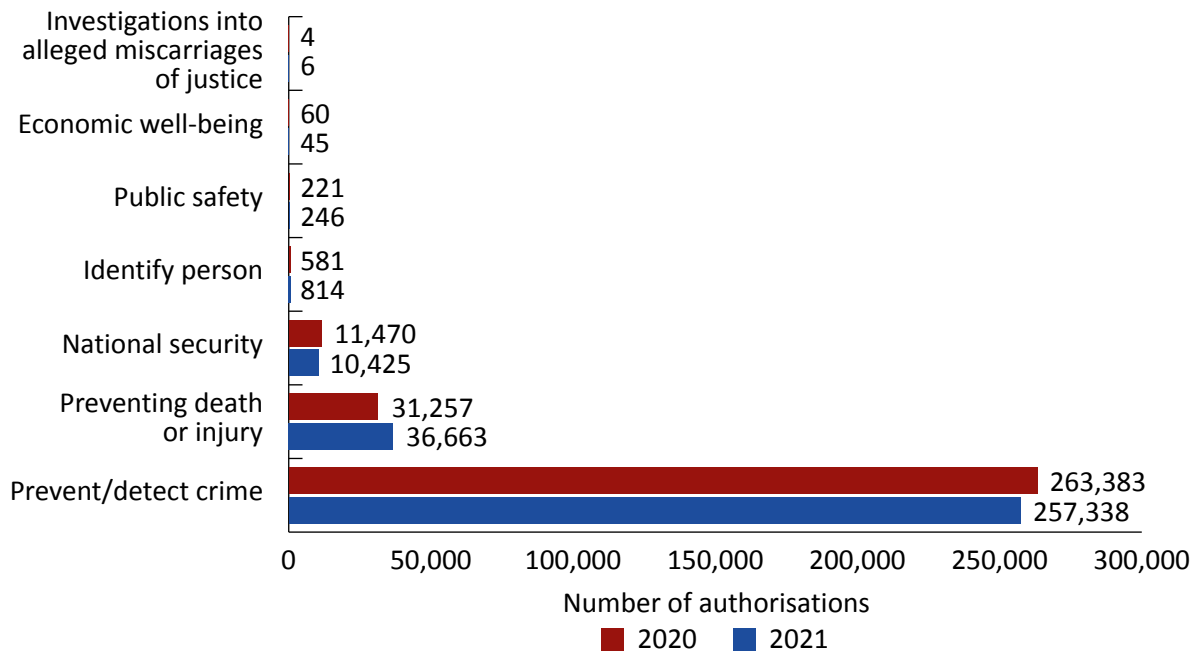
- 19.21 Figure 19.6 sets out the number of authorisations obtained in relation to sensitive professions. CD acquired and disclosed under the IPA does not include content. Nonetheless, there must be considerations as to whether there is a risk that acquiring the data will thereby create an unjustified risk that sensitive professional contacts will be revealed, or that there will be other substantive adverse consequences which are against the public interest. The 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 Parliament, ministers of religion or doctors. Public authorities must record the number of such applications and report to the IPC annually. Most applications relating to sensitive professionals were submitted because the individual had been a victim of crime. For example, it might be the case that a Member of Parliament or a lawyer received threatening or malicious calls and CD requests were made in an attempt to attribute phone numbers or email addresses to perpetrators.

Figure 19.6: Communications data authorisations involving members of a sensitive profession, 2018 to 2021



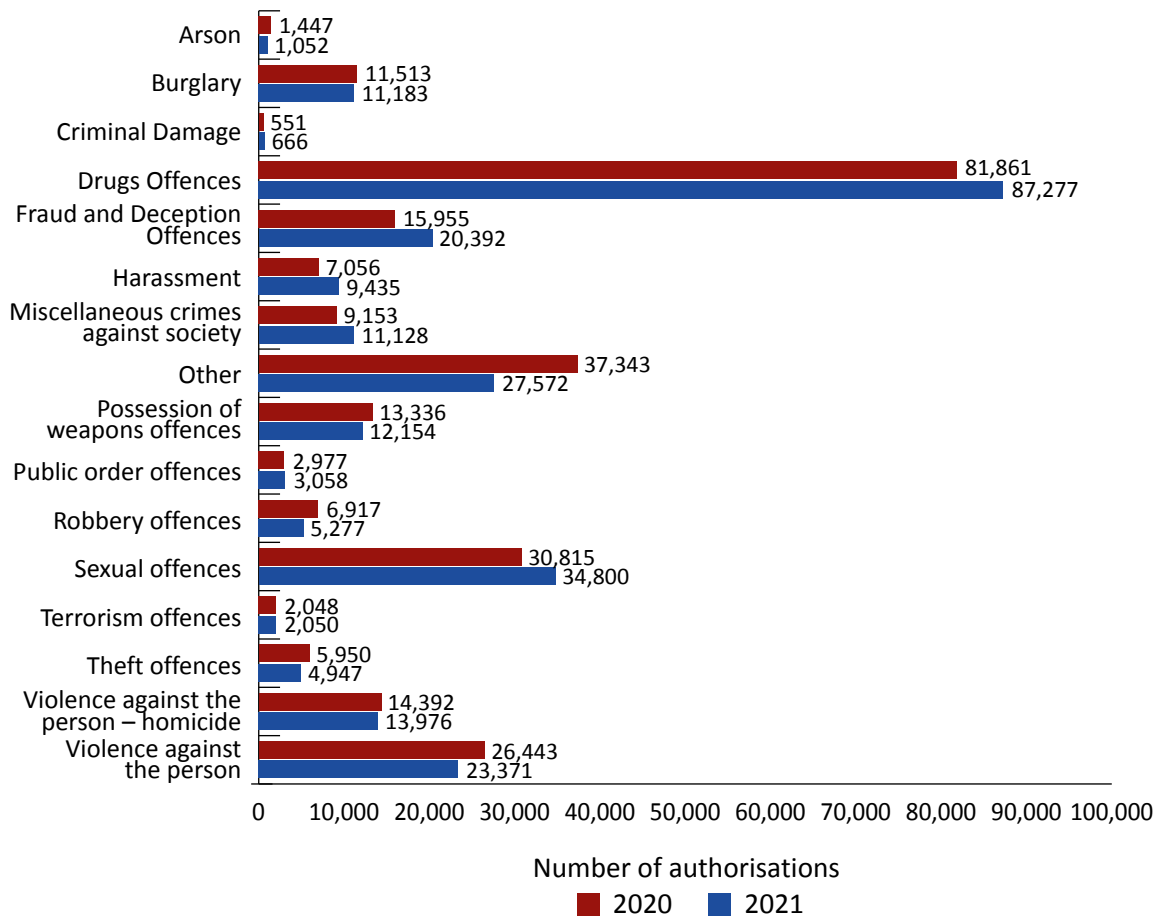
- 19.22 In 2021, seven applications for CD were made to confirm or identify a journalist's source, none of which were urgent. One application was refused by a Judicial Commissioner. As set out in Chapter 4, a further 13 applications were made across other powers to identify a journalist's source.
- 19.23 Figure 19.7 shows the number of CD authorisations for each of the seven statutory purposes. Prevention and detection of crime remains the principal purpose, representing 84.2% of the total authorisations.

Figure 19.7: Communications data authorisations by statutory purpose, 2020 to 2021



- 19.24 For each CD authorisation, where the statutory purpose is “prevention and detection of crime”, public authorities who can use this purpose are required to keep a record of what types of crime the authorisation relates to. One authorisation may relate to more than one of the crime categories (as shown in detail in figure 19.8), which is why the total number of crime types exceeds the number of authorisations shown in table 19.7 above.
- 19.25 Figure 19.8 shows the number of authorisations where the CD is being sought for an “applicable crime” purpose as set out at sections 60A(7), 61(7) or 61A(7) of the IPA. Drug offences make up the largest number of authorisations (32.5%), followed by sexual offences (13.0%).

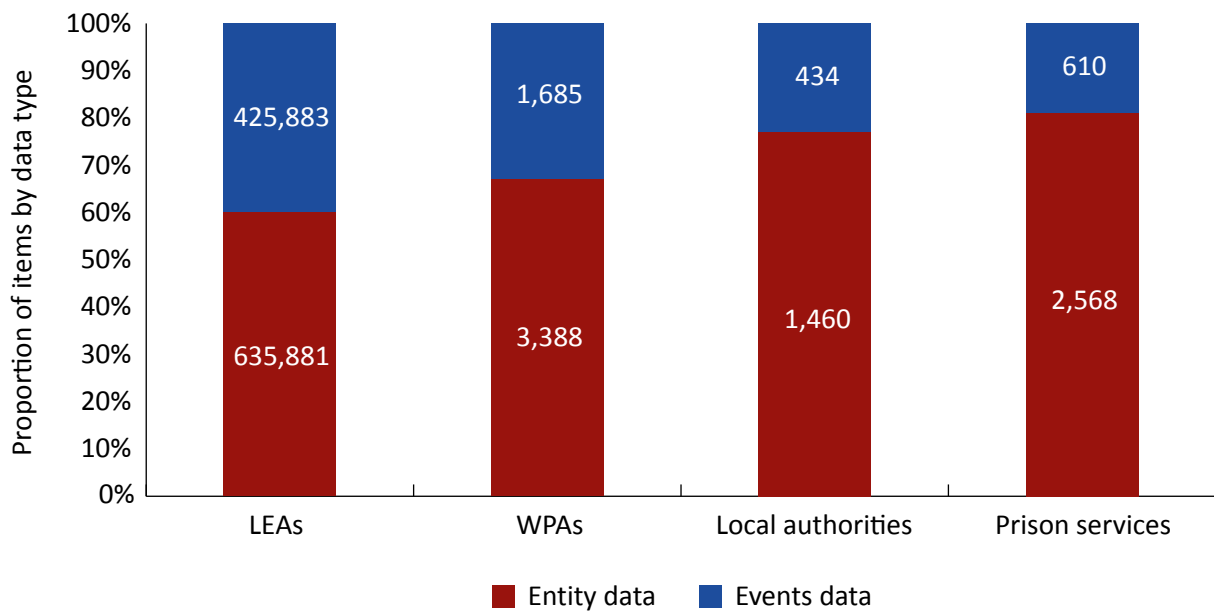
Figure 19.8: Communications data authorisations by crime type under the “prevent and detect crime” statutory purpose, 2020 to 2021



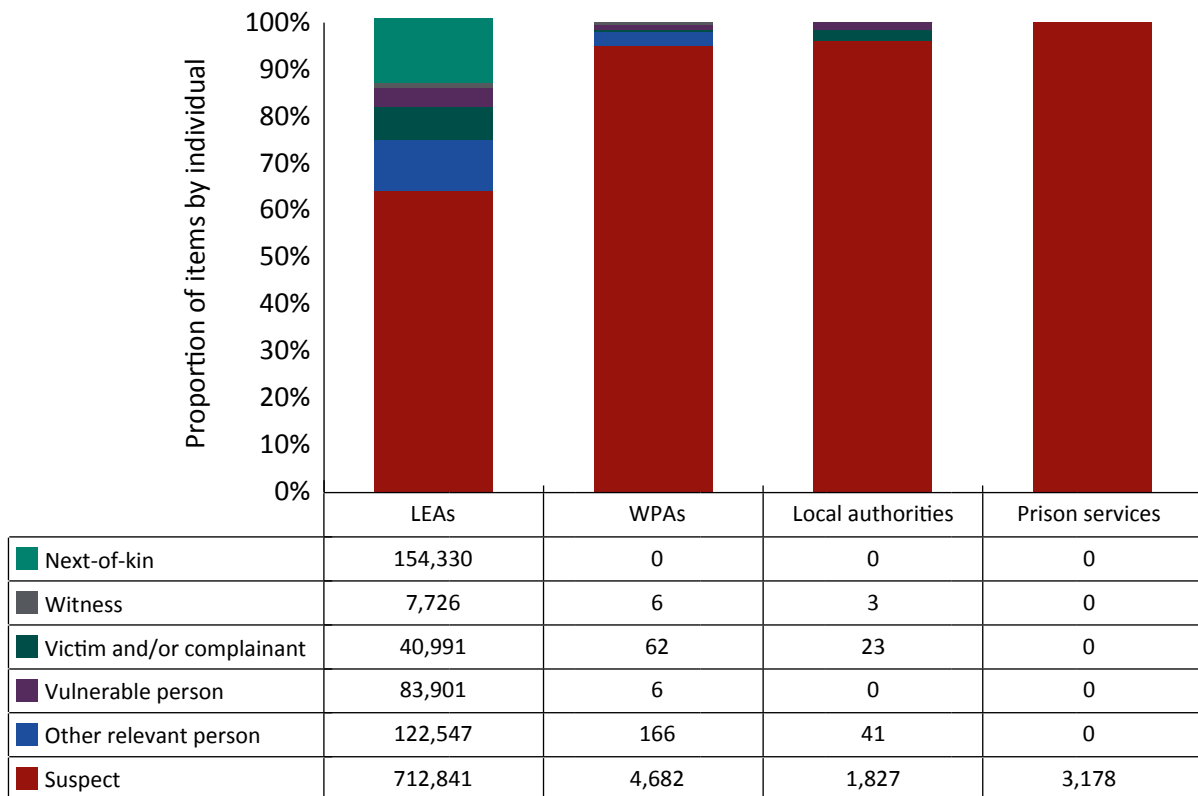
19.26 Figure 19.9 shows the total number of items of CD sought in authorised applications by whether the items of data were categorised as either events or entity data.⁴¹

41 All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories:

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

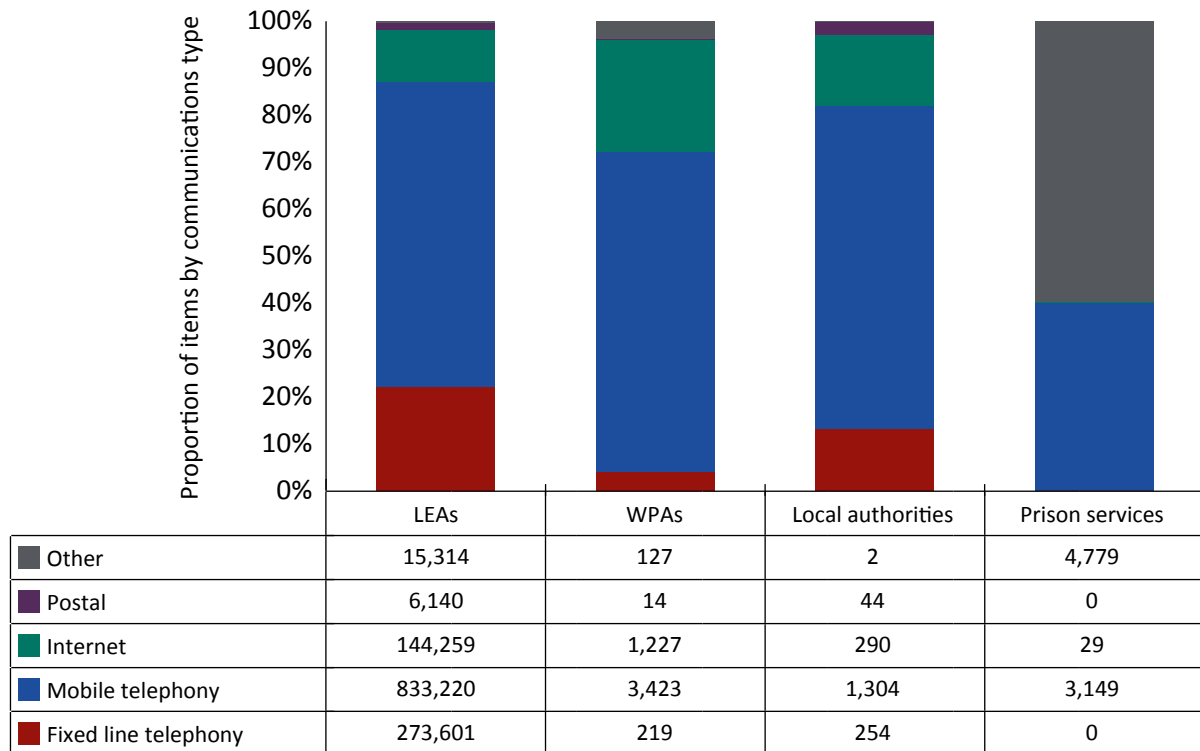
Figure 19.9: Communications data items by data type, 2021

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

Figure 19.10: Communications data items by individual (subject), 2021

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

Figure 19.11: Communications data items by communications type, 2021



Office for Communications Data Authorisations (OCDA)

19.29 Table 19.8 sets out the volume of applications received by OCDA between 2019 and 2021.

Table 19.1: Applications submitted to OCDA, 2019 to 2021

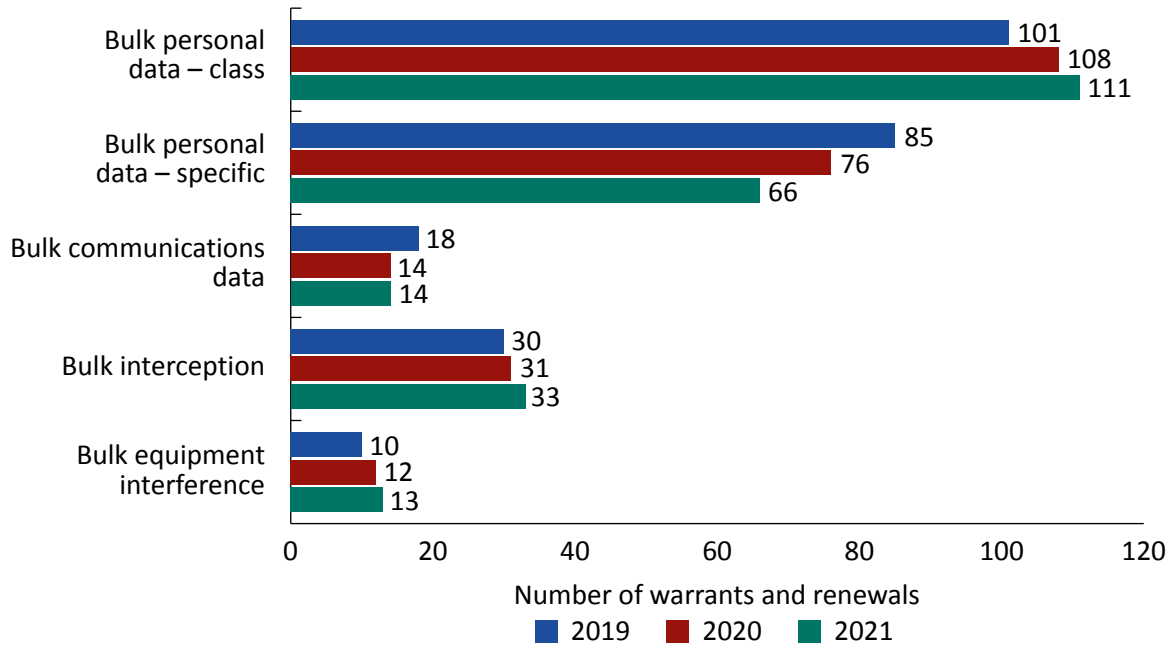
	2019		2020		2021	
Total applications	71,610		226,383		245,272	
Decisions made	71,208	99.4%	223,322	98.6%	242,535	98.9%
Of which						
Authorised	63,688	88.9%	199,482	88.1%	222,009	90.5%
Returned			23,596	10.4%	20,244	8.3%
Rejected			244	0.1%	282	0.1%
Withdrawn	385	0.5%	3,051	1.3%	2,736	1.1%
Applications with no decision at year end (31 December)	17	0.0%	10	0.0%	1	0.0%

Note: 2019 figures are not wholly comparable as OCDA only became functional in March 2019.

Bulk Powers

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

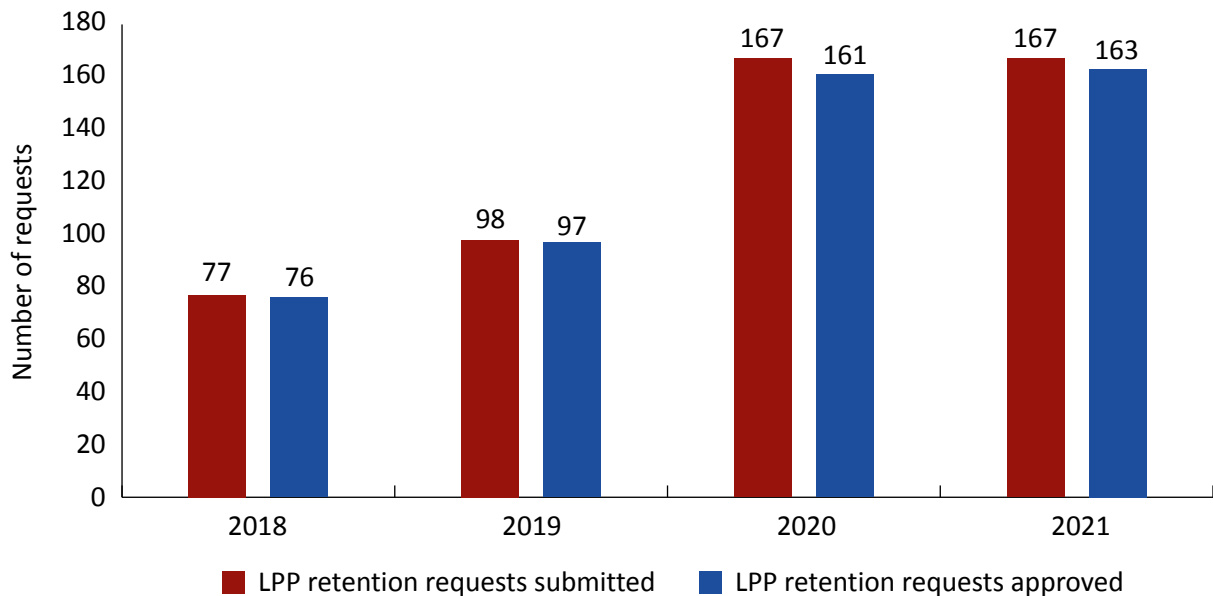
Figure 19.12: Bulk warrants and renewals by type, 2019 to 2021



Legal professional privilege (LPP) material

19.31 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 2021, 163 approvals from 167 applications were made.

Figure 19.13: Number of requests submitted and approved for LPP material, 2018 to 2021



Intelligence Services Act 1994

- 19.32 Section 5 of the Intelligence Services Act (1994) relates to interference with property or with wireless telegraphy by the intelligence agencies. In 2021, 434 warrants were granted.
- 19.33 Section 7 of the ISA applies to acts done outside the UK and which are necessary for the proper discharge of a function of SIS and GCHQ only. In 2021, 78 warrants were issued.

The Principles

- 19.34 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, who are outside UK jurisdiction. They came into effect on 1 January 2020 and replaced the Consolidated Guidance. They are intended to support 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.

Table 19.9: Cases reviewed under The Principles, 2020 to 2021

Number of cases reviewed		2020	2021
Cases reviewed on inspection		93	68
Cases reviewed proactively due to contentious legal or policy issues ¹		8	7
Triggers: Total number of all cases (not limited to those reviewed on inspection)	Personnel knew or believed torture, unlawful killing or extraordinary rendition would occur	0	0
	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	2	3
	Personnel identified a real risk of cruel, inhumane or degrading treatment (CIDT) and submitted for approval	15	17
	Personnel identified a real risk of rendition and submitted for approval	3	0
	Personnel identified a real risk of unacceptable standards of arrest and/or detention and submitted for approval	28	34

Notes:

¹ The figures for "Cases reviewed proactively due to contentious legal or policy issues" and "personnel knew or believed torture, unlawful killing or extraordinary rendition would occur" were incorrectly printed in table 20.8 in the 2020 Report and these have been corrected in the above table.

Annex A. Definitions and glossary

Annex A is divided into three parts:

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

Definitions

Term	Definition
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
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>

Term	Definition
Communications data	Communications data is the “who”, “where”, “when” and “how” of a communication but not its content. It enables the identification of the caller, user, sender or recipient of a phone call, text message, internet application or email (together with other metadata), but not what was said or written. In addition to electronic communications it also covers postal services, enabling the identification of a sender or recipient of a letter or parcel.
Covert human intelligence sources	<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>Another type of CHIS is known as a “relevant source”. This is the term used to describe staff from a designated law enforcement agency that are trained to act as undercover operatives and are subject to an enhanced authorisation and oversight regime.</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	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.
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 – only with authorisation from one of our 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	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.

Term	Definition
Interception	Interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.
Intrusive surveillance	This is surveillance which is carried out, for example, using eavesdropping devices in residential premises or in private vehicles. It may involve the covert presence of a listening device to capture conversations and ensure that the individual being observed is unaware that surveillance is taking place.
Modification	A modification is a change to a warrant authorising the use of investigatory powers. It is requested after the warrant has been issued. A modification to a warrant could be, for example, adding an additional individual so that their communications can be lawfully intercepted.
National Security Notice	<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 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>
Property interference	Property interference is the covert interference with physical property, but also covers wireless telegraphy. This may be for the purpose of conducting a covert search or trespassing on land. For example, police may trespass to covertly install a listening device in a person's house.
Relevant Error	A relevant error is an error made by a public authority when carrying out activity overseen by IPCO. A relevant error is defined in section 231(9) of the Investigatory Powers Act 2016.
Section 7 of the Intelligence Services Act 1994	Section 7 of the Intelligence Services Act 1994 enables the Foreign Secretary to authorise activity by the intelligence agencies outside the UK that would otherwise be unlawful under domestic law.
Serious Error	Section 231(2) of the Investigatory Powers Act 2016 defines a serious error as one where significant prejudice or harm has been caused to an individual as a result of a relevant error.
Targeted interception	Targeted interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.

Term	Definition
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 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>
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 modification – for law enforcement agencies, a 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.</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 whether to approve the decision to issue the warrant and notify the authority of the Judicial Commissioner’s decision; or • decide to refuse to approve the decision, in which case activity under the warrant must stop and the Commissioner may direct that any information obtained under the urgent warrant be destroyed.

Further details on the authorisation process for each of these powers can be found on our website.⁴²

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 • Her Majesty’s Revenue and Customs (HMRC) • National Crime Agency (NCA) • The Home Office (Border Force and Immigration Enforcement)

42 See: <https://www.ipco.org.uk/investigatory-powers/the-powers/>

Wider Public Authorities (WPAs)

- British Broadcasting Corporation (BBC)
- Care Quality Commission
- Centre for Environment, Fisheries and Aquaculture Science (CEFAS)
- Charity Commission
- Competition and Markets Authority
- Criminal Cases Review Commission
- Department for Business, Energy and Industrial Strategy (Insolvency Service)
- Department for Levelling Up, Housing and Communities (DLUHC)
- Department for Work and Pensions (DWP)
- Department for the Economy for Northern Ireland
- Department for the Environment, Food and Rural Affairs (DEFRA)
- Department for Transport – Air Accidents Investigation Branch (AAIB)
- Department for Transport – Driver and Vehicle Standards Agency (DVSA)
- Department for Transport – Marine Accident Investigation Branch (MAIB)
- Department for Transport – Maritime and Coastguard Agency (MCA)
- Department for Transport – Rail Accident Investigation Branch (RAIB)
- Environment Agency
- Financial Conduct Authority (FCA)
- Food Standards Agency
- Food Standards Scotland
- Gambling Commission
- Gangmasters and Labour Abuse Authority (GLAA)
- General Pharmaceutical Council
- Health and Safety Executive
- Health and Social Care Northern Ireland
- Her Majesty's Chief Inspector of Education, Children's Services and Skills (OFSTED)
- Her Majesty's Prison and Probation Service (HMPPS)
- Independent Office for Police Conduct (IOPC)
- Information Commissioner's Office (ICO)

Wider Public Authorities (WPAs) (continued)	<ul style="list-style-type: none"> • Marine Scotland • Maritime Management Organisation • Medicines and Healthcare Products Regulatory Agency • 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
AI	Artificial intelligence
AI	Authorising individual
ACL	Access control levels
AO	Authorising officer

APCC	Association of Police and Crime Commissioners
CAB	Covert Authorities Bureau
CCA	Criminal Conduct Authorisations
CDR	Call data records
CFU	Counter Fraud Unit
CIDT	Cruel, inhuman or degrading treatment
CJEU	Court of Justice of the European Union
CMA	Computer Misuse Act 1990
CMT	Compliance Monitoring Team
COM	Covert Operations Manager
CoP	Code of Practice
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CSP	Communications service provider
DPA	Data Protection Act 2018
DSA	Directed surveillance authorisation
DSO	Designated Senior Officer
DSU	Dedicated Source Unit
DV	Developed vetting
ECHR	European Convention on Human Rights
EION	European Intelligence Oversight Network
ERS	Error Reduction Strategy
FACT	Federation against Copyright Theft
FIORC	Five Eyes International Oversight Review Council
HMGCC	Her Majesty's Government Communications Centre
ICR	Internet Connection Records
IIOC	Indecent images of children
IP	Internet protocol
IPA	Investigatory Powers Act 2016
IPAR	Internet Protocol Address Resolutions
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
ISA	Intelligence Services Act 1994
JC	Judicial Commissioner
KET	Knowledge Engagement Team
LPP	Legal professional privilege
LTHSE	Long-Term High Security Estate
ML	Machine learning
MoU	Memorandum of Understanding

MPS	Metropolitan Police Service
NCDS	National Communications Data Service
NCMEC	National Centre for Missing and Exploited Children
NPCC	National Police Chiefs' Council
NSIRA	National Security and Intelligence Review Agency (Canada)
NSWG	National Source Working Group
NUWG	National Undercover Working Group
NFC	Near field communications
NGO	Non-governmental organisation
OCDA	Office for Communications Data Authorisations
OpSy	Operational Security Officer
OSJA	Overseas Security and Justice Assistance
PCC	Police and Crime Commissioner
PIC	Participation in crime
PSI	Prison Service Instruction
PSNI	Police Service of Northern Ireland
RN	Retention notice
RfRs	Returns for Rework
RIPA	Regulation of Investigatory Powers Act 2000
RIP(S)A	Regulation of Investigatory Powers (Scotland) Act 2000
ROCU	Regional Organised Crime Unit
RRD	Retention, review and deletion
S4E	Selection for examination
SIO	Senior Investigating Officer
SOP	Standard operating procedure
SOU	Special operations unit
SLE	Service level expectations
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
TAP	Technology Advisory Panel
TIDU	Technical Intelligence Development Unit
TSU	Technical Surveillance Unit
TO	Telecommunications operator
UCPI	Undercover Policing Inquiry
UTC	Universal co-ordinated time
WGD	Warrant Granting Departments

Annex B. Budget

The table below gives a breakdown of the financial statements for the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) for the financial year 2021/22.

	IPCO 01/04/2021 – 31/03/2022 Budget total: £6.4million	OCDA 01/04/2021 – 31/03/2022 Budget total: £9.8million
	2021/22 Full Year Outturn	2021/22 Full Year Outturn
Pay costs	£4,653,395	£ 4,596,023
Travel and subsistence	£168,183	£10,485
Office supplies and services	£12,190	£12,144
Training and recruitment	£4,053	£7,878
Estates	£1,030,606	£501,654
IT and communications	£205,869	£1,047,336
Legal costs (including consultancy)	£26,896	£859
Other costs and services	£38,452	£432
Capital costs	£5,875	£1,000,000
Total	£6,145,519	£7,176,811

The IPCO annual budget allocation is £6.4million. Pay costs continue to account for the majority of budget spend. As a result of attrition and recruitment delays, actual spend was lower than budgeted. We are recruiting to fill vacant positions and anticipate an increase in pay costs in the financial year 2022/23.

Estates costs are higher this financial year as a result of essential building works, including refreshed security measures.

Inspection associated travel accounts for the majority of our travel and subsistence expenditure. Costs have increased in comparison to 2020 when we conducted a significantly higher proportion of inspections remotely.

The OCDA annual budget allocation is £9.8million (£8.4million RDEL and £1.4million CDEL).⁴³ As OCDA is still in an expansion stage with staffing levels increasing, pay costs in 2021/22 were under budget as we continue to recruit up to our designated headcount. This position is expected to continue with recruitment exercises to increase the number of Authorising Individuals expected to continue into the 2022/23 financial year.

43 Resource departmental expenditure limits and capital departmental expenditure limits.

Travel and subsistence remained low as staff continued to work from home with limited travel due to the pandemic. We later moved to a hybrid working pattern which also enabled staff to travel less as meetings continued to be available via remote video conferencing. Due to staff continuing to work from home, office supplies consisted largely of ergonomic equipment procurement to assist homeworking.

OCDA utilises a bespoke IT platform to receive applications. The running costs and development of various systems to allow for application transfer accounts for the vast majority of the IT costs with an annual budget of £2million to support maintenance and development.

Annex C. Serious errors

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

The following terms are used in this annex:

- TO: telecommunications operator
- NCMEC: National Centre for Missing and Exploited Children
- IPAR: Internet Protocol Address Resolution [a request made to a TO to find out the customer assigned IP at a particular time and date]
- Residential VPN: A ResVPN User's IP address is only visible to the proxy and not the internet site or service they are accessing

Error investigation 1

	Public Authority
Human or Technical:	Technical
Classification:	Hacking
Data acquired:	Customer information relating to an IPAR
Description:	<p>A public authority received a NCMEC report advising use of a social media account to upload indecent images of children. The report provided details of a UK IP address used to upload the indecent images. Once the IP address was resolved, the circumstances contained within the NCMEC report led officers to conduct a safeguarding visit. No evidence of illegal activity was found on that visit.</p> <p>Once reported to IPCO, the investigation focussed on the data provided to the NCMEC by the overseas TO.</p> <p>Within a month, two further incidents occurred: one involving the same TO (error investigation 9) the other involving a Child Protection System (see error investigation 10).</p>
Consequence:	<p>A safeguarding visit was carried out at a home of a family unconnected to this investigation.</p> <p>After extensive investigation and consultation with industry experts and members of the Technology Advisory Panel, it was established the cause of the error was a technical issue related to the use of a Virtual Private Network. The exact cause of the error could not be identified as the cause was beyond the control of the public authority acquiring the communications data (CD). However, the circumstances did not amount to a relevant error.</p>

Error investigation 2

	Public Authority
Human or Technical:	Human
Classification:	Breach of Code
Data acquired:	Subscriber information and call data relating to a telephone number
Description:	<p>A public authority acquired CD linked to an internal investigation. During an inspection, an IPCO Inspector identified that the justification for its acquisition failed to reach the threshold of the request for CD being lawful.</p>
Consequence:	<p>A set of minimum requirements has been provided to the operational community and to OCDA authorising officers by the IPC to clarify the acquisition of CD in certain cases.</p>

Error investigation 3

	Public Authority
Human or Technical:	Human (Third Party)
Classification:	Incorrect Data (Human)
Data acquired:	Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	A national helpline reported concerns for a person they had been in contact with. During the transfer of the IP address to the public authority, the national helpline inadvertently provided an IP address not connected to this incident.
Consequence:	Police visited the premises of a family 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. This incident was resolved without the need to acquire further CD.

Error investigation 4

	Public Authority
Human or Technical:	Human (Applicant)
Classification:	Incorrect Data (Human)
Data acquired:	Subscriber information and call data relating to a telephone number
Description:	A public authority was trying to locate a patient who had walked out of a care home. The officer who attended provided their Force Control Room with a number for the patient that turned out to be a number linked to another investigation.
Consequence:	Police contacted an individual unconnected to their search. The person sought was located safe and well. The effect on those contacted was assessed not to have caused significant prejudice or harm.

Error investigation 5

	Public Authority
Human or Technical:	Human (Researcher)
Classification:	Transposition
Data acquired:	Customer information relating to an IPAR
Description:	<p>A public authority received a NCMEC report advising use of a social media account to upload an indecent image of a child. The report provided details of a UK IP address used to upload the image.</p> <p>Once the details of the customers using this IP address were resolved, the information was passed to another public authority. Officers attended the address and with no one at home, they left to return later. Before returning, a transposition error was discovered and the revisit cancelled.</p>
Consequence:	<p>A visit to a family unconnected to this incident was stopped before they became aware.</p> <p>As no contact with the customer was made, no harm was caused.</p>

Error investigation 6

	Public Authority
Human or Technical:	Human (Applicant)
Classification:	Transposition
Data acquired:	Subscriber information and call data relating to a telephone number
Description:	<p>A public authority sought data on a number believed to be used by a wanted person. The number had been obtained from another public authority. Three persons who featured within the CD acquired were contacted in attempts to locate the wanted person. It was soon established that the number passed was incorrect by one digit.</p>
Consequence:	<p>Contact made with three individuals unconnected to a search for the wanted person.</p> <p>The effect on those contacted was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error.</p>

Error investigation 7

	Public Authority
Human or Technical:	Human (Single Point of Contact)
Classification:	Incorrect Data (Human)
Data acquired:	Customer information relating to an IPAR
Description:	<p>A national helpline reported concerns for a person with whom they had been in contact. Details of the IP address (minus the time zone) were passed to the public authority. Given the urgency, an assumption was made that the time zone was the prevailing one, i.e. British Summer Time.</p> <p>An officer who attended the address was able to establish that the location was not the correct address and left without disturbing the occupants.</p> <p>A second resolution this time in Greenwich Mean Time was carried out and a different location was identified. This proved to be the correct address.</p>
Consequence:	<p>A visit to a family unconnected to this incident was stopped before they became aware.</p> <p>No contact with the customer was made and so did not meet the threshold of a serious error.</p>

Error investigation 8

	Public Authority
Human or Technical:	Human (Third Party)
Classification:	Incorrect Data (Human)
Data acquired:	Customer information relating to an IPAR
Description:	<p>A national helpline reported concerns for a person they had been in contact with. During the transfer of the IP address to the public authority, an incorrect digit had been included.</p> <p>The correct IP address was then resolved which enabled officers to conduct their welfare check.</p>
Consequence:	<p>Police visited the premises of a family 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.</p>

Error investigation 9

	Public Authority
Human or Technical:	Technical
Classification:	Hacking
Data acquired:	Customer information relating to an IPAR
Description:	<p>A public authority using the Child Protection System identified two homes believing the IP addresses allocated to each had been sharing indecent images of children.</p> <p>Officers then attended each address under a search warrant. While no arrests were made, all internet enabled devices were seized. Upon examination no incriminating material was found.</p> <p>Once reported to IPCO, our investigation led to a belief that a Residential VPN had been used to mask the activity of the real culprit. In turn, this conclusion was assessed to have also occurred in error investigations 1 and 10.</p>
Consequence:	<p>Warrant executed at the homes of families unconnected to this investigation.</p> <p>After extensive investigation and consultation with industry experts and members of the Technology Advisory Panel, it was established the cause of the error was a technical issue related to the use of a Virtual Private Network. Although the exact cause of the error could not be identified as the cause was beyond the control of the public authority acquiring the CD, the circumstances did not amount to a relevant error.</p>

Error investigation 10

	Public Authority
Human or Technical:	Technical
Classification:	Hacking
Data acquired:	Customer information relating to an IPAR
Description:	<p>A public authority received a NCMEC report advising use of a social media account to upload indecent images of children. The report provided details of a UK IP address used to upload the indecent images. Once resolved, officers attended the home of the customer under a search warrant. While no arrests were made, 11 internet enabled devices were seized.</p> <p>Upon examining the seized devices, no incriminating material was found on any of them. With no error in the resolution of the IP address, the matter was not initially reported to IPCO.</p> <p>The incident was later identified and linked to error investigation 1.</p>
Consequence:	<p>A warrant was executed at the home of a family unconnected to this investigation.</p> <p>After extensive investigation and consultation with industry experts and members of the Technology Advisory Panel, it was established the cause of the error was a technical issue related to the use of a Virtual Private Network. Although the exact cause of the error could not be identified as the cause was beyond the control of the public authority acquiring the CD, the circumstances did not amount to a relevant error.</p>

Error investigation 11

	Public Authority
Human or Technical:	Human (Other)
Classification:	Intelligence
Data acquired:	Subscriber information and call data relating to a telephone number
Description:	A public authority sought data on a number believed to be used by a wanted person, which had been obtained from the public authority's intelligence system. Officers attended the address linked to the number and a brief search was conducted. A review discovered the number was that of an associate. It had been incorrectly recorded as belonging to the wanted person.
Consequence:	Visit and search of a home based on incorrectly recorded information. The effect on those present through the visit was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error.

Error investigation 12

	Public Authority
Human or Technical:	Human (Third Party)
Classification:	Incorrect Data (Human)
Data acquired:	Subscriber information and call data relating to a telephone number
Description:	A third party reported a concern for welfare and provided to the public authority a telephone number for their patient. The CD acquired led officers to speak to the user of this number. During the conversation it became clear that an error had occurred and the user was not the patient being sought.
Consequence:	Police contacted a person unconnected to this incident. The effect on the person spoken to was assessed not to have caused significant prejudice or harm and so did not meet the threshold of a serious error. The person at the centre of this incident was located safe and well.

Error investigation 13

	Public Authority
Human or Technical:	Human (Third Party)
Classification:	Incorrect Data (Human)
Data acquired:	Subscriber information and call data relating to a telephone number
Description:	<p>A public authority was investigating a potential kidnap. Based on a telephone number supplied, officers acquired CD and attended an address. On speaking to the user of this number it became apparent that the person was not involved.</p> <p>The initial information was rechecked and the initial number supplied found to be incorrect.</p>
Consequence:	<p>Police visited a person unconnected to this incident.</p> <p>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.</p>

Error investigation 14

	Public Authority
Human or Technical:	Human (SPoC)
Classification:	Transposition
Data acquired:	Subscriber information
Description:	<p>A public authority was investigating a crime where the suspect had been identified via social media. The telephone number linked to the social media account was resolved to an address in another force area. An enquiry by this other force led officers to speak to the subscriber of the number. It became apparent quickly that the subscriber was not involved. A check of the acquisition process found the number on the notice supplied to the TO was incorrect.</p>
Consequence:	<p>Police visited a person unconnected to this incident.</p> <p>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.</p>

Error investigation 15

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data (System)
Data acquired:	Customer information relating to an IPAR
Description:	<p>A public authority using a live web chat function received a message of an intention to carry out a serious criminal act. The IP address connected to this message was identified and resolved to the customer's address. Officers attended this address and made an arrest. Following questioning, officers suspected a possible error with the IP address associated to the message.</p> <p>Their suspicion proved to be correct when it was confirmed that the web chat software had recorded the arrested person's own web chat wrongly as that of the subject of this investigation.</p>
Consequence:	<p>Arrest of a person unconnected to this investigation.</p> <p>Following investigation, IPCO determined the cause of this error was a defect in the software procured from a commercial provider. As such it was not a failure by a public authority to comply with any requirements imposed on it by the IPA or the Code of Practice, and therefore not a relevant error (under section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority). The software defect was rectified to prevent any further occurrence and the public authority notified of its obligation under section 67 of the Data Protection Act 2018 to report the incident to the Information Commissioner. The person wrongly arrested is pursuing a civil claim against the public authority concerned.</p>

Error investigation 16

	Telecommunications operator (TO)
Human or Technical:	Human (Third Party)
Classification:	Incorrect Data (Human)
Data acquired:	Customer information relating to an IPAR
Description:	A public authority was trying to locate a missing person. The overseas TO linked to their social media account provided a postal address based on the profile provided. The address was visited and while having the same name, was not the missing person. A check with the family established the wrong profile had been provided.
Consequence:	Police visited the premises of an individual unconnected to their search. 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 missing person was located safe and well.

Error investigation 17

	Telecommunications operator (TO)
Human or Technical:	Human (Third Party)
Classification:	Incorrect Data (Human)
Data acquired:	SIM data
Description:	A public authority was investigating the supply of controlled drugs. An application for CD was approved and acquired from the TO. This led to officers visiting an outlet that had no connection to this investigation. A review led SPoCs to question with the TO the data it had provided. In turn, the TO was able confirm the error occurred from data supplied to them by a third person.
Consequence:	Police visited a business premises unconnected to their investigation. Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.

Error investigation 18

	Telecommunications operator (TO)
Human or Technical:	Human (Customer)
Classification:	Incorrect Data (Human)
Data acquired:	Subscriber information
Description:	A public authority was trying to locate a person linked to a concern for welfare after a 999-call dropped out. The TO linked to the number was approached and details of the subscriber supplied. It transpired the address provided was incorrect as the customer had failed to update a change of address.
Consequence:	Police visited the premises of individuals unconnected to their search. The corrected subscriber check led another set of officers to a house where the person was located. Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.

Error investigation 19

	Telecommunications operator (TO)
Human or Technical:	Human (Disclosure Officer)
Classification:	Incorrect Data (Human)
Data acquired:	Mobile IPAR
Description:	A public authority made a request to a TO for data concerning the use of a mobile device over the internet via a cellular network. The data provided identified details of a person unknown to the investigation. This was challenged with the TO and a possible technical error was suggested and reported to IPCO. Our investigation found that a human error, rather than a technical error, had occurred.
Consequence:	CD obtained on a number unconnected to this investigation. Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.

Error investigation 20

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data (System)
Data acquired:	13 different Communications Data Record (CDR) data sets involved
Description:	<p>A TO reported to IPCO a technical issue resulting in a possible excess or shortfall of certain data sets returned.</p> <p>The cause was established and fixed.</p> <p>The issue was briefed out to all relevant public authorities.</p>
Consequence:	<p>After three months, a review assessed that there had been no discernible impact.</p> <p>Under Section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p> <p>In this case no error by the public authority was made.</p>

Error investigation 21

	Telecommunications operator (TO)
Human or Technical:	Human (Disclosure Officer)
Classification:	Incorrect Data (Human)
Data acquired:	Customer information relating to an IPAR
Description:	<p>A public authority was trying to locate a missing person. The overseas TO linked to their social media account provided under an authority detail of their most recent logon. The IP address used was resolved resulting in officers attending the customer's home address. On finding no link to the missing person an error was suspected.</p> <p>It transpired the IP address provided was incorrect, the result of human error.</p>
Consequence:	<p>Police visited the premises of individuals unconnected to their search.</p> <p>The corrected IP address check led another set of officers to where the person was located.</p> <p>Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p> <p>In this case no error by the public authority was made.</p>

Error investigation 22

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data (System)
Data acquired:	Mobile Event Data
Description:	<p>A public authority queried the results supplied to them by a TO. The public authority queried whether there was a time zone error within the call data.</p> <p>As a result the TO carried out a review, finding 119 data sets where the automated system had not changed the date stamp from Universal Co-ordinated Time to British Summer Time.</p> <p>Upon discovery and as a matter of urgency all affected public authorities were contacted.</p>
Consequence:	<p>Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p> <p>In this case no error by the public authority was made.</p>

Error investigation 23

	Telecommunications operator (TO)
Human or Technical:	Human (Disclosure Officer)
Classification:	Incorrect Data (Human)
Data acquired:	Account information
Description:	<p>A public authority was investigating a murder. As part of this investigation CD was sought from a TO. This led officers to question its subscriber at their home address. On speaking with them the officers quickly suspected an error.</p> <p>A check with the TO involved confirmed what they had supplied to have been erroneous.</p>
Consequence:	<p>Contact made with a person unconnected to this investigation.</p> <p>After three months, a review assessed no discernible impact.</p> <p>Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p> <p>In this case no error by the public authority was made.</p>

Error investigation 24

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data (System)
Data acquired:	Short Message Service (SMS)
Description:	<p>A TO reported to IPCO a technical issue resulting in a possible excess or shortfall of SMS activity. The cause was established (time zone changes GMT/BST) and fixed.</p> <p>The issue was communicated to all relevant public authorities.</p>
Consequence:	<p>After three months, a review assessed that there had been no discernible impact.</p> <p>Under Section 231(9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p> <p>In this case no error by the public authority was made.</p>

Annex D: Public engagements

The Investigatory Powers Commissioner (IPC) undertook several public engagements in 2021. Details of those engagements are given below.

Meetings with Ministers

Date	Meeting
24 March	The Rt Hon. Michael Ellis QC MP, Attorney General
16 June	The Rt Hon. Dominic Raab MP, Foreign Secretary

Engagement with NGOs and academics

Date	Event
30 March	Meeting with Liberty
1 June	Meeting with Reprieve
28 October	Meeting with Privacy International

Engagement with Public Authorities

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

Date	Meeting
8 February	Matthew Rycroft CBE, Permanent Secretary, Home Office
10 March	Dr Jo Farrar, Second Permanent Secretary, Ministry of Justice and Chief Executive Officer HM Prison and Probation Service
8 April	Max Hill QC, Director of Public Prosecutions
12 May	Jonathan Hall QC, Independent Adviser on Terrorism Legislation
22 June	John Wadham, PSNI Human Rights Adviser
3 September	Elizabeth Denham CBE, Information Commissioner
28 October	Professor Fraser Sampson, Biometrics and Surveillance Camera Commissioner
15 November	Sir John Mitting, Chair, Undercover Policing Inquiry
22 November	Metropolitan Police Service meeting to discuss the Daniel Morgan Inquiry report
2 December	The Rt Hon. Lord Justice Singh, President, Investigatory Powers Tribunal

Engagements with media

Date	Meeting
28 October	Joshua Rozenberg QC (hon), Legal Gazette

Engagements with overseas bodies

Date	Event
20 September	International Oversight Working Group (virtual). The IPC was represented by a member of the Technology Advisory Panel and an IPCO Inspector
7-8 October	European Intelligence Oversight Conference, Rome
8-10 November	Five Eyes Intelligence Oversight and Review Council meeting (virtual)

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