

IPCO

Investigatory Powers
Commissioner's Office

Annual Report 2018

Annual Report of the Investigatory Powers Commissioner 2018

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 5 March 2020

Laid before the Scottish Parliament by the Scottish Ministers 5 March 2020

HC 67

SG/2020/8



© Crown copyright 2020

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

ISBN 978-1-5286-1604-1

CCS0819890016 03/20

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office.

Contents

| | |
|--|------------|
| Letter to the Prime Minister | 5 |
| 1. Introduction by the Investigatory Powers Commissioner Lord Justice Fulford | 6 |
| 2. Legal and Policy | 9 |
| 3. Protecting confidential or privileged information | 22 |
| 4. Engagement | 24 |
| 5. Inspection methodology | 27 |
| 6. MI5 | 35 |
| 7. Secret Intelligence Service (SIS) | 43 |
| 8. Government Communications Headquarters (GCHQ) | 49 |
| 9. Ministry of Defence | 57 |
| 10. Consolidated Guidance | 59 |
| 11. Law Enforcement Agencies | 66 |
| 12. Public authorities | 82 |
| 13. Local authorities | 87 |
| 14. Prisons | 95 |
| 15. Warrant Granting Departments | 100 |
| 16. Technology Advisory Panel | 102 |
| 17. Errors and breaches | 104 |
| 18. Statistics | 114 |

| | |
|---|------------|
| Annex A: Glossary of authorities | 120 |
| Annex B: Budget | 122 |
| Annex C: Serious errors | 123 |
| Annex D: Communications Data | 135 |
| Annex E: Public engagements | 139 |

Letter to the Prime Minister

The Rt Hon. Boris Johnson MP
Prime Minister
10 Downing Street
London
SW1A 2AA

December 2019

Dear Prime Minister,

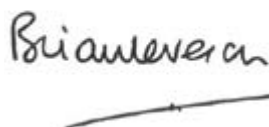
I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office from 1 January to 31 December 2018.

Although I am submitting the Report, having recently been appointed as the Investigatory Powers Commissioner, this covers a period under my predecessor, the Rt Hon Lord Justice Fulford, and the introduction in the following pages therefore comes from him. The Report is, as those before have been, written in two sections. This public report includes information on the use of covert powers by UK authorities and includes the details required of my office under section 234 of the Investigatory Powers Act 2016. The Confidential Annex to this report contains sensitive details which should not be published for reasons of national security.

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.

I would like take this opportunity to thank Lord Justice Fulford for his exemplary work as Commissioner, as well as the other Judicial Commissioners and the team of the Investigatory Powers Commissioner's Office. Although I have only been in post for a few weeks, it is clear that an incredibly high standard has been set for the oversight of the use of covert powers across the UK, which we can build on through the years to come. I also wish to pay tribute to the work of the authorities that we oversee; they have demonstrated exceptional dedication and professionalism, which are critical to the successful application of these powers.

Yours sincerely,



The Rt Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

1. Introduction by the Investigatory Powers Commissioner Lord Justice Fulford

I am very pleased to be able to discharge my responsibilities as Investigatory Powers Commissioner in presenting the 2018 report on the *'carrying out of the functions of the Judicial Commissioners'*. This is my second IPCO Annual Report to the Prime Minister and, in the event, it is my last.

Under the terms of the Investigatory Powers Act 2016, the Report must include information on the following:

- statistics on the use of the relevant investigatory powers, such as the number of warrants received, how they were used by the individual applicant authorities and the impact of their use;
- the operation of the safeguards under the Act in relation to material covered by legal professional privilege and confidential journalistic material and sources;
- the ways in which certain targeted warrants were handled;
- details of the operational purposes, as set out in the warrants;
- the number of errors reported to the Investigatory Powers Commissioner's Office (IPCO), and the number of individuals to whom we provided relevant information as a consequence of the errors;
- details of the work of the Technology Advisory Panel (TAP);
- an explanation of our resources; and
- the public engagements undertaken by the Judicial Commissioners (JCs) and members of my staff.

Structure of the report

Last year, the report was organised into chapters which reflected each of the powers we oversee and it contained a significant level of detail as to how each of these powers were used. That provided a highly useful explanation of the work of IPCO but it would be unnecessarily repetitive if this approach is adopted each year. As a result we have used a markedly different structure in the present report, with chapters on each of the types of organisations we inspect and focusing on the key findings from our inspections. This gives a clearer sense of the range of issues we address in each of the different bodies we oversee, without readers needing to move between the various chapters to comprehend the full picture. IPCO continues to develop a new inspection regime for the multiple organisations for which we have responsibility, and I have no doubt that my successor will have his own views on how best to present the information we gather each year.

There undoubtedly remains an imbalance in the amount of information we provide, in the sense that there is more detail of our inspections of the intelligence agencies in comparison with the inspections of other public authorities. This is unavoidable, given the number and the depth of the inspections

we carry out at the security services. The complexity of their work and the range of powers they exercise has the consequence that our inspectors often visit each of the three Agencies more than once a month, and over the year we concentrate disproportionately on their activities. This is entirely necessary and I am satisfied that the balance of reporting reflects an appropriate allocation of resources.

I will not repeat or seek to summarise in this introduction the multiplicity of issues covered in detail elsewhere in the report, but there are nonetheless a small number of key points I would wish to make.

The first full year of IPCO

The challenges of establishing the new team continued throughout 2018. We experienced lengthy delays in recruitment, particularly in the time taken by the vetting process; the Inspectorate only reached full strength in January 2019 and our much-needed policy and engagement teams only joined during the summer of 2019. Even with these welcome developments, at the end of 2019, we do not yet have a full team in place. This has undoubtedly had an impact on our ability to take the initiative in a number of areas, especially in terms of our external communications and engagement, both of which are important fields that undoubtedly need development. I am confident, however, that we will see significant improvement in this context over 2020.

Much of our focus during 2018 was in preparing for the introduction of the double lock arrangements for the use of the most intrusive powers. New processes were designed and tested and, as I indicated last year, the JCs have had the benefit of an extensive training programme, engineered to give them the best possible understanding of the range of powers utilised by the agencies and authorities. As this was a year of transition, the statistics at the end of the report do not provide as full a picture as they will in future years, but it is clear that there were only a few refusals by the JCs of the applications they considered. It is critical that this should not be interpreted as a failure by the JCs to provide rigorous scrutiny of the applications. Nothing could be further from the truth.

These applications only come to IPCO after there has been detailed, multi-layered consideration within the organisation requesting the authorisation and, when applicable, the Warrant Granting Department. In-house legal advice is regularly given and approval is required from either the Secretary of State or a senior officer. These steps constitute a critical filtering process. Furthermore, when an application is considered to be novel or contentious, the JCs and the warrant-granting departments are frequently briefed in advance, at which stage preliminary, non-binding views of a general nature are often given as to the proper and lawful approach to be taken by the agency or authority seeking authorisation before any warrants are submitted for consideration. This process tends to ensure that unnecessary mistakes are avoided in the applications. Our inspections have continually revealed the high level of challenge provided by those in the Warrant Granting Departments (before the applications are put before the Secretary of State) and by the authorising officers within the various relevant bodies. This means that there has been detailed scrutiny of the applications by multiple individuals, including either the Secretary of State or a senior officer, before the application is received by IPCO.

I have encouraged the JCs to seek clarification or additional information if they have questions or concerns about a particular application. This process frequently involves discussions between the JCs and IPCO's legal team, assisted by the Inspectorate, with a certain amount of toing and froing with the applicant body and, when relevant, the Warrant Granting Department. This process is carefully controlled and properly documented to maintain the essential arms-length relationship, and it avoids an unnecessary refusal when the substance of the application is lawful and all that is required is further detail or an element of explanation, if this is available.

As a result, the applications, in their final form when considered by the JCs, have a high likelihood of being approved. In my view, this reflects the strengths of the process rather than any kind of failure by IPCO to uphold the necessary high standards of legality.

New and emerging technologies

It is essential that all public authorities are able to understand and, when appropriate, deploy the relevant new and developing technologies, against the background of proper guidance and regulation. On inspections, we focus particularly on how new and emerging technologies are used, ensuring they offer lawful and viable options for investigation. A number of these new techniques have the added bonus of helping to reduce inappropriate collateral intrusion. This is a complicated arena because the statutory framework is not always best framed to cope with these often rapid changes. For example, we have been involved in detailed discussions about the use of automatic facial recognition (AFR, also known as live facial recognition (LFR)) technologies during the last year. AFR is a surveillance tool, the use of which by both public authorities and other bodies (such as corporate organisations which are outside IPCO's statutory oversight) has seen a growth and which has, in 2019, been the subject of litigation and independent review by the Information Commissioner. This is a paradigm example of why Her Majesty's Government (HMG) needs to formulate a clear position as to which of these new and emerging techniques should be deployed, and how this is to occur, to ensure their use is lawful, not least by way of proper regulation and oversight. I am aware that this is a complicated problem that HMG is working to address but it is critical that the relevant authorities are "ahead of the game", anticipating and providing for these changes rather than simply responding to the inevitable and expensive legal challenges that will follow a lack of substantive and properly formulated regulation.

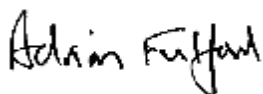
OCDA

As this is my last official opportunity, I wish to pay tribute to the way in which the Office for Communications Data Authorisations (OCDA) has been established. OCDA commenced work in 2019 and will, as a result, feature materially for the first time in next year's annual report, but much of the preparation for the new office was completed in 2018. As with IPCO, OCDA is the responsibility of the Investigatory Powers Commissioner and we were faced with many of the same accommodation, resourcing and logistical challenges that we resolved with the creation of IPCO. The work of those involved in establishing this new office was exemplary, and OCDA is now fully and successfully operational.

Moving On

I write this as I prepare to leave the post of Investigatory Powers Commissioner. It has been an enormous privilege to be the first IPC and I regret my early departure. However, the pull of the full-time judiciary, and particularly my new role as Vice-President of the Court of Appeal (Criminal Division), was too strong to resist. I would, however, like to take this opportunity to express my profound gratitude to everyone who provided such a high-level of assistance during my tenure as IPC. I shall never forget nor cease to be impressed by the levels of professionalism and dedication I have witnessed in this critical and sensitive area of our public life. It is a testament to the success of IPCO and OCDA, and to the many outside bodies and individuals who helped in their creation, that they have been established successfully within very short timeframes, and – as unwaveringly reported to me – they have not had an adverse impact on the operational agility of any of the public bodies who are entitled to seek to exercise investigatory powers.

I am relieved to leave both organisations in the undoubted safe pair of hands of Sir Brian Leveson. I have no doubt that he will bring his own particular vigour and probing intellect to the role. I wish him every success in his new endeavour.



Sir Adrian Fulford

2. Legal and Policy

Overview

- 2.1 Policy and operational developments can have a substantial effect on the work of the Investigatory Powers Commissioner's Office (IPCO) and the powers we oversee can be the subject of direct and indirect challenge in the UK and European courts. In the recent past we have seen attempts to strike down both the relevant legislation and individual powers. We monitor these cases with care given they can directly affect our oversight role and we provide such assistance as the courts or Investigatory Powers Tribunal (IPT) may reasonably require of us.
- 2.2 This chapter gives an overview of the key legal and policy issues that impacted on IPCO in 2018.

Implementation of the Investigatory Powers Act 2016 (IPA)

- 2.3 The introduction of the 'double lock' (as defined overleaf) has established a crucial new element to judicial oversight of the UK's intelligence and security agencies, giving Judicial Commissioners (JCs) the responsibility of independently reviewing authorisations sought under the Act. Before commencing this role, the JCs undertook extensive training, covering the work of the intelligence and law enforcement agencies and how each power is used operationally. These briefings, which were made possible by the provision of a substantial dedicated team from the intelligence agencies, significantly contributed to the JCs' understanding of the operation of investigatory powers before and after the commencement of the double lock on 27 June 2018.
- 2.4 The relevant sections of the Investigatory Powers Act 2016 (IPA) commenced in stages from June 2018, as follows:

| Date | Public authority | Change |
|------------------------|--|--|
| 27 June 2018 | UK Intelligence Community (UKIC) and the Ministry of Defence (MOD) | Double-lock of all warrants, except bulk personal and bulk communications data (BCD) |
| 22 Aug 2018 | UKIC | Double-lock of bulk personal and BCD warrants |
| 26 Sept 2018 | Law Enforcement Agencies (LEAs) | Double-lock of targeted interception warrants |
| 5 Dec 2018 | LEAs | Applications for targeted equipment interference submitted under the IPA |
| 5 February 2019 | All authorities with CD powers | Changes to serious crime provisions and statutory purposes for communications data (CD) applications |

| Date | Public authority | Change |
|-----------------------|---|---|
| 27 Feb 2019 | Government Communications Headquarters (GCHQ) | Double-lock of CD applications relating to journalistic sources |
| 15 Mar 2019 | Secret Intelligence Service (SIS) | Double-lock of CD applications relating to journalistic sources |
| 22 Mar 2019 | MI5 | Double-lock of CD applications relating to journalistic sources |
| 18 Mar 2019 (rolling) | Public authorities | Double-lock of CD applications relating to journalistic sources and introduction of authorisations via the Office for Communications Data Authorisations (OCDA) |

- 2.5 In addition to the preparatory briefings referred to above, we have benefited from a wide range of discussions on emerging issues. We now hold, for example, quarterly meetings of the JCs for consideration of the present intelligence threats, technological or operational developments and legal challenges.
- 2.6 The JCs occasionally seek additional information about applications for warrants before making a decision. The Investigatory Powers Commissioner (IPC) and the JCs have encouraged briefings from the agencies well in advance of receiving novel or contentious applications; this process is working well and is welcomed by all.
- 2.7 We have been increasingly impressed by the advantage of IPCO's dual role: first, undertaking the review of warrants and, second, having retrospective oversight of the use of investigatory powers. This combination of responsibilities provides IPCO with a detailed level of insight into the factors relevant to applications for warrants and the use of covert powers which otherwise would not exist. JCs regularly ask the inspectors to focus on particular issues during the latter's' oversight visits and the inspectors similarly share information relevant to the warrant process with the JCs. In other words, these two functions – warrantry and ex post facto (retrospective) inspection – serve significantly to enhance each other and the confidence in the overall system.

The double lock process

The Investigatory Powers Act 2016 (IPA) brought a significant change to the way in which certain investigatory powers are authorised and overseen. The most significant change was the introduction of what has become colloquially termed the 'double lock' mechanism. This means that, following Secretary of State authorisation, an IPA warrant cannot be issued until it has been approved by a JC.

The appeals process

- 2.8 Under section 23 (5) of the IPA, if a JC (other than the IPC) refuses to approve the application for a warrant, the requesting authority may ask the IPC to decide whether to approve the decision to issue the warrant.

First use of the appeals process

- 2.9 A single decision was appealed in 2018 when, in November, a JC refused a pair of applications for warrants from SIS.
- 2.10 SIS sought two warrants authorising the retention and examination of a particular class of bulk personal datasets. The authorisations were approved by the Foreign Secretary but rejected by a JC. The JC was not persuaded that the data sought could appropriately be obtained under a class authorisation or that the Head of the Agency had given sufficient consideration to the application.
- 2.11 The case for appeal can be summarised as:
- the Secretary of State could be satisfied that the Head of SIS had applied his mind to the provisions of sections 202 and 203 of the IPA so as to have concluded that none of the section 202 restrictions applied to any of the datasets sought to be retained and examined;
 - the JC's decision was inconsistent with certain relevant determinations by other JCs; and
 - the material in the datasets did not contain protected data and therefore could be held under a class warrant.
- 2.12 The IPC reviewed the case, considering the application and the argument set out by the Foreign and Commonwealth Office (FCO) and SIS. In granting the appeal, the IPC disagreed with the 'personal certification role' that the JC had accorded to the Head of the SIS at the time the warrants were submitted to the Secretary of State. The IPC concluded that the section 202 issues were appropriately addressed by the applicant agency in the two renewed warrant applications. The IPC was also satisfied that there was sufficient information before the Secretary of State to justify a conclusion that the datasets did not contain protected data.

Technical capability notices (TCNs), national security notices (NSNs), and communications data retention notices

- 2.13 The IPA introduced the power for the Secretary of State to issue notices to communications service providers and UK companies to assist public bodies and agencies working under the Act. These provisions consolidated a number of existing arrangements and established a clear mechanism for authorising this activity. The JCs perform the double lock function, ensuring that each notice given is necessary and the actions required of the company or operator is proportionate to the stated aims of the work.

TCNs and NSNs

- 2.14 The Technology Advisory Panel (TAP) and IPCO's legal team assisted the JCs in considering TCNs and NSNs once the provisions had come into force during 2018. Briefings, covering technical detail and practical processes, were given to the JCs to assist in their consideration of these applications. The notices covered activity that had been authorised under the previous provisions and accordingly the TCNs and NSNs sought in 2018 were designed to bring them within the IPA statutory framework.

2.15 The JCs approved the notices in each case and written reasons were provided.

Technical Capability Notices (TCNs)

Under s253, the Secretary of State, with approval from a JC, may use TCNs to give telecommunications or postal operators notice of the requirement to have the capability to provide assistance with interception, equipment interference and the acquisition of bulk communications data (BCD). After a TCN has been issued, a company can act quickly and securely when a warrant is authorised.

National Security Notices (NSNs)

Under s252 IPA, a Secretary of State, with approval from a JC, can use an NSN to direct a UK telecommunications officer to act in the interests of national security. This covers actions to assist the security and intelligence agencies, which may be additionally authorised under a warrant. NSNs could, for example, ask a company to provide access to a particular facility.

Communications data retention notices

2.16 In November 2018, a JC considered and approved a number of communications data retention notices. These notices reflected the amendments to the IPA contained in the Data Retention and Acquisition Regulations 2018 which list the statutory purposes for which CD is to be retained, including the changes to the 'crime purpose' in order to comply with EU law.

Communications data retention notices

Section 87 of the Investigatory Powers Act 2016 gives the Secretary of State the power to give a data retention notice to a telecommunications operator or postal operator, requiring them to retain relevant communications data (CD) for a maximum of 12 months, if it is considered necessary and proportionate for one or more statutory purposes. A notice to retain CD can only be given where the Secretary of State, having taken into account relevant information, considers it necessary and proportionate to do so and where the decision to do so has been approved by a Judicial Commissioner.

Review of the Consolidated Guidance

Background

2.17 In 2010, the Government published the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees* (the Consolidated Guidance). The purpose of the Consolidated Guidance was to ensure, in accordance with the UK Government's core policy, that UK personnel 'do not participate in, solicit, encourage or condone the use of torture or cruel, inhuman or degrading treatment or punishment for any purpose'.

- 2.18 The Consolidated Guidance had three principal objectives:
- to protect individuals abroad from harm because of actions by British officials when they were involved in sharing intelligence with foreign partners, in situations when the person was in detention or detention was sought or would occur;
 - to protect British officials from legal liability and to ensure that all conduct of British officials was lawful as a matter of both domestic and international law; and
 - to ensure wide-ranging compliance in the context of intelligence sharing with the national policy, and particularly the United Kingdom's refusal to be involved in unlawful killing, the use of torture or cruel, inhuman or degrading treatment, or extraordinary rendition.
- 2.19 The Intelligence Services Commissioner oversaw the use of the Consolidated Guidance from its instigation. The Prime Minister directed that this oversight should be carried out by the IPC from 1 September 2017. Findings from our oversight are summarised in chapter 10.
- 2.20 On 28 June 2018, the Intelligence and Security Committee of Parliament (ISC) published its report on Detainee Mistreatment and Rendition. The report was in two parts, the first concerning the period from 2001 to 2010 and the second on current issues. Taking account of the evidence it had heard, the ISC made a number of suggestions as to how the Consolidated Guidance could further be clarified. The Committee's overall view was that the document needed to be reviewed, but indicated that it was not for the ISC to 'rewrite Government policy, or to provide endorsement'.

The IPCO review

- 2.21 On the same day that the ISC Report was published, the Prime Minister invited the IPC 'to make proposals to the Government about how the Guidance could be improved, taking account of the ISC's views and those of civil society'. The IPC was keen that this should take the form of a full public consultation and, on 20 August 2018, we published a consultation document seeking views on a range of questions.¹ We received nine written submissions, from Non-Governmental Organisations (NGOs), and academics and from Her Majesty's Government (HMG).²
- 2.22 On 12 December 2018, Lord Anderson of Ipswich KBE QC hosted an invitation-only event on behalf of the IPC for some of those who had responded or had a particular interest in this area. The event enabled detailed exploration of the central points raised in the responses. It was held at Chatham House and the IPC was extremely grateful to all the participants, who illuminated the risks of torture and inhuman treatment for those in detention in this general context along with the operationally difficult decisions that need to be taken by those entrusted with undertaking this work.
- 2.23 The discussions at Chatham House led, in part, to the decision by the IPC to propose a complete redraft of the Consolidated Guidance as part of his submission to the Prime Minister. He was keen to understand the practical implications of each of the suggested amendments, which was a question which the agencies were uniquely equipped to answer. This process of liaising with them took some time to conclude but his recommendations, which were submitted to the Prime Minister on 12 June 2019, have now been accepted in full.³ The new '*Principles relating to the detention and interviewing of detainees overseas*

1 <https://ipco.org.uk/docs/IPCO%20Consultation%20on%20the%20Consolidated%20Guidance.pdf>

2 <https://ipco.org.uk/default.aspx?mid=13.11>

3 <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-07-18/HCWS1738/>

and the passing and receipt of intelligence relating to detainees’ (The Principles) were published by the Government on 18 July 2019.⁴

The Principles

- 2.24 The IPC’s letter to the Prime Minister of 12 June 2019⁵ sets out the reasons for his proposals but the key points from the new document are summarised below:
- **The need for clarity:** the new document is intended to remove any perceived uncertainty and obscurity, clarifying the core elements of the UK’s policy when applying The Principles in an operational setting;
 - **The types of harm covered:** The Principles will be expressly engaged when there is a risk of unlawful killing, extraordinary rendition or rendition occurring in a detention context;⁶
 - **Threshold of risk:** the threshold of risk for the future is ‘real risk’ rather than ‘serious risk’. This test is generally applied in equivalent contexts (for example, whether there are substantial grounds for believing there to be a ‘real risk’ of torture or cruel, inhuman and degrading treatment (CIDT) or punishment when an individual is faced with extradition);
 - **Non-state actors or groups:** The Principles now explicitly apply when UK personnel might be working with non-state actors or groups; and
 - **Error reporting and whistleblowing:** the new regime now aligns with other aspects of oversight by IPCO, since The Principles create a formal error-reporting process for the agencies, and a formal whistleblowing provision which mirrors the IPC’s statutory responsibilities under section 237 of the IPA.
- 2.25 There were some suggestions that were raised during the consultation process that the IPC did not adopt:
- **Scope:** it was suggested that The Principles should extend to all cases when information is shared and there is a real risk that there will be a serious adverse outcome (such as unlawful killing), regardless of whether this will occur in the context of detention. Given that the fundamental underpinnings of this guidance has been to protect those who are in, or are at risk of, detention, the IPC determined that for the purposes of the present review the current link to detention ought to remain. It will be for the Prime Minister to decide whether consideration should be given to expanding the present focus;
 - **The role of Ministers:** the majority of non-government respondents argued that the revised guidance should include an absolute prohibition on Ministers authorising UK action when there was a real risk of unlawful killing, torture, extraordinary rendition, or CIDT. The IPC concluded, after extensive consultation, that the actions of Ministers are already comprehensively governed by two key requirements: Ministers must act in accordance with domestic and international law and they are bound by the Ministerial Code. Ministers are accountable to Parliament, and in the view of the IPC it would be unhelpful to duplicate, or seek to add to, the clear legal and procedural framework which currently governs ministerial action; and

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818306/20190718_The_Principles_relating_to_the_detention_and_interviewing_of_detainees_overseas.pdf

5 <https://ipco.org.uk/docs/20190612%20Letter%20to%20PM%20.pdf>

6 The term “rendition” is most commonly used to cover the extra-judicial transfer of an individual from one jurisdiction or State to another and “extraordinary rendition” is generally used to refer to rendition when there is a real risk of torture or cruel, inhuman or degrading treatment.

- **A post-notification framework:** it was argued that a post-notification process for individuals who had been mistreated following a failure to apply any new guidance or principles would assist them in seeking redress. This, however, would require statutory change and was, therefore, beyond the remit of the IPC's review. That said, the Principles place a duty on public authorities who become aware of abuses to notify the IPC as soon as possible. This will ensure early oversight by IPCO of the alleged conduct.

2.26 The Principles will take effect from 1 January 2020. IPCO and the relevant authorities, particularly the National Crime Agency (NCA) and Metropolitan Police's Counter Terrorism Command (also known as SO15⁷), are jointly analysing the implications for the future inspection regime and will provide a full report on the first year of operation in IPCO's 2020 Annual Report.

Juvenile Covert Human Intelligence Sources (CHIS)

- 2.27 A juvenile CHIS (covert human intelligence source) is an individual engaged in CHIS activity who is aged below 18 years. Under the Regulation of Investigatory Powers Act 2000 (RIPA), the use of juveniles as CHIS is governed by statute. Until August 2018, use of a juvenile CHIS could only be authorised for a month at a time. The CHIS Code of Practice (COP) has now been updated and the authorisation period has been extended to four months, with the requirement that such cases are reviewed on at least a monthly basis.⁸ These changes came into force on 15 August 2018.
- 2.28 During the course of Parliamentary debate on change to the Code, concerns were raised about juveniles being used as CHIS in any circumstances. Although anecdotal evidence suggested that this happened only on very rare occasions, there was an absence of actual statistics to support this. The IPC, therefore, ordered an immediate review of all public authorities within the UK which had the statutory power to use CHIS, to ensure we had a comprehensive record of how often these powers were deployed in relation to juveniles. The conclusions of this review, following a careful accuracy check, were reported in March 2019 in a letter to the Rt Hon Harriet Harman QC MP, the Chair of the Joint Committee on Human Rights. This letter is available on the IPCO website.⁹
- 2.29 In conducting this review, we sought information covering the period between January 2015 and the end of 2018. The majority of public authorities declared no recorded use of these powers with respect to young people between these dates. The returns showed that only 17 juvenile CHIS authorisations had been approved across 11 public authorities during the entirety of this four-year period; of these, one was 15 years old at the time of authorisation while the others were 16 or 17 years of age.
- 2.30 These results supported the evidence from inspections and other sources that these authorisations are only ever granted in exceptional circumstances. It would be inappropriate to provide further detail about the deployment of particular individuals in this context or to discuss the types of criminality about which they had been asked to report; to do so, with such small numbers, heightens the risk of particular juveniles falling under suspicion or revealing tactics which should not be disclosed. However, there are a few important points which can properly be noted:

7 Metropolitan Police Service Counter Terrorism Command (SO15)

8 Under RIPA(S)A the authorisation period remains one month for juveniles

9 [https://www.ipco.org.uk/docs/IPCO's%20letter%20to%20Harriet%20Harman%20MP%20\(24-08-18\).PDF](https://www.ipco.org.uk/docs/IPCO's%20letter%20to%20Harriet%20Harman%20MP%20(24-08-18).PDF)

- We consider in detail the authorisations for all juvenile CHIS on inspections. This involves an examination of the authorisation, review, renewal and cancellation paperwork, as well as risk assessments. We also usually meet the officer responsible for authorisation and the day-to-day management of a juvenile as a CHIS and will closely review the documentation which records the rationale for their continued use and conduct;
- On the basis of these detailed reviews, the IPC is satisfied that those who grant such authorisations do so only after very careful consideration of the inherent risks. Concerns around the safeguarding of children and the public authority's duty of care to the child are key considerations in the authorisation process;
- On many occasions Authorising Officers (AOs) refuse to sanction the use of a juvenile. The very small number of juveniles who have been authorised as CHIS during the last four years, often for limited periods, are in most cases on the cusp of adulthood. Public authorities are reticent to authorise juveniles unless the criminality and risk of harm to individuals and communities are of a high order and cannot be resolved in less intrusive ways; and
- As the IPC explained in his letter to the Joint Committee,¹⁰ juveniles considered as potential CHIS are already engaged in criminality, often at great personal risk. Juvenile CHIS are not tasked to participate in criminality they are not already involved in. Becoming a CHIS can, potentially, offer a way to extricate themselves from such harm; the IPC noted that decisions to authorise were only made where this is the best option for breaking the cycle of crime and danger for the individual.

2.31 We will keep the use of this particularly sensitive tactic under close review on our regular inspections of the relevant public authorities and we will provide annual updates on the number of authorisations, as well as any specific issues of note, through future Annual Reports.

Additional targeted interception and targeted examination provisions (section 17(2) of the IPA)

2.32 The IPA introduces provisions for several categories of authorisations, formalising the permissions and safeguards for what might be considered to be atypical applications. These include operations where the target set may not be well defined, or where there is a higher-than-usual expectation of intrusion into privacy, including potentially that of the public. These are often referred to as thematic warrants. This is an area which was extensively debated in Parliament during the passing of the Act; this has therefore been an important feature of our oversight and will continue to be so.

Section 17(2) of the IPA provides additional permissions to apply for targeted interception warrants or targeted examination warrants. These may relate to:

- (a) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
- (b) more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation; or
- (c) testing or training activities.

¹⁰ <https://www.ipco.org.uk/docs/Juvenile%20CHIS%20March%208%202019.pdf>

- 2.33 Examples of how these powers might be used are given in the Code of Practice (CoP). By example, this might include a criminal gang or suspected terrorist cell where the identity, and perhaps number, of individuals is unknown but they are assessed to have a common purpose which the relevant agency is investigating. The ability to apply to conduct intrusive actions against a number of unidentified individuals has been of great interest to our Judicial Commissioners (JCs), who have introduced a rigorous review process focusing their approval considerations on whether the bounds of the application are well defined and the scope of the operation is appropriately foreseeable. Because of the sensitivity of the operations covered by this kind of warrant, we are unable to provide statistics or specific examples of use. However, from our inspections and oversight to date, we have seen that the use of the provisions under section 17(2) are, in the majority of cases, used to authorise interception of communications to a small group of targets, as would be expected from these examples.
- 2.34 The legislation does not specify an upper limit for the scale of these authorisations. There are scenarios where it might be appropriate for an authority to seek the authorisation to intercept communications to a larger number of individuals in relation to a specific operational objective. This is only permissible where this is necessary and proportionate; our JCs need to be satisfied that the operational objectives cannot be achieved by other, less intrusive, means. We have been pleased to note that oversight via inspection and the double lock has confirmed that all intercepting agencies apply these safeguards appropriately and, in all cases reviewed, the requirement to use the relevant tactic is clear.
- 2.35 Management of any section 17(2) authorisations relies on a robust modification process. The IPA introduces major and minor modifications for interception warrantry, building on that which was in place under RIPA.
- 2.36 Major modifications are authorised by a Senior Official in the relevant Warrant Granting Department¹¹ whilst minor modifications can be authorised by a senior person within the intercepting agency. A major modification can be used for the name of an individual, premises or organisation to be added to a warrant or amended. Minor modifications can be used to remove them, or to add a factor. These provisions mean that if a new target is identified, and can be named or described, then a Senior Official at the warrant granting department may authorise interception of communications factors related to that individual. The Senior Official will consider the necessity and proportionality case for intercepting communications relating to the new target in the context of the warranted operation. If, however, a new communications factor is identified for an individual already listed on the warrant's permissions or under group descriptions, then a senior person within that agency can authorise its interception.
- 2.37 Major modifications should then be notified to a JC.
- 2.38 Additionally, urgent provisions allow for major modifications to be made within the intercepting agency and to be retrospectively approved by the warrant granting department.

11 Warrants under the Investigatory Powers Act 2016, Regulation of Investigatory Powers Act 2000 and the Intelligence Services Act may be issued by a Secretary of State. In practice, most warrants are granted by the Home Secretary, Foreign Secretary, Defence Secretary, Secretary of State for Northern Ireland, the Cabinet Secretary for Justice in Scotland. The departments working under these Secretaries of State are referred to as the Warrant Granting Departments.

Where a thematic warrant is in place:

Scenario A: Minor modification – An individual is named on the warrant and his mobile telephone is subject to interception. The agency identifies a second mobile number used by this individual. A Senior Official within that agency may consider whether it is necessary and proportionate to additionally intercept that number.

Scenario B: Minor modification – The agency has been intercepting both telephones but they are not producing valuable intelligence. The agency judges that it is not proportionate to continue this interception and ceases intercepting both telephones. A Senior Official may approve removing those telephone numbers from the warrant.

Scenario C: Major modification – A criminal associate of the named individual above is identified. He is not named on the warrant but is involved in the same activity. The intercepting agency assesses that it is necessary and proportionate to intercept his telephone. A Senior Official at the Warrant Granting Department will consider whether it is necessary and proportionate to intercept the telephone under the thematic authorisation.

Scenario D: New application – A criminal associate of the named and unnamed individual is identified. Intelligence indicates that he is involved in different criminal activity, which is not within the scope and objectives of the thematic warrant. The Secretary of State and a Judicial Commissioner will consider whether it is necessary and proportionate to intercept his telephone in the context of a specific threat case and details of the planned operation.

Changes to the acquisition of Communications Data (CD)

- 2.39 The IPA made substantial changes to the acquisition of CD, including by overhauling the application process for this widely used tactic. Under an amendment to the IPA, from early 2019 non-urgent authorisations¹² for CD will be independently reviewed by the Office for Communications Data Authorisations (OCDA). OCDA, which is headed by the IPC but is separate from IPCO, carries out the important function of safeguarding an individual's right to privacy under the Human Rights Act 1998 (HRA). The authorising officers will make independent decisions on whether to grant or refuse CD requests, ensuring that all requests to obtain CD by UK authorities are lawful, necessary and proportionate.
- 2.40 From 5 February 2019, local authorities may seek to acquire 'events data', including itemised billing and cell site location for the purposes of investigations. This power was not previously available to local authorities and marks a change in how they will be able to progress independent investigations. It is important to note that, where such 'events data' is sought for the prevention and detection of crime, local authorities, as well as law enforcement, will need to demonstrate that the investigation meets the defined threshold of serious crime.¹³ This means that the offence must be one:
- for which a person who has reached the age of 18 (21 in Scotland or Northern Ireland) is at risk of being sentenced to a term of 12 months or more;
 - which was committed by a corporate body;
 - which involved violence or resulted in substantial financial gain or was committed by many persons in pursuit of a common purpose;

¹² With the exception of applications for the purposes of national security.

¹³ The definition of 'serious crime' is set out at s.263(1) of the IPA, as amended by s.86(2A).

- which involved, as an integral part of it, the sending of a communication; or
- which involved, as an integral part of it, a breach of a person's privacy.

2.41 We anticipate that this new capability will lead to a rise in the number of applications in 2019. We will monitor this change closely, to ensure that the process is legally compliant. We have monitored applications passing through OCDA particularly carefully in the initial stages of transition and will report on this in more detail in the 2019 report.

Big Brother Watch judgment

2.42 On 13 September 2018, the European Court of Human Rights (ECHR) handed down its judgment in *Big Brother Watch v UK* (BBW judgment).¹⁴ The case related to three aspects of the UK's investigatory powers regime under RIPA 2000:

- bulk interception;
- intelligence sharing; and
- the targeted acquisition of communications data.

2.43 The Court heard arguments that activity in these areas interfered with the Applicants' rights under Articles 8, 10 and 14 of the ECHR and challenged, under Article 6, the comparability of the procedure before the Investigatory Powers Tribunal (IPT).

2.44 By a majority, the First Section of the Court accepted the utility and importance of bulk interception powers, stating '*the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within a State's margin of appreciation*'. However, there were two areas where the Court determined that the regime was not compliant with Article 8:

- The court decided that the bulk interception of 'external communications' breached Article 8 in light of 'the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications'. The IPA has already introduced heightened safeguards, including the introduction of operational purposes which limit the purposes for which bulk data may be examined, and oversight requirements, but HMG has committed to working with IPCO to establish how oversight of selectors could be enhanced; and
- The Court did not accept that the interception and use of CD that is derived from bulk interception ('related communications data' in RIPA terms; 'secondary data' in IPA terms) constituted a lesser intrusion into Article 8 than examination of content and should therefore not be exempt from the safeguards that apply to content under RIPA. In particular, the Court determined that similar safeguards should apply to the examination of related CD as applied to the examination of content where an individual is known to be in the British Islands (under RIPA 2000, the examination of such content may only take place where it is certified as necessary by the Secretary of State). The developments in technology and the way in which communications data can be utilised by UKIC¹⁵ to investigate an individual means it can be highly intrusive.

¹⁴ https://www.echr.coe.int/Documents/Press_Q_A_Brother_Watch_ENG.pdf

¹⁵ The term UKIC is used to refer to the UK's intelligence agencies MI5, SIS and GCHQ and may also refer to Defence Intelligence. In most instances throughout this report, UKIC will be used to refer to the intelligence agencies, noting that not all powers available to the agencies are applicable to Defence Intelligence.

- 2.45 The Court did not find a violation of the ECHR in relation to the application and operation of the UK's intelligence sharing regime.
- 2.46 Following the judgment, in October 2018 we received a number of bulk interception warrants and bulk equipment interference warrants for consideration from GCHQ. In light of the issues raised by the Big Brother Watch (BBW) judgment, the IPC and his deputy met HMG on several occasions prior to consideration of the warrants. Their reasons on approving the warrants required HMG to take steps to address the Court's judgment by the date on which it would become final.
- 2.47 We continued to hold meetings with HMG in order to understand the position being taken in response to the judgment. A letter signed by both the Foreign Secretary and Home Secretary was received by the IPC prior to the judgment becoming final on 13 December 2018. This outlined HMG's planned response to the issues raised by the judgment. In particular, HMG proposed that where an intelligence service intended to select for examination secondary data in relation to an individual known to be in the British Islands, it would be beneficial for the examination to be certified as necessary and proportionate by the Secretary of State. This was proposed to be achieved on a thematic basis given the high number of requests that would otherwise be made and the process will be subject to inspection at GCHQ in 2019.

Assistance to the Investigatory Powers Tribunal (IPT)

- 2.48 IPCO has a statutory obligation to assist the IPT and does so on a regular basis. During 2018 we assisted the IPT in a number of matters, only a limited amount of which can be made public. One key case that was resolved in 2018 was *Privacy International and (1) Secretary Of State For Foreign And Commonwealth Affairs (2) Secretary Of State For The Home Department (3) Government Communications Headquarters (4) Security Service (5) Secret Intelligence Service* IPT/15/110/Ch.
- 2.49 This case primarily concerned the lawfulness of the acquisition, use and sharing of Bulk Communications Data (BCD) and Bulk Personal Data (BPD) under the previous statutory regimes and, to a lesser extent, the overall effectiveness of the oversight in those areas. This case spanned a number of years with a significant judgment being given in July 2018.
- 2.50 We supported the Tribunal by answering numerous questions and performing searches against the databases held by our predecessor organisations, primarily the Office of the Intelligence Services Commissioner (ISComm).
- 2.51 The Tribunal, in July, dealing with the matters outstanding from its judgments of 17 October 2016 ([2017] 3 AER 647) and 11 September 2017 ([2018] 2 AER 166) relating to BCD and BPD concluded unanimously (save in relation to one issue, set out below):
1. that in relation to many directions made prior to October 2016 by the Foreign Secretary to Communications Service Providers to provide BCD to GCHQ, they were not in accordance with law;
 2. (by a majority) that the regime in respect of sharing of BCD and BPD with foreign agencies complies with Article 8 of the ECHR;
 3. that the regime in respect of sharing BCD and BPD with industry partners complies with Article 8 ECHR; and

4. that the steps taken by way of collection, retention and use of BCD or BPD by the Respondents comply with the requirements of proportionality pursuant to Article 8 ECHR and EU law.

2.52 The Tribunal further unanimously dismissed an application by the Claimant to set aside its conclusions in its judgment of 17 October 2016. The full judgment of the Tribunal can be found on their website.¹⁶ While this judgment deals with the previous legislative regimes, it is significant because the powers to obtain bulk data have been incorporated into the IPA 2016.

¹⁶ <http://www.ipt-uk.com/judgments>

3. Protecting confidential or privileged information

Overview

3.1 The Investigatory Powers Act 2016 (IPA) provides enhanced protection for certain forms of confidential or privileged information and the Investigatory Powers Commissioner's Office (IPCO) has a statutory role in authorising and overseeing the acquisition and retention of such material. The Act and Code of Practice (CoP) introduce specific safeguards for privileged material.

Legal professional privilege (LPP)

3.2 These safeguards reflect the fundamental right of individuals and organisations to seek legal advice and to conduct litigation in a confidential manner without fear that those communications will be targeted, save in certain defined circumstances.

3.3 For example, a warrant to intercept communications will only be granted in exceptional and compelling circumstances if the purpose, or one of the purposes, is to acquire or select for examination items subject to LPP. This measure protects individuals and companies seeking legal advice and ensures that a higher level of protection is established for members of the legal profession. Additionally, authorities must inform IPCO if they think it is necessary to retain LPP material; this decision is subject to approval by a Judicial Commissioner (JC).

3.4 The amended CoP for both Covert Surveillance and Property Interference and Covert Human Intelligence Sources (CHIS), published August 2018, contain enhanced regimes for the reporting of the inadvertent acquisition of LPP material as well as a more formal role for the Investigatory Powers Commissioner (IPC) in determining whether public authorities can retain such material. Although this relates to the Regulations of Investigatory Powers Act 2000 (RIPA), the new Codes mirror the enhanced protections within the IPA 2016. We anticipate that our 2019 Annual Report will reflect a significant increase in LPP issues that have been brought to our attention by public authorities.

3.5 IPCO also provides advice when an authority is uncertain whether an item is legally privileged. In these circumstances, the material is considered in order to determine whether the public interest in retaining it outweighs the public interest in the confidentiality of the item.

LPP oversight issues

3.6 Overall, compliance with LPP safeguards during 2018 was good. Only one public authority notified us of an instance when LPP material had been acquired under the IPA in circumstances not anticipated at point of application. In that case, the relevant authority ensured that the material acquired was handled in accordance with the CoP and that the confidentiality of the material was protected prior to it being assessed by IPCO. We have noted that public authorities are usually cautious, sometimes extremely so, regarding the potential acquisition of LPP.

Authorities need to have a good understanding of the relevant provisions to ensure that they are able to properly obtain LPP material in the restricted circumstances provided by the law.

Retention of items subject to legal professional privilege

- 3.7 A total of 77 applications were made to IPCO in relation to the retention of LPP material. Of those, 76 were approved.

Confidential journalistic material and sources of journalistic information

- 3.8 The IPA also includes safeguards for confidential journalistic material and sources of journalistic information. Applications under the IPA will state whether it is the purpose of the application to obtain confidential journalistic material or to identify sources of journalistic material and whether it is likely that such material will be obtained. In all cases, we would expect the application to consider the necessity and proportionality of obtaining the anticipated intelligence in the context of the European Convention of Human Rights (ECHR) Article 10, which protects freedom of speech.
- 3.9 In addition, the CoP set out additional protections for sensitive professions, including journalists (for example paras 8.8-8.44 of the Communications Data CoP). We examine the handling arrangements in place at each organisation to ensure that these safeguards are met. Again, given the small numbers involved, we were able to examine a high proportion of casework in relation to confidential material.
- 3.10 Our inspections confirmed that the safeguards in place at each authority in relation to journalistic material were adequate and that any access to this confidential material was properly considered and authorised. In 2018, six applications were made for warrants under the IPA where the purpose was to obtain material which the intercepting agency believed would relate to journalistic confidential material. In all cases, the JCs were satisfied that the case for obtaining confidential material met the relevant threshold under the IPA.
- 3.11 In December 2018, Professor Tim Crook contacted us to request additional information relating to the use of investigatory powers to obtain data relating to journalists. Whilst we were able to provide some of the information that Professor Crook requested, it was not possible to provide the information in full as this would have been prejudicial to national security and the ongoing functions of the public bodies overseen by IPCO.
- 3.12 As shown at Annex D, 203 communications data requests were made in relation to an individual of journalistic profession. On the basis of our inspections, we are satisfied that in the majority of these cases, the application related to the protection of a witness or victim, for example in the case of harassment of an individual who falls into one of these professions. However, we recognise that the statistics we produce in this area could be clearer and we will, therefore, work with the relevant public authorities on improving these for future reports.

Additional safeguards for health records

- 3.13 The intelligence agencies may apply for a specific Bulk Personal Data (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 in 2018.

4. Engagement

Overview

- 4.1 It is an important priority for the Investigatory Powers Commissioner's Office (IPCO) to engage with relevant external bodies and individuals. Full details of the Investigatory Power Commissioner's (IPC's) external engagements are given at Annex E. During 2018, we met Non-Governmental Organisations (NGOs), academics, the Investigatory Powers Tribunal (IPT) and overseas oversight bodies, along with representatives of the bodies over whom we have oversight. Discussions were held on a wide range of topics from the Consolidated Guidance through to the approach the Judicial Commissioners (JCs) should take when reviewing warrant applications. The IPC's ambition is that this engagement should happen on a more regular and structured basis than the present ad hoc and partial arrangements but, nonetheless, to date this has provided invaluable assistance to IPCO.
- 4.2 We aim to strengthen oversight internationally by developing collective understanding of how oversight is undertaken by each nation. There are undoubted impediments to international cooperation by oversight bodies, as the sensitivity of the work of national security agencies will frequently mean it is necessary to protect the details of intelligence operations and capabilities. This creates an obstacle to the open dialogue that would otherwise accompany unrestricted collaboration. Additionally, domestic legislation and other obligations and restrictions within each country may impose restraints on joint activity. That said, there is a strong mutual belief in, and a desire to achieve, international cooperation to the extent that it is legitimately achievable in the context of the oversight of investigatory powers.

UK engagement

- 4.3 By way of example of our approach in this area, IPCO participated in a project with the Human Rights, Big Data and Technology Project at the University of Essex, contributing to discussions concerning the authorisation process and how oversight of digital-surveillance practices should best be conducted. We were pleased to take part in a series of workshops on specific topics concerning surveillance techniques.
- 4.4 These workshops enhanced IPCO's understanding of some of the public concerns about intrusive powers, including bulk collection of communications data (CD) and the sharing of intelligence with overseas agencies. There were also wide-ranging discussions on the issue of accountability.
- 4.5 Chapters 2 and 10 detail our engagement with a range of interested parties in relation to the review of the Consolidated Guidance and our ambition to improve the clarity of information published on how the Guidance is used by Her Majesty's Government (HMG). IPCO completed a formal consultation process to receive the views of civil society and others with an interest in this area, such as NGOs, academics, other Government departments and the intelligence services. Specifically, we have spoken on several

occasions to members of Reprieve, an international organisation working to eliminate human rights abuses. Reprieve's challenge to transparency in relation to the application of the Guidance has helped inform thinking on how best to address public concerns in this sensitive area and shows the value of this kind of engagement to our work.

International engagement

Five Eyes

- 4.6 We have continued to develop productive relationships with other key oversight bodies in Europe and with the Five Eyes group (the US, Canada, Australia and New Zealand). We participated in the Five Eyes Intelligence Oversight and Review Council (FIORC) conference, which was held in Australia and hosted by the Office of the Inspector-General of Intelligence and Security. Sir Kenneth Parker represented IPCO at the 2018 event, along with a member of the Technology Advisory Panel (TAP)¹⁷ and the IPCO legal adviser. FIORC is a forum within which the oversight bodies exchange views, compare best practices for oversight and explore where cooperation on reviews and the sharing of results is appropriate. For example, sharing material across borders is an issue of growing significance; there is an emerging common objective to ensure this is lawful and the subject of effective oversight.

UN Human Rights Council's International Intelligence Oversight Forum

- 4.7 IPCO has contributed to the work of the UN's Special Rapporteur on the Right to Privacy, Professor Joe Cannataci, since 2016.¹⁸ Judicial Commissioner, Sir Nicholas Blake and an Inspector attended the UN Human Rights Council's International Intelligence Oversight Forum hosted by Professor Cannataci in Malta in October 2018. Sir Nicholas spoke on the double lock process and the need to ensure that judicial independence is not undermined by the need to be briefed from time to time by the authorities we oversee. He emphasised the strengths of IPCO's dual role in warranting and retrospective inspection.

Europe

- 4.8 In April 2018, the IPC visited Berlin and attended a series of meetings organised by diplomats from the German Embassy in London. The IPC met members of the Federal German Parliamentary 'G-10' Control Commission who undertake a similar role to our JCs; the Permanent Under Secretary of State for Intelligence at the Federal Chancellery;¹⁹ and the Vice-President of the German foreign intelligence service (the Bundesnachrichtendienst).
- 4.9 We also held meetings with the Stiftung Neue Verantwortung (SNV), an independent think tank that develops ideas as to how to bring about technological change in society, the economy and the state. We have, in particular, worked with Thorsten Wetzling, who heads the SNV's research on surveillance and democratic governance. He recently published *Upping the Ante on Bulk Surveillance – An International Compendium of Good Legal Safeguards and Oversight Innovations*.¹⁹ Wetzling has suggested the UK is an example of a country that has implemented best practice, both because of the openness of our oversight regime and the important dialogue with civil society on establishing proportionate standards for the review of bulk powers.

¹⁷ Details on the Technical Advisory Panel (TAP) are given in their report in Chapter 17.

¹⁸ https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_HRC_40_63.DOCX

¹⁹ https://www.stiftung-nv.de/sites/default/files/upping_the_ante_on_bulk_surveillance_v2.pdf

- 4.10 We welcomed the *Joint Statement: Strengthening Intelligence Oversight Cooperation* by the oversight agencies of Belgium, Denmark, the Netherlands, Norway and Switzerland, which was published on 14 November 2018.²⁰ In establishing a closer working relationship between those countries, the statement also addressed the potential of an oversight gap, in the context of overseeing international data exchange by the intelligence and security services, and outlined potential ways to tackle this risk. We anticipate that this more collaborative approach to oversight will help in a number of areas, not least by developing a collective approach to human rights standards and the safeguards that should apply to the exchange of personal information between intelligence services and law enforcement agencies.
- 4.11 A meeting of a larger group of European oversight bodies was hosted in Paris by the Presidents of the French Commission Nationale de Contrôles des Techniques de Renseignement (CNCTR) and the Belgian Comité Permanent de Contrôle des Services de Renseignement et de Sécurité (CPR) in December 2018. This was an introductory meeting between many of the European oversight bodies who will be gathering again in The Hague in December 2019.

20 <https://ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx>

5. Inspection methodology

Overview

- 5.1 The establishment of the Investigatory Powers Commissioner's Office (IPCO) provided an opportunity to review our approach to inspections across the range of powers we oversee. We were able to test some new approaches during 2018, with a view to making better use of the expertise of our Inspectors and helping them develop their experience into new areas. Our current conclusion from this experience is that one size of inspection does not fit all, even within categories of institution. We need to be flexible in our approach to inspection planning to ensure that the demands our visits make on public authorities are proportionate but allow us the access we need. We are keen to build on this learning and will continue to work with the authorities we oversee to develop our methodology as the impact of the new legislation becomes clearer.
- 5.2 This chapter sets out our current inspection methodology and the reasons behind that approach. This helps to explain some of the differences in how our findings are presented, as it will always be the case, for example, that we focus on the work of the intelligence services more than other organisations. The chapters that then follow, which give further detail of our inspection findings from 2018, reflect the balance of time we commit across the range of authorities we oversee.

Selection of material for inspection

- 5.3 With the exception of some smaller establishments which rarely use their powers, Inspectors do not attempt to view all the authorisations in any particular area. IPCO does not aim to review a fixed statistically representative sample because each inspection should be a process of gaining insight into the methodologies used by, and the activities of, the individual authorities. On some occasions, the authorisation casework might be marginal to an inspection that focuses on, for example, protective monitoring methodologies or the adequacy of staff training.
- 5.4 It is important to note that it is the Chief Inspector or Inspector who selects the material to be viewed on any inspection, rather than the authority we are inspecting. The selection may reflect issues raised by the Investigatory Powers Commissioner (IPC) or the Judicial Commissioners (JCs) in the course of considering applications, may pick up trends or issues in error reporting or will follow up on recommendations from previous inspections to ensure they have been addressed.

Inspection reports

- 5.5 A report is issued after each inspection. These set out our conclusions and recommendations and identify any areas of vulnerability or non-compliance. The report is sent to the head of the agency or authority and, if appropriate, is copied to the relevant Department of State.
- 5.6 We use three categories of recommendation:

| Colour | Recommendation |
|--------|--|
| Red | Signifies a critical issue where immediate action must be taken |
| Amber | Relates to an issue where a process may need to be reviewed |
| Green | Denotes general recommendation where we believe improvements could be made at an early stage to prevent any issue of non-compliance arising in the future or point to areas where operational efficiencies could be made or additional information is required to make an assessment |

We also identify areas of good practice which may be of interest to other similar organisations. We also make observations or identify areas of good practice which may be of interest to other similar organisations.

- 5.7 We are working to standardise our reports across the different powers we oversee. In 2018, reports differed substantially in terms of style and content, which reflected the range and complexity of the areas covered by our inspections and the different approaches taken by our predecessor organisations. Our intention is to issue reports which enable organisations to take action on the basis of our recommendations but, in addition, we aspire to enable them to identify where improvements and efficiencies could eliminate wider compliance vulnerabilities. This will continue to be a focus of our work for 2019.
- 5.8 Our reports are drafted for use by the relevant agency and typically contain operational detail which cannot be disclosed because of the statutory secrecy provisions contained in the Regulations of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA). The reports may, for example, include a summary of briefings given during an inspection or details of a new technique or a specific operation of interest. We hope, however, that through the carefully chosen examples in this and other reports, we can explain the work of IPCO without breaching those provisions.

A changing approach to inspections

- 5.9 In 2018, we considered whether bringing together Communications Data (CD) inspections (formerly conducted by the Interception of Communications Commissioner's Office) and surveillance inspections (formerly carried out by the Office of the Surveillance Commissioner) would establish a more robust oversight model than hitherto, providing greater insight into the work of each public authority. For some bodies, where these powers are not used together or by the same department or team, carrying out joint inspections would bring no obvious benefit and could be burdensome. However, put generally, our initial experience shows that carrying out a single inspection, covering IPA and RIPA powers used by Law Enforcement Agencies (LEAs), offers benefits for both IPCO and the inspected authority. We have also found that best practice recommendations can have greater impact if they are considered across the piece, rather than by one operational

team. Our combined reports to a Chief Constable give a sense of the health of the whole organisation and action can then be taken by the authority as a whole.

- 5.10 Another significant development has been for Judicial Commissioners (JCs) to join inspections. This has a dual benefit: first, it enhances the JCs' awareness of the context of operations, which is frequently relevant to their consideration of applications; and, secondly, it gives the JCs an opportunity to challenge aspects of policy and methodology at individual authorities. We have continued this practice through 2019.

Oversight of the UK Intelligence Community (UKIC)

- 5.11 The creation of IPCO enabled a wholesale reconsideration of the oversight model for the UK's Intelligence Community (UKIC). Our objectives have been to establish more challenging and comprehensive oversight than previous Commissioners were able to achieve with the limited resources available to them. We now encourage the agencies to demonstrate their methodology and rationale for the work they undertake to our Inspectors, who are then able to investigate in detail and understand how internal oversight works. This model has broadened the scope of IPCO's inspections to cover matters of policy and practice relevant to the application of covert powers. Through frequent inspections, briefings and audits we speak to more staff at the agencies than had previously been possible. It is worth noting that this would have been impossible without the support, and resources, provided by the agencies in response to this change. The level of assistance with which we have been provided has been, without exception, exemplary.
- 5.12 In real terms, this means we meet members of each agency, in one guise or another, on a monthly, and at times weekly, basis. We are still exploring ways of working with UKIC to maximise our oversight without unnecessarily impeding operations. In some instances, we conduct inspections in which several powers are considered together: for example, inspecting property interference and surveillance jointly provides a valuable opportunity to scrutinise how different covert powers are used on operations. This has enabled IPCO to consider whether the relevant powers are used rationally, in a way that is proportionate, to validate operational requirements. In other instances, for example with the Consolidated Guidance, we have inspected the three intelligence agencies at the same time. This has afforded real insight as to how the agencies work together in order to minimise risks and has resulted in a high level of confidence in their collaborative approach. This approach has enabled IPCO to identify and resolve previously undetected issues, such as different approaches taken by different agencies to caveats on intelligence sharing with foreign services.
- 5.13 The balancing act for IPCO is, therefore, to design an inspection programme which allows sufficient scope to follow the threads of our investigations across UKIC without losing the detail and focus of bespoke, single-agency inspections.

Oversight of bulk powers

- 5.14 An important area of our oversight of UKIC is the use of bulk powers. Although the IPA introduces specific powers to conduct bulk operations, the capability to do so is not new. These powers continue to be controversial because of public fears about indiscriminate collection and, as a consequence, oversight of the implementation of the relevant safeguards and the way in which material is collected and selected for examination is a priority for our Inspectors. We are confident that the majority of the data gathered by way of bulk collection is not reviewed by analysts, although it will be automatically screened

against specific criteria to enable the agencies to extract intelligence relevant to clearly identified operational purposes. The IPA introduces new requirements for recording justifications for accessing material, which have also become a focus of our inspections. The safeguards referred to above include the physical infrastructure and technology that houses bulk material and we will ensure that access to this data is strictly limited to those with a legitimate operational role, who are appropriately vetted and trained. IPCO considers these restrictions, along with intensive oversight of them, to be fundamental to preventing abuse of these significant powers.

- 5.15 In 2018, UKIC inspections were overseen by Sir John Goldring and Lord Bony. In addition, the IPC and Sir John were briefed on a variety of key issues during the course of the year; they were supported in this work by a Chief Inspector and his team of eight Inspectors, three of whom are solely involved with UKIC inspections. During the first half of 2018, a team of two or three Inspectors and a JC, in most instances, conducted the inspections of each of the relevant covert powers at each agency and where possible, they aimed to undertake a second inspection of those powers in the second half of the year.
- 5.16 Before an inspection, the agency is asked to provide a list of all the relevant authorisations and casework, including internal approval documents. By way of example they will be required to provide details of the instances when the Consolidated Guidance was applied. The agency provides sufficient initial detail to enable the inspection team to select material for further scrutiny. For example, again with the Consolidated Guidance, the agency will routinely identify whether a submission or application had been sent to the Secretary of State, along with any liaison partner which was involved.²¹ In the case of the Intelligence Services Act (ISA) section 5 authorisations (property warrants), the selection document might include details of the type of property or type of interference. This allows us to, broadly, select a cross-section of authorisations or to focus on a specific area of interest, such as vehicle tracking.
- 5.17 Using a larger team of Inspectors to oversee UKIC has given IPCO the flexibility to deploy experts on the use of particular covert powers. For example, surveillance Inspectors have joined the team to scrutinise UKIC's use of directed surveillance powers. This has provided greater confidence that UKIC, law enforcement and the public authorities are being tested to the same standard. We are confident that all the authorities overseen by IPCO will start to benefit from this more flexible and coherent approach to oversight over the coming years.

Law Enforcement Agencies

- 5.18 Two Chief Inspectors head up an inspectorate of seven communications data (CD) experts and eight RIPA and Police Act experts, who are responsible for conducting all law enforcement, public and local authority inspections.

Covert Human Intelligence Sources (CHIS) and Surveillance

- 5.19 Our annual covert human intelligence sources (CHIS) and surveillance inspections generally last between three and five days, depending on the size of the agency being inspected. We use on-site inspections to examine the internal records for any relevant activity conducted under RIPA. For instance, the use of covert human intelligence sources (CHIS) enables LEAs to frustrate offenders and prevent or detect crime; oversight includes considering how CHIS

²¹ The term 'liaison partner' refers to any overseas government body with whom UK bodies collaborate or share intelligence, such as local or national police, foreign government departments and foreign intelligence agencies.

are recruited, and the way in which tasking and well-being considerations are managed. We scrutinise contact notes and the assessments of the necessity and proportionality of the use of CHIS, to ensure that authorities are properly using CHIS in accordance with the specified intelligence requirements. We focus on (i) how expeditiously the CHIS is formally authorised after the initial approach, to avoid 'status drift' (for instance, there is a need to guard against an unauthorised source giving intelligence to a LEA for a sustained period during their recruitment); (ii) whether contacts with the CHIS are fully documented; (iii) whether authorisations are properly considered and explained by the authorising officer (AO); (iv) if there is a regime for the proper handling and management of the CHIS; (v) whether risk assessments are dynamically maintained and updated; and (vi) if there is suitable security surrounding the management of the intelligence provided by the CHIS product and the individual's real identity.

- 5.20 We interview staff who manage CHIS (frequently within Dedicated Source Handling Units or similarly named teams). We also interview other frontline staff to discuss their dealings with members of the public to ensure that, inadvertently or otherwise, the latter are not acting in a capacity that requires a CHIS authorisation.
- 5.21 As explained in chapter 2, IPCO looks at all cases when juvenile CHIS are used, given their clear potential vulnerability. We inspect how law enforcement bodies use undercover officers, particularly as to how undercover officers are managed and the way in which their safety and welfare is overseen. Generally, we focus on the authority's duty of care to these individuals. A third area of interest is when CHIS participate in criminality, with the approval of an AO. This tactic is used very infrequently and, invariably, when a CHIS is involved in an offence that is already underway.
- 5.22 We also conduct inspections in advance of a renewal of authorisations of relevant sources (undercover police operatives), as set out in the enhanced oversight regime established by Statutory Instrument 2013/2788.²² In relation to surveillance, IPCO also receives briefings on new equipment and techniques and we review how officers and staff are trained. A range of individuals are interviewed, including operational staff and authorising officers. We challenge the rationale for operations undertaken, to ensure that the most proportionate techniques were used and, presently, we focus on the handling of intelligence, to ensure that all relevant material is appropriately safeguarded and destroyed when retention is no longer justified. Decisions in this context are complicated by the disclosure requirements of criminal proceedings, whereby law enforcement bodies may be required to retain copies of intelligence for longer than otherwise would be operationally necessary. We test whether staff properly understand the requirements of the law in this context and the records that track the use of the technical equipment used to carry out covert activity are carefully reviewed. It is worth noting that we particularly scrutinise authorisation records which have been approved via the double lock when a JC has given specific instructions or imposed restrictions.

Intercepting Agencies

- 5.23 We also inspect the nine intercepting agencies on an annual basis.²³ Inspections are conducted by two or three Inspectors, accompanied in some cases by a JC. This includes scrutiny of the Warrant-Granting Departments in the Home Office and Foreign and Commonwealth Office (FCO).

²² http://www.legislation.gov.uk/uksi/2013/2788/pdfs/uksi_20132788_en.pdf

²³ Intercepting Agencies: Government Communications Headquarters (GCHQ), Her Majesty's Revenue and Customs (HMRC), Metropolitan Police Service (MPS), Ministry of Defence (MOD), MI5, National Crime Agency (NCA), Secret Intelligence Service (SIS), Police Scotland, Police Service of Northern Ireland (PSNI)

- 5.24 In advance of an interception inspection, we ask the intercepting agency or WGD to provide a full list of the relevant authorisations. This will include contextual details to aid the process of selecting particular authorisations for scrutiny at inspection. Casework is reviewed, to establish whether the internal documentation adequately sets out the matters taken into consideration, including why the interception is deemed necessary and how intrusion into privacy will be managed and minimised. We interview individuals involved in the interception, including analysts and linguists.
- 5.25 A significant proportion of authorisations are reviewed where the application was originally approved under the urgent provisions, or when the requesting agency judged that there was likely to be confidential or privileged material. The policies and practices that are designed to safeguard sensitive material are considered with care.
- 5.26 More generally, throughout 2018, we worked with the interception agencies to ensure that their systems and processes were adequate to meet the requirements of the IPA. Where possible, query-based searches are conducted to test compliance and identify how the intercepted material is being used. We consider whether intrusion was appropriately handled and minimised and whether the interception was stopped at the appropriate point in the operation. We also look at whether the retention, storage and destruction arrangements are adequate.

Communications Data (CD)

- 5.27 Annual CD inspections range from three to five days in duration, depending on the size of the force or agency and the volume of CD that is acquired. For example, one Inspector might visit a small force to assess their compliance, whilst a larger metropolitan force or agency will require a team of Inspectors in order to target individual themes and disciplines.
- 5.28 Our CD inspections are designed to ensure public authorities are acquiring CD for the correct statutory purpose and in compliance with RIPA and the Codes of Practice (CoP). We scrutinise their records and, in particular, focus on the methodologies used to ensure any unrelated private information that has been unavoidably obtained is appropriately documented and handled.
- 5.29 Before an inspection, we require the authority to complete a schedule of information; this will include any relevant statistics and documentation and we then select the records for inspection. The key staff involved in the application, authorisation and acquisition of CD are interviewed. In some cases, we conduct a 'reverse audit' whereby a selection of data is obtained directly from a telecommunications operator and cross referenced to the relevant application in the force or agency. This is to ensure data has been acquired for the correct statutory purpose.
- 5.30 Certain key themes are pursued on every CD inspection:
- The operational independence of the senior officer who authorises the acquisition of CD (known as the Designated Person);
 - Any applications that relate to sensitive professions;
 - Data acquired in support of internal professional standards investigations;
 - Data acquired under an oral authorisation using the urgency provisions;

- The acquisition of data relating to Internet Protocol Addresses when, due to the format and nature of the data, the risk of an error occurring is higher than usual; and
- The recordable and reportable non-serious errors that have occurred during the reporting period, to identify any trends or learning that can be passed to other public authorities, and to ensure any action taken to avoid recurrence is sufficient.²⁴

Protected Information

- 5.31 During law enforcement inspections we also review any applications requiring the disclosure of protected information. The investigation of protected electronic information is carried out under Part 3 of RIPA. Any such applications are managed by the National Technical Assistance Centre (NTAC).

Other Public authorities

- 5.32 Depending upon the scale and levels of covert activity for each public authority, inspections are either annual (as in the case of the Department for Work and Pensions, and the Home Office's Immigration Enforcement), or once every two or three years.
- 5.33 At each inspection, we interview key officials on the use and management of covert tactics and examine any relevant policies. The provision of, and procedures for, training are similarly considered. We scrutinise a representative sample of authorisations and associated paperwork. The methodology for public authorities mirrors that described for local authorities, set out below.

Local authorities

- 5.34 Routinely, we simultaneously inspect an authority's use of both CHIS and surveillance powers under RIPA Part 2. We aim to inspect local councils across England, Wales and Scotland every three years. IPCO additionally inspects local authorities via the National Anti-Fraud Network (NAFN), which processes all CD requests for local authorities. In 2018, three Inspectors conducted a one-day inspection of NAFN.
- 5.35 A remote inspection involves sending a questionnaire for the authority to explain their compliance management processes and to provide details as to how they have used their powers since the last inspection. These results are analysed before a member of the authority is interviewed over the telephone. We seek an explanation for any ambiguities and test the authority's understanding of the relevant legislation and CoP. The authority is able to raise any issues and advice is given by the Inspector on best practice. The opportunity will be taken to inform the authority of successful ways of working adopted elsewhere. Remote inspections are used if the relevant authority is not using covert powers and there are no concerns about compliance. We will not do two remote inspections in a row and will always ensure that an on-site inspection takes place on the next occasion. We are particularly concerned to ensure that covert powers are not being inadvertently used outside of the oversight regime and that all authorities are fully prepared to utilise these investigatory powers in a lawful manner. In the rare event that we are dissatisfied with the results of a remote inspection, an on-site visit takes place shortly thereafter.

²⁴ See the Errors chapter for more information.

- 5.36 Although inspections by way of visits constitute the gold standard, we judge we have achieved an appropriate balance which ensures regular and thorough oversight of all UK local authorities.
- 5.37 For both types of inspection, authorities must demonstrate compliance with the relevant legislation, the CoP and their own internal policies, and we ensure the adequacy of staff training in all relevant areas.

Prisons

- 5.38 We conduct an annual inspection of Her Majesty's Prison and Probation Service (HMPPS), along with a selection of the 88 prisons across England, Wales and Northern Ireland. Prison inspections usually last one day and this process is overseen by one of our JCs, Dame Linda Dobbs. They are generally conducted by a single Inspector, at least biannually, but we are trying to improve that during 2019. The regularity of inspections is based on a prison's previous compliance record and its previous recommendations.
- 5.39 The prison inspection regime focuses on ensuring proper notification to all inmates that their communications are recorded and may be monitored, alongside appropriate mechanisms to conduct interception of authorised telephone calls and the monitoring of mail. The inspections take into account the Prison Service Instructions (PSIs) which are issued by HMPPS. Certain information is requested ahead of the inspection to help inform the intended course of the inspection and advice is given as to how to prepare. Each prison is asked to complete a statistical return, which includes disclosing any breaches which may then be investigated further if appropriate.

6. MI5

Overview

- 6.1 We conducted regular inspections at MI5 during 2018, across the range of investigatory powers they use, speaking to a variety of senior staff, legal and technical officers and, to a lesser extent, practitioners. Compared with previous years, we adjusted the proportion of warrant applications and internal authorisations (such as directed surveillance authorisations) that we reviewed, favouring more in-depth conversations with subject-matter experts and demonstrations of MI5's complex IT infrastructure. We believe this model of scrutiny establishes an enhanced understanding of MI5's operational work and of how covertly obtained data is used and retained.

Findings

- 6.2 In general, we concluded that MI5's use of investigatory powers available under the Investigatory Powers Act 2016 (IPA), Intelligence Services Act (ISA) and the Regulation of Investigatory Powers Act 2000 (RIPA) were compliant with the statutory provisions, the Codes of Practice (CoP) and internal policies that we have seen. Importantly, in 2018, we were not informed of serious compliance risks in relation to certain technology environments used by MI5 to store and analyse data. We judge that, by January 2018 (indeed, most probably considerably earlier), MI5 had a clear understanding of the principal compliance risks associated with these technology environments, to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in those systems. The risks were also sufficiently clear that they should have been communicated to the Investigatory Powers Commissioner (IPC), who was not briefed by MI5 on the issue until February 2019.
- 6.3 It is a matter of serious concern that MI5 did not bring these compliance issues to the attention of the Investigatory Powers Commissioner's Office (IPCO) attention at an earlier stage. Having been briefed, we immediately began working closely with MI5 to understand the level of risk, which was continuing, in relation to warranted data in particular and to scrutinise the measures implemented and planned to remedy the risks. Further detail of this is provided at paragraph 6.44-6.46 below. This also means that our findings in relation to MI5's use of specific investigatory powers, set out below, are based on the inspections conducted during 2018, prior to our being made aware of these significant problems.

Covert Human Intelligence Sources (CHIS)

- 6.4 MI5 authorise UK agent and undercover operations under RIPA. Some overseas operations do not require RIPA authorisation but are nevertheless subject to detailed operational assessments. The quality of the applications is generally high and the records of the agent handlers, controllers, authorising officers and legal and security advisors providing the explanation for the decisions taken in these complex cases is of a very high standard.

- 6.5 Nonetheless, there is clear room for improvement in the way that MI5 manage and record the CHIS review process. We recommended that the process of conducting a review of CHIS authorisations should itself be examined to determine if the current arrangements are compliant with the CoP. At our most recent inspection, MI5 outlined the work that they are doing to provide a remedy, part of which included issuing new guidance and updating their policy in this area.

CHIS Participation in Criminality (PIC)

- 6.6 MI5 has an internal policy governing participation in criminal activity (PIC) by its agents. IPCO has been directed by the Prime Minister to oversee MI5 compliance with this policy and we examine a high proportion of these cases to ensure that this activity meets a high necessity threshold.
- 6.7 Typically, we examine the PIC authorisations alongside the RIPA paperwork relating to the agent or undercover operative. In every case that we examined, we noted good articulation of the matters taken into consideration and we concluded that the activity authorised was proportionate to the anticipated operational benefits.
- 6.8 However, we are concerned that MI5 lack reliable central records around PIC activity and that there is no consistent review process. We recommended that MI5 should implement a system to capture accurately the extent of participation in criminality by CHIS across the organisation. This should record the number of PIC authorisations, the nature of the activity authorised and the number of times each authorisation has been relied upon.
- 6.9 This area of activity is relevant to an ongoing Investigatory Powers Tribunal (IPT) case (also known as The Third Direction case).

Surveillance and Property Interference

- 6.10 MI5 make considerable use of a wide variety of surveillance capabilities that are authorised internally under Directed Surveillance Authorisations (DSAs). We examined several authorisations during two inspections and were satisfied that each case we examined was necessary and proportionate. As with CHIS, however, we were concerned that MI5 did not have an adequate review process in place. MI5 explained that their review process for ongoing surveillance operations was informal, relying on conversations between the authorising officer, investigator and surveillance operators. The content of these discussions is often not documented. We noted that this falls short of the requirements in the CoP and therefore recommended that MI5 should establish an appropriate mechanism for conducting and recording reviews, including accurately recording formal review dates.
- 6.11 We were pleased that MI5 responded to this recommendation ahead of our second inspection in 2018. MI5 have overhauled their procedures and are developing a number of mitigations which will include changes to their electronic workflow process. We endorse this approach. We note that such changes, especially to IT systems, will take time to deliver but we are confident that progress is being made.
- 6.12 In 2017, we noted that MI5's DSAs covered a range of techniques but that, as the authorisations were renewed, there was often insufficient consideration of the ongoing necessity for including all of the previously-authorized techniques. We have seen a gradual improvement in this area but will continue to keep it under review.

- 6.13 In 2017, we also reported concern at the high number of errors at MI5 in relation to a specific category of directed surveillance actions. MI5's initial response did not reflect the need to ensure that end-to-end intelligence handling processes were appropriate. In response to these criticisms, MI5 looked at each stage of their intelligence-handling system for this technique and established a series of safeguards, both manual and automated, to prevent further breaches in this area.
- 6.14 Applications for directed surveillance and property warrants often made reference to the collection of biometric data. We asked MI5 to provide details on how this sensitive data is collected, retained and used. We sought to understand how this material was safeguarded and what value it gave to MI5's investigators, in particular working with police counterparts. We received a detailed briefing from MI5 about their collection and retention of biometric data. We discussed the retention of this material in detail and were satisfied that MI5's processes were appropriate and the retention of relevant data was proportionate. We were content that MI5 have a detailed policy in place to govern this activity.
- 6.15 We examined MI5's use of intrusive surveillance (surveillance which takes place in a private residence or private vehicle when there is a higher expectation of privacy). Intrusive surveillance is authorised via a warrant signed by a Secretary of State and is typically authorised in combination with a property warrant to authorise interference with property, for instance the concealment of a listening device in a home or private vehicle. We were satisfied with MI5's use of these powers and made no recommendations.

Targeted Interception (TI) and Equipment Interference (EI)

- 6.16 Overall, we were satisfied that MI5 had achieved a high level of compliance with the requirements of both RIPA and the IPA throughout the year in relation to targeted interception (TI) and had successfully transitioned its internal arrangements to the new IPA regime.
- 6.17 For equipment interference (EI), we inspected MI5's compliance with Section 5 of the ISA, to the extent that it applied in early 2018, and the new IPA regime following commencement of Part 5 of the Act. We concluded that MI5 has been fully compliant, including with the requirements of the new EI regime with respect to the authorisation of EI operations and the acquisition of data.
- 6.18 Following transition to the IPA, MI5 is making extensive use of combined warrants under schedule 8 of the Act. MI5 can apply for combined interception and equipment interference warrants under the IPA and we will therefore be inspecting MI5's use of targeted powers under the IPA in a single, combined inspection in 2019.
- 6.19 We were satisfied that MI5 is applying the IPA's safeguards for confidential material, including legally privileged material, carefully and accurately. However, we have recommended to MI5 that, when a warrant is renewed or cancelled, MI5 should summarise clearly whether confidential material was obtained during the period under review.
- 6.20 In the initial months after the introduction of the IPA, IPCO Inspectors have focussed on thematic warrants. Our inspections have found that the internal processes around managing modifications are robust and fit for purpose. Both major and minor modifications are being written to a good standard and our inspections have seen evidence of good processes to manage how communications factors are added and removed from the authorisation. However, this section of the Act was implemented in late 2018 and we will, therefore, provide a more extensive overview in our 2019 report.

- 6.21 MI5 did not apply for any warrant under section 17(2)(c) in relation to training or testing activities in 2018. We have discussed the use of these provisions with MI5 and expect that this provision will be relied upon more extensively in 2019. At present, MI5 conducts some activities under RIPA's directed surveillance provisions which may be appropriately authorised under the IPA. We will continue to engage with MI5's operational and legal experts in this area. It is worth noting that surveillance Inspectors from IPCO have examined the relevant authorisations and are satisfied that the relevant activities are being properly conducted, with consideration to any intrusion that may result.

Targeted equipment interference warrants section 101(1) and (2)

- 6.22 There was a gradual transition of extant warrants throughout the second half of the year after the EI element of the IPA came into force in June. Our inspections are retrospective and we need to set a cut-off date some time before the inspections. We therefore looked at relatively few IPA warrants in 2018. We conducted 'light touch' inspections during this period to accommodate for the transition.
- 6.23 Thematic warrants, as authorised under sections 101(1) (b)-(g) and (2) (b)-(e), can be broad in scope; they can cover a large group of people, a wide geographical area and lead to the acquisition of a large volume of data. Paragraph 5.13 of the CoP notes that a thematic warrant may be appropriate where the relevant statutory tests are met and where a series of individual warrants is not practicable, or where the proposed activity is more suitably dealt with by a thematic subject-matter in light of, for example, the operational circumstances.
- 6.24 The IPA also allows for the use of general descriptors on such warrants. Para 5.16 of the CoP notes:
- “that it may not always be reasonably practicable to include the names or descriptions of each and every one of the persons, organisations or locations. Accordingly, thematic warrants fall into two types, those where it is reasonably practicable to include additional details and those where it is not.”**
- 6.25 Paragraph 5.18 goes on to explain that:
- “the practicability of providing individual names or descriptions will need to be assessed on a case by case basis by the equipment interference authority making the application and will depend upon, for example, the existing intelligence picture, the scale and pace of the operation, the nature of the equipment to be interfered with and the time constraints of the particular operation.”**
- 6.26 During this period the Judicial Commissioners (JCs) have approved thematic warrants covering a number of circumstances, including those with general descriptors. One application was rejected by a JC in November 2018. The JC judged that the group of individuals described did not fall within the definition of 17(2)(a) and that the requested activity should be appropriately handled in reliance on 17(2)(b) using major modifications to approve the interception in relation to targets who were not fully identified at the point of application. A JC subsequently approved an application for this operation which included a more prescriptive description of the intended targets. At future inspections we will be giving particular attention to thematic warrants, especially where the authority is able to change the scope of intrusion without seeking external approval (Targeted Interception). We will also be testing whether the circumstances described when applying to use a general descriptor were valid.

Bulk communications data (BCD)

- 6.27 The last IPCO Annual Report described the processes by which MI5 and the Government Communications Headquarters (GCHQ) access bulk communications data (BCD), both of which include consideration of the principles of necessity and proportionality. The procedures and operational requirements within the agencies differ and mean it is not possible to provide comparable statistical information about access to, and use of, BCD.
- 6.28 There were some existing section 94 Directions in 2018 which related to MI5.²⁵ These directions have been replaced by bulk acquisition warrantry relating to UK telecommunication operators, which commenced in October 2018. Because this area is subject to the double lock, the focus of our inspections has therefore changed to scrutinising the acquisition, retention, use and disclosure of warranted data. We also examine the procedures in place to access and examine the data. We interviewed those in charge of intelligence operations, senior managers authorising access, analysts in operational teams and those who manage and carry out audits of the access.
- 6.29 During our inspections at MI5, we concluded that the submissions to the Secretary of State were highly detailed, explained clearly why the acquisition, retention, access to and analysis of BCD was required in the interests of national security, and set out the intelligence requirements they were seeking to address. The submissions included extensive detail as to how the BCD would address operational requirements, the expected value of the intelligence derived from it and why there was no viable alternative to the proposed acquisition of BCD.
- 6.30 The Home Secretary's direction required MI5 to carry out a review every six months and share findings with the Home Office. We scrutinised the review documentation at MI5; we were satisfied that the six-monthly reviews for all existing section 94 directions were comprehensive, containing a summary of the data that had been retained and how the BCD was to be handled, analysed and accessed. The reviews included the operational justification and legal basis for continued retention and use and set out the value to relevant operations. The reviews documented an assessment of the collateral intrusion that occurred as a result of MI5 having possession of, and access to, the BCD and set out consideration of the issues and consequences of alternative forms of acquisition and the potential contingencies involved.
- 6.31 Until 8 October 2018, the MI5 process for accessing BCD, acquired and retained by the agency as a consequence of section 94 directions, substantially mirrored that set out in Chapter 2 Part 1 RIPA and the CoP for the Acquisition and Disclosure of Communications Data. That process required the investigator or analyst to set out in an application why it was necessary and proportionate to access the data. A designated person of appropriate seniority in the organisation then considered whether to give authority for access to the data MI5 retained. Overall, we concluded that MI5's applications were of a high standard and satisfied the principles of necessity and proportionality.
- 6.32 This process changed substantially once bulk acquisition warrants were introduced in October. The applicant is now required to complete an application prior to submitting the search query, selecting the operational purpose and recording why the proposed examination is necessary.

25 Previously, the Secretary of State issued directions to communications service providers under section 94 of the Telecommunications Act 1984, which enabled the intelligence agencies, specifically MI5 and GCHQ, to obtain communications data in bulk. The IPA repeals this power and replaces it with bulk acquisition warrants.

- 6.33 During inspections, we are given access to the system used by MI5's investigators and analysts for their applications and we undertake random sampling and run query-based searches on the system. For example, Inspectors might use the system to identify every application which included the word 'journalist'. This means that our Inspectors can, for example, evaluate the analysts and investigators' necessity and proportionality considerations, examine particular operations and identify requests for more intrusive data sets or those requiring data over longer time periods.
- 6.34 The Targeted Communications Data CoP (paragraphs 8.23 to 8.33 and 8.38 to 8.44) contains detailed guidance for examination where the purpose is not to identify or confirm a journalistic source but where this is nonetheless likely. These protections are not mirrored in the Bulk Data CoP. We have, therefore, proposed that UK Intelligence Community (UKIC) should read across the additional guidance provided in the Targeted Communications Data CoP when considering BCD related to journalism and have proposed to the Home Office that the Codes should be amended to ensure consistency.
- 6.35 MI5 have been working to demonstrate a number of improvements that they have brought in to their authorisation processes, internal oversight and audit of this work, post October 2018, but we believe that there is more to be done in this area. They have developed a capability to undertake retrospective internal audit checks, which commenced in October 2018, and the managers we interviewed explained and demonstrated how it is envisaged the audit processes will develop and work in the future. Some basic internal retrospective audit checks are taking place but the process is in its fledgling stage.

Bulk Personal Datasets (BPD)

- 6.36 The use of BPD is an area that has been under close scrutiny by IPCO during 2018, both through inspections and via the double lock. This reflects the level of public interest in how this data, which is vital to everyday work by investigators and analysts, is used and retained by MI5. Prior to the implementation of IPA warrants to approve BPDs, we were content that MI5's records were well kept and clearly articulated. This continues to be the case since the introduction of the double lock.
- 6.37 In preparing for the commencement of Part 7 of the IPA, which governs UKIC's retention and use of BPDs, MI5 independently considered each bulk data holding to ensure that appropriate safeguards were in place and the IT infrastructure complied with the IPA. MI5 introduced a front-end system to record the justification given by their officers when querying bulk data. MI5 also scrutinised the necessity and proportionality case for retaining each dataset, along with an assessment as to whether it was 'bulk' or 'targeted' in nature (that is, whether or not the majority of individuals to whom the dataset related were of interest or likely to become of interest to MI5 in the pursuit of its statutory functions).
- 6.38 Under the new provisions of the IPA, MI5 is required to keep the proportionality of its BPDs under constant review. Before the commencement of section of the Act, MI5 judged it appropriate to retain all BPD holdings for ten years; the justification for this period of retention had been explained to the Commissioner. Under the IPA, MI5 is required to assess whether the retention of each of its BPDs remains necessary and proportionate every six months, upon renewal of the warrant. However, we have recommended that MI5 should take a more nuanced approach, considering whether retention is proportionate for all fields in BPD holdings and for each BPD held. We were not satisfied that MI5 was meeting this recommendation in full at the end of 2018 and they are now introducing a new process to discharge this requirement.

- 6.39 One key element of the IPA is the introduction of specific protections for sensitive personal data which is held or is likely to be held in BPDs retained for examination by any agency. During our discussions with UKIC ahead of the implementation of this element of the legislation, we questioned how the presence of sensitive data would be marked and identified to the authorising officer. We were satisfied that this was made clear in all cases. We are confident that the presence of any sensitive personal data would be identified during the initial analysis and that there is therefore no risk that a substantial proportion of sensitive personal data would improperly be obtained under a class BPD warrant. Our inspection at MI5 has confirmed that any sensitive data is being held appropriately.

Operational purposes

- 6.40 The IPA establishes defined operational purposes for the use of BPD. An agency may only use bulk data for an operational purpose listed on the warrant under which the BPD is being retained and examined. Under the Act, the full list of operational purposes is approved by the Prime Minister and, given the sensitivity of the work of the intelligence agencies, this list remains classified. It would not, therefore, be appropriate for IPCO to comment further other than to confirm that our JCs have been content with the case for applying the operational purposes in all authorisations reviewed.
- 6.41 Section 215 of the IPA provides for the modification of bulk personal data warrants by adding, varying or removing any operational purpose. However, this provision has not so far been used as each agency has applied to retain any BPD for use across all active operational purposes. This is in accordance with the BPD CoP, which makes clear that *'other than in exceptional circumstances it will always be necessary'* for BPD warrants to include all operational purposes. This eliminates the possibility of intelligence failure, where an agency was unable to access legally acquired data for a specific purpose. We are persuaded that the reactive nature of intelligence work means that this approach is necessary. We have therefore not reviewed any modifications at MI5 in relation to BPD in 2018.
- 6.42 MI5 will occasionally retain and examine a BPD in reliance on a specific warrant. Where the BPD is shared with the Secret Intelligence Service (SIS) and/or GCHQ, or MI5 has plans to share the BPD with them, the warrant may legitimately include all operational purposes. However, in cases where MI5 is the sole user of a BPD (so does not allow staff from SIS or GCHQ to access the dataset), examination of that dataset is only permissible for those operational purposes which correspond to one of MI5's statutory functions, which are more narrowly drawn than those of SIS and GCHQ. We have recommended that MI5 ensure that, in such cases, selection for examination of data within the BPD only takes place for operational purposes which correspond to MI5 statutory functions.
- 6.43 Our 2018 inspection of MI5's use of BPDs fell during the transition period after the implementation of BPD warrants and selection for examination processes. We have therefore not examined the use of operational purposes in practice but intend to examine this in 2019.

Non-compliance investigation

- 6.44 As noted above, we were informed in February 2019 of serious compliance risks associated with certain technology environments in use by MI5. The information initially supplied to IPCO suggested there were serious deficiencies in the way the relevant environment implemented important IPA safeguards, particularly the requirements that MI5 must limit to the minimum necessary the extent to which warranted data is copied and disclosed, and that warranted data must be destroyed as soon as there are no longer any relevant grounds for retaining it.
- 6.45 IPCO began a detailed investigation with assistance from members of the Technology Advisory Panel (TAP). Whilst the environment could only be accessed by appropriately cleared MI5 personnel, we identified a number of serious deficiencies, in particular an inconsistent approach to controls around the extent to which users were able to copy data and place it into storage areas within the environment.
- 6.46 Following this investigation, and on the basis of detailed information from MI5 on the mitigations it had put in place in response to our initial findings, the IPC determined in April 2019 that MI5 was capable of handling warranted data in compliance with the IPA's safeguards. However, the IPC also directed that MI5's use of the environment must be subject to further, detailed inspection as some of the mitigations were yet to be fully implemented. MI5's use of the relevant technology environments is therefore subject to ongoing, detailed scrutiny during 2019 and we will report further in the next Annual Report.

7. Secret Intelligence Service (SIS)

Overview

- 7.1 We conducted regular inspections of the Secret Intelligence Service (SIS) at both the London headquarters and overseas stations throughout the year. These inspections focused on the range of powers used by SIS. SIS work overseas is conducted under section 1 of the Intelligence Services Act (ISA) and in reliance on section 7 as required and when properly authorised. We have discussed with SIS whether oversight of work carried out under section 1, which does not currently fall within the Investigatory Powers Commissioner's Office's (IPCO) formal remit, should be expanded to increase IPCO scrutiny of SIS's work. To date, briefings in relation to work conducted under section 1 that fall outside of IPCO's statutory remit have been delivered during station inspections with formal oversight of this work falling to the Foreign and Commonwealth Office (FCO) and (post facto) the Intelligence and Security Committee (ISC). It is for the Government to consider whether there are sufficient resources in this area to ensure that this oversight is carried out to a satisfactory standard.

Findings

- 7.2 We have been impressed by the careful consideration by legal officers which permeates SIS's work and use of covert powers. The international scope of SIS's function places officers within a complex framework of domestic, foreign, international and European legislation. SIS has taken time to brief and debate certain issues with our office and has drawn to our attention a number of sensitive and complicated issues. We are confident that SIS's legal teams are consistently engaged in operational matters and in dialogue with counterparts at other agencies and within departments of state, including the FCO in particular.
- 7.3 SIS work closely with liaison partners in countries where intelligence is shared regularly, if not daily. Under the Investigatory Powers Act 2016 (IPA), the Secretary of State is required to ensure that an intercept or equipment interference (EI) product is only disclosed overseas if the relevant safeguards will apply to such an extent (if any) as the Secretary of State considers appropriate. This requires SIS to have sufficient understanding of the handling arrangements in place with relevant foreign partners to provide any advice required by the Secretary of State. To help achieve this, and as a matter of best practice more generally, we have suggested that SIS officers should take steps to understand how UK data will be used or retained by partner services. We recommended that SIS should progress data handling and retention work, where possible and appropriate, with liaison and create a record covering how intelligence will be stored, accessed, reviewed and deleted by partners.
- 7.4 During some station inspections, we focused on how SIS manages its relationships with liaisons posing higher human rights and compliance risks. SIS applies particularly close scrutiny to decisions to share intelligence to facilitate or solicit a detention, as this often engages the Consolidated Guidance. Overall, we were impressed with the rigorous

way SIS makes judgements about risk in this context: every officer we spoke to clearly demonstrated a strong grip on compliance and legal issues which are evidently treated as a core part of SIS's everyday work. We made a number of recommendations to further improve the way SIS presents its assessment of risk in submissions to the Secretary of State. We note, however, that SIS must carefully balance submissions to the Secretary of State, which must set out key considerations and details that they are obliged by the legislation to provide, but cannot necessarily give a comprehensive overview of all elements of the operation; this is due both to the complexities and number of possible scenarios that the operation might encounter and to restrictions imposed by Departments of State in relation to the length and format of submissions.

Covert Human Intelligence Sources (CHIS)

- 7.5 Agent running activity under the Regulation of Investigatory Powers Act 2000 (RIPA) is a small proportion of SIS's work, the majority of which is overseas and is therefore appropriately authorised under the ISA. However, SIS officers do undertake some agent operations and undercover activity in the UK which require authorisation under RIPA, as does some such activity conducted overseas. During our two CHIS inspections, we scrutinised a number of these cases in greater depth than in previous inspections. We intended to probe how SIS was conducting oversight and management during agent handling work to meet the requirements of the CHIS Code of Practice (CoP). We asked for and were provided with a wider range of documents than we had seen before and were able to gain greater assurance around the end-to-end agent running process at SIS. We previously noted that SIS's paperwork did not always explicitly set out the extent to which operational actions would take place in the UK, either physically or technically, but have now seen a trend towards greater clarity.
- 7.6 In some areas, SIS's methodology deviates from the CHIS CoP. We were concerned that in many of the cases we inspected the authorisation chain was compressed with either the CHIS being the Case Officer, the Case Officer being the Controlling Officer or the Controlling Officer being the Authorising Officer (AO). In some cases, the AO was not of greater seniority than others in the chain, which is not ideal. The CoP does allow for AOs to authorise their own activity in certain circumstances (in small organisations, for security reasons or in urgent cases), but these should be exceptional rather than the norm. SIS is not a small organisation but is organised in a series of smaller units that are separate for security reasons. We have recommended that SIS should, wherever possible, separate the roles and record any instances where an AO is authorising their own activity and that, in such cases the AO should record the reason for doing so. These instances should then be brought to our attention prior to inspection so that we can apply additional scrutiny to ensure that the AO has fully discharged their obligations and adequately recorded their consideration.
- 7.7 On a few occasions in 2017, SIS officers mistakenly did not obtain the necessary RIPA authorisation in relation to agent activity in the UK. We noted in our 2017 report that SIS were implementing new training to address this issue, which would prevent future errors. We are satisfied that this has been initiated. However, SIS informed us that their Head Office team had identified a RIPA error relating to an overseas agent engaging with a subject of interest (SOI) in the UK while preparing for our station inspection. Shortly after this inspection a second similar error was identified at another station. SIS are aware that work to ensure that all staff working overseas are up-to-date on training in this area, and understand the local, international and UK legal frameworks relevant to their operations. We will continue to keep a spotlight on this area.

Surveillance and Property Interference

- 7.8 Our findings in this area are consistent with last year's report; SIS conducts very little surveillance activity in the UK and our inspections have not identified any issues in terms of methodology or intelligence handling. We were content that the limited surveillance activity undertaken by SIS in the UK was necessary and proportionate.
- 7.9 At one inspection, we spoke to surveillance practitioners at SIS. As above, we are mindful of the complexities of work that might have a global or trans-national reach and wanted to test that operators are clear on the restrictions and safeguards in place under RIPA. We are confident that SIS officers are trained on how RIPA applies to surveillance activities and understand when an authorisation should be sought before proceeding.

Targeted Interception (TI) and Equipment Interference (EI)

- 7.10 As with the other agencies, our inspection of these powers in 2018 bridged the gap between the old RIPA and new Investigatory Powers Act 2016 (IPA) regimes. In general, SIS achieved a good level of compliance. In most cases, renewal applications always included a statement of whether confidential information had been collected, although it was not always clear if confidential information had not been collected. We suggested that a more consistent approach should be adopted and that nil returns should be articulated in the renewal application if material had not been collected.

Additional targeted interception and targeted examination provisions

- 7.11 As detailed in chapter 2, the IPA sets out provisions to obtain warrants to interception communications for a group of persons or more than one organisation or set of premises. We did not inspect any thematic authorisations at SIS during 2018. We will focus on this in the future, although previous inspections and our oversight via the double lock confirm that this activity will be limited given SIS's focus on activities outside of the UK. From conversations with SIS, we are confident that they will apply careful consideration before seeking thematic authorisations.
- 7.12 SIS did not apply for any warrants under section 17(2)(c) in relation to training or testing activities in 2018.

Targeted equipment interference warrants

- 7.13 As described in chapter 6 we conducted light touch inspections of these warrants towards the end of 2018 and did not inspect a substantial number of thematic authorisations. We intend to review these closely in 2019. Our oversight via the double lock did not raise any concerns in this area and the JCs did not reject any thematic applications.

Bulk Communications Data (BCD)

- 7.14 SIS has not undertaken bulk acquisition of Communications Data (CD) in 2018. SIS has access to certain BCD lawfully obtained by the Government Communications Headquarters (GCHQ) and MI5 where it is operationally necessary.

Bulk Personal Datasets (BPD)

- 7.15 SIS holds datasets covering a wide variety of mission areas. We worked closely with SIS throughout 2018, in advance of IPA implementation, to understand the nature of their bulk data holdings and how this data would continue to be used and handled under the new authorisation framework. For this reason, we have a high level of confidence in how SIS safeguards data and have no concerns in this area.
- 7.16 The IPA has required the UK Intelligence Community (UKIC), and SIS in particular, to overhaul documentation in relation to BPD. Each warrant application must set out in general terms the nature of the data being held, how and why it will be retained and how long the data is expected to be valuable to analysts for the specified purpose. This information is typically clarified in relation to individual datasets on internal approval documentation. This process has meant that there has been a significant improvement in the clarity of records which we expect to continue.
- 7.17 The categorisation of a dataset as a BPD relies on the assessment that the data within the set relates to a majority of individuals who are not, and are not likely to become, of interest to the intelligence agency in the pursuit of its statutory functions. In some cases, datasets will be held where the data is 'targeted', in other words the data relates to individuals who are, in the majority, assessed to be of intelligence interest. In this instance, the BPD authorisation process does not apply. We have been impressed by the rigorous process in place to assess and approve the categorisation of data internally and have welcomed discussions on a sample of targeted data. We have reviewed minutes of relevant panel meetings and interviewed senior officers responsible for these decisions. This has given us a good level of confidence that data is being appropriately categorised and handled. We have encouraged SIS to ensure that this is an iterative process and that they should remain aware of changes in the nature of their data holdings and how that data is being accessed and analysed by their officers. This is an area which we will continue to inspect carefully to ensure this very sensitive data is appropriately protected.
- 7.18 Due to the sensitivity of the data, we are not able directly to access the data holdings or analytical systems. In both cases, these are subject to access controls. We have received live demonstrations from analysts, showing how data is queried both manually and automatically and how it is used for specific intelligence aims. In previous years, we have looked at protective monitoring around these systems and have questioned individual analysts about a sample of searches conducted through the year. This continues to be a key element of our inspections and provides a basis of confidence for the value statements set out by SIS in both authorisation paperwork and internal review documents.
- 7.19 We noted in 2017 that SIS intended to 'refresh' their protective monitoring process. UKIC initiated a Strategic Protective Monitoring (SPM) project which was to amalgamate SIS, MI5 and GCHQ protective monitoring systems to enable a single UKIC team as well as provide some new analytics. However, the project was formally closed and a new project or programme will be started once requirements have been assessed. This is a sensitive area of work which needs to be handled carefully to establish a consistent and appropriate mechanism to ensure that protective monitoring continues to be fit for purpose as next generation systems are implemented. We will therefore continue to engage with UKIC on this matter.
- 7.20 In previous years, we have noted concerns that bulk datasets had not been ingested into SIS's analytical systems. We note that the IPA does not establish any specific requirements in terms of the ingestion of data, provided a relevant warrant is in place to authorise the retention and examination of that data. However, we would not expect UKIC to apply to

renew an authorisation to retain and examine a bulk dataset which was not available for analysis if steps were not being taken actively to resolve any data ingestion issues. Our discussions with UKIC have identified that each agency's review panel regularly considers any datasets that have not been fully ingested and, in some cases, has refused to re-authorise datasets which have not been ingested into relevant systems. We will continue to review any relevant notes from these panels and on a case-by-case basis may in the future challenge unnecessary delays if they do occur.

- 7.21 As mentioned above, the IPA introduces safeguards for sensitive personal data. Any BPD comprising a substantial proportion of sensitive data must be retained under a specific, not class, authorisation. Our inspection at SIS identified that any relevant data is being appropriately marked and authorised. Our inspections considered why certain categories of sensitive personal data might be necessary for the discharge of SIS's functions. We were persuaded by the documented justification in all cases reviewed.

Operational purposes

- 7.22 As above, we are satisfied that the responsive nature of SIS's work necessitates the retention of the vast majority of its warranted BPDs for all current operational purposes. SIS has not made any modifications under section 215 of the IPA in 2018. We would not expect this approach to change in 2019.
- 7.23 We did not inspect SIS's records in relation to selection for examination of BPD material in 2018 because our inspection was conducted during the transition period after the implementation of BPD warrants. We intend to inspect these records in 2019 and anticipate that this safeguard will enable us to confirm that data is being accessed appropriately by officers with a clear business need to do so.

Section 7 of the Intelligence Services Act (ISA)

- 7.24 SIS conduct a range of activities overseas under section 7 of the ISA. On inspection, SIS proactively brought a number of sensitive and complex operations to our attention in addition to material that we selected for review. We considered submissions to the Foreign Secretary to cover work conducted at a number of stations and discussed those cases with the teams working under those authorisations either in person or via video conference. In each case we reviewed, SIS set out the legal framework for their operation, taking domestic and international law into consideration. This detail is typically thorough and clearly set out.
- 7.25 In 2017, we raised the concern that considerations of privacy were not well documented by SIS on internal approvals. This concern related to the way that SIS officers recorded privacy considerations for operations and activities conducted lawfully under authorisations approved by the Secretary of State. Previous Commissioners have noted similar concerns in relation to SIS's record keeping, but that this does not reflect a lack of consideration in SIS's operational planning. Nonetheless, we have urged SIS to improve record keeping such that they are able to demonstrate how their work respects individuals' right to privacy, and takes steps to minimise intrusion, where possible. We have seen a general improvement in SIS's documentation, including to introduce more consistent internal records for reliance on section 7 authorisations and therefore have no ongoing concerns on this issue.

- 7.26 SIS's submissions to the Foreign Secretary are supplemented by internal documents, including decision documents. Papers presented clear, detailed arguments as to why it remained necessary, proportionate and lawful to proceed with operations. SIS's internal record keeping has been the subject of recommendations in previous years and we have continued to make a number of recommendations which focused on ensuring SIS has a comprehensive audit trail of decisions taken. However, we are satisfied that SIS have dedicated substantial resources to ongoing training and IT improvements to enable this work.
- 7.27 We reviewed a number of specific submissions covering potentially high-risk cases. We were pleased that these included a strong necessity and proportionality argument for running the case in question, along with robust processes for keeping the risks involved under constant review.
- 7.28 SIS is engaged in several programmes of work which amount to training and 'capability building' with foreign liaison services and/or military and intelligence units. With this work, SIS is delivering against Her Majesty's Government's (HMG's) objectives to promote good human rights practice and assist partner governments to build capable investigative services, often against a specific local threat that impacts upon British interests. In some cases, the local liaison service and internal partners will have a very poor human rights record; SIS therefore seeks to insulate its provision of training, equipment and, similar to a specific unit from the wider liaison service, to ensure any capability SIS provides is not abused.
- 7.29 This work to safeguard and control the use of any training or capability is essential to ensure that SIS are not contributing to unlawful or unacceptable activity. We have discussed several examples of this model with SIS officers in London and overseas, and with legal officers, and are confident that SIS take their international obligations extremely seriously. When reviewing section 7 authorisations, we consider the mitigations in place in each case and the credibility of those mitigations. We were generally satisfied with the mitigations SIS set out in submissions, but in future inspections we intend to investigate further how SIS assesses its capacity building work against the risk that HMG might inadvertently provide training or support which could develop a liaison partner's ability to conduct unlawful acts.
- 7.30 For SIS, capacity building is conducted with a small, discrete unit formed of a select number of staff from the relevant liaison partner and subject to close supervision by SIS, often known as a joint unit. One of the key risks SIS must consider in this context is whether the capabilities acquired by members of the joint unit might be disclosed into their wider service and then be used for purposes beyond the scope of the mission and of the authorisation. In general, this risk was carefully assessed in submissions and credible mitigations were presented to Ministers. However, in a small number of cases we remained unconvinced that SIS could credibly control and limit the disclosure of the relevant capability.
- 7.31 In 2019, we intend to investigate further how SIS assesses its capacity building work against the risk that HMG provides training or support which could develop high risk liaisons' ability to conduct unlawful acts, which has implications for the Consolidated Guidance and other legal considerations.

8. Government Communications Headquarters (GCHQ)

Overview

- 8.1 We inspect the Government Communications Headquarters (GCHQ) individually as well as, on occasion, in combination with UK Intelligence Community (UKIC) partners as explained above. GCHQ contributed to the work to prepare for the Investigatory Powers Act 2016 (IPA), including to the training programme for our Judicial Commissioners (JCs), leading in particular on some of the more technical areas and helping to develop a realistic understanding of how bulk powers are used.

Findings

- 8.2 It is worth noting that GCHQ's reliance on bulk powers under the IPA is greater than they originally anticipated.²⁶ This reflects the realities of enacting the legislation rather than a substantial change in GCHQ's working model or a response to the availability of those powers.
- 8.3 Our inspections show that GCHQ's IT protects all data to the standard set out in the IPA as a default. Where there is an operational requirement to access data, which will include bulk communications data (BCD) and/or bulk personal data (BPD), an analyst must justify why the access and examination of the data are necessary and proportionate and must record the specific intelligence requirement and priority for each search. We have found that this establishes the most consistent and cautious approach to safeguarding operational data; all data is protected to the standards set out in the IPA as a default.
- 8.4 The internal procedures within GCHQ have been modified to take account of the commencement of bulk acquisition warrants within Chapter 2 Part 6 of the IPA and the accompanying Code of Practice (CoP). We will continue to work with GCHQ to ensure that these are adequate.
- 8.5 In November 2018, GCHQ published details of their UK Equities Process.²⁷ This relates to GCHQ's work with technology companies to maintain the intended level of security of publicly used technologies. This document explained that many, but not all, technical vulnerabilities are disclosed to vendors and GCHQ set out the internal review process that they use to assess whether the best course of action is to inform the company, rather than to exploit the vulnerability for national security purposes without disclosing it to the vendor. This process includes scrutiny by a panel of technical experts from GCHQ, National Cyber Security Centre (NCSC), UKIC and the Ministry of Defence (MOD). GCHQ invited the Investigatory Powers Commissioner's Office (IPCO) to oversee this process in November

26 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/761147/Letter_from_the_Security_Minister_to_Dominic_Grieve_QC_MP_December_2018.pdf

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

2018 on a non-statutory basis and our initial findings will be addressed in our 2019 Annual Report.

- 8.6 During 2018 we probed GCHQ's work with contractors to supplement the Investigatory Powers Tribunal's (IPT's) review of the lawfulness of GCHQ's disclosure of bulk data to industry partners. We inspected how GCHQ use industry partners, considering the range of work in which contractors are involved and the lawful basis for this activity. We interviewed a number of individuals involved in joint programmes of work and were satisfied with their understanding of the legal requirements and safeguards around their work. We reviewed the internal oversight mechanisms for industry contractors working both within GCHQ and off-site and were satisfied that these were rigorous and mirrored those in place for GCHQ's own officers.
- 8.7 We were briefed on the physical and personnel security considerations and safeguards in place at GCHQ and for off-site working. GCHQ impressed upon us that contractors working within GCHQ are treated in the same way as permanent staff; all individuals are subject to the same vetting, training, management and oversight. We concluded that the disclosure of material to industry partners was necessary and appropriate, given the unique capabilities that these partners offer, and that the level of oversight provided by GCHQ was adequate.
- 8.8 In some cases we reviewed in relation to GCHQ's work with industry partners, however, we were not satisfied that the internal documentation for the project provided a fully-auditable record of actions tasked, conducted and authorised. GCHQ has suggested that this may reflect a lack of consistency of approach, rather than a failure to document considerations. We will review this issue in more detail in our 2019 Annual Report.
- 8.9 We were satisfied on the basis of inspections in 2018 that GCHQ is generally managing the sharing of intelligence with foreign partners appropriately, having inspected the mechanisms used by GCHQ to record requests for data and to disclose data to foreign partners.

Covert Human Intelligence Sources (CHIS)

- 8.10 In 2017, we asked GCHQ to adapt its covert human intelligence sources (CHIS) application template to document more information on necessity, proportionality and intrusion considerations. GCHQ worked with UKIC partners and have aligned their records, which focus on articulating and justifying the level of collateral intrusion in particular. GCHQ has also given consideration to how law enforcement bodies might authorise and record similar operations. We were pleased to note that GCHQ's response to this recommendation comprised a broader and collaborative consideration of the underlying principles.
- 8.11 Because of the nature of their work, GCHQ conducts little agent activity under the Regulations of Investigatory Powers Act 2000 (RIPA); that which they do is typically online. Our inspection focused on the adequacy of training offered to the team and level of oversight of their work within GCHQ. We were satisfied that the standard of training was high and that officers had a good understanding of the relevant legal requirements. However, we made a number of recommendations in relation to internal oversight of CHIS-related activity and in the future will expect GCHQ to demonstrate that authorising officers have an in-depth and up-to-date understanding of casework that they oversee.

Surveillance

- 8.12 This last point also applies to Directed Surveillance Authorisations (DSAs). This again is a marginal element of GCHQ's work but we have made recommendations to improve the rigour of internal oversight.
- 8.13 Our inspection also identified that GCHQ's review paperwork for surveillance activity lacked sufficient detail to enable independent judgement. We have made recommendations to standardise the content of review documentation to ensure that authorising officers are meeting the requirements of the Code of Practice (CoP).

Targeted Equipment Interference and Property Interference

- 8.14 The majority of GCHQ's technical operations in the UK are now authorised under the IPA. Any operation that is conducted without the intention to obtain communications, equipment data or other information will continue to be authorised under section 5 of the Intelligence Services Act (ISA). We have inspected warrants covering UK-based programmes of work which relate to operations conducted by and/or in collaboration with industry partners. We are content that the scope of these operations and the role of the partner are clearly articulated on the authorisation casework.
- 8.15 We noted a lack of clarity on the details of planned operations on GCHQ's applications for warrants under section 5. In particular, we noted that the extent of any likely collateral intrusion was not well documented and, in some cases, details of highly technical operations were not given in full (such as the precise nature of the equipment to be targeted). Having said this, it is worth noting that GCHQ's warrantry and legal policy teams worked closely with UKIC partners and IPCO to agree standards of drafting ahead of IPA implementation. In particular, GCHQ has recognised the need to articulate complex technical operations which will be authorised via the double lock. We therefore expect that the clarity of authorisations will improve significantly in 2019.

Additional targeted interception and targeted examination provisions s17(2)

- 8.16 As detailed in chapter 2, the IPA sets out provisions to obtain warrants to interception communications for a group of persons or more than one organisation or set of premises. Our inspection at GCHQ fell while they were in the transition phase, and we intend to look closely at the use of thematic warrants in 2019, noting GCHQ's statement that the nature of GCHQ's work lends itself more to bulk collection rather than reliance on thematic authorisations.
- 8.17 GCHQ did not make any applications under the provision s17(2)(c) in relation to training and testing in 2018.

Targeted equipment interference warrants s 101(1) and (2)

- 8.18 As explained in chapter 6, GCHQ transitioned extant authorisations into the IPA regime during the latter half of 2018 and we conducted light touch inspections to accommodate this. We intend to inspect internal mechanisms as well as IPA warrantry closely in 2019. Our oversight via the double lock did not raise any concerns relating to GCHQ's operations in this area and the JCs did not reject any thematic applications.

Bulk Interception (BI) and Equipment Interference (EI)

- 8.19 In 2018, GCHQ transitioned its lawful authority for conducting bulk interception and bulk equipment interference from RIPA warrants to warrants under Part 6 of the IPA. GCHQ's use of bulk powers is a vital and sensitive area of operations, which we have scrutinised closely as the IPA has come into force. GCHQ gave a number of briefings to JCs and members of the Technology Advisory Panel (TAP), including demonstrations on a range of technical topics. These were augmented by demonstrations of how data is held and safeguarded within GCHQ and how it is accessed by operators.
- 8.20 A higher proportion of GCHQ's EI operations than previously envisaged are conducted in reliance on bulk equipment interference (BEI) warrants. We have questioned this approach and underlined the importance of making internal records open to inspection. GCHQ sets out clear arguments in all of their warrant applications for the necessity and proportionality of using bulk techniques in pursuit of their statutory functions. We are satisfied with this argument, but continue to challenge this assertion on a case-by-case basis to ensure that this is the correct approach in each instance. Overall, we were content with the way in which GCHQ is managing its use of EI powers and were satisfied that the necessity and proportionality of individual operations is being well accounted for in internal records of reliance on the key bulk warrants. These are subject to an enhanced level of post facto inspection. Nevertheless, given the scale of GCHQ activity which is being internally approved under bulk warrants, we will continue subjecting EI operations to particularly detailed scrutiny on inspections.
- 8.21 The European Court of Human Rights (ECHR) judgment in the Big Brother Watch case concluded that there should be more robust independent oversight of the selectors that are used by analysts to examine material that has been collected under a bulk interception warrant. This conclusion is also relevant to bulk equipment interference. In 2018, we scrutinised analysts' justifications as to the necessity and proportionality of material they selected for examination from bulk systems. In 2019, we plan to explore enhancing further our oversight of the process for selecting material from bulk intercept by examining the technical processes by which GCHQ filters material collected in bulk before it is made available for examination. Given the volumes of data involved, it is critical to the proportionality of GCHQ's operations that this process is managed effectively.
- 8.22 Whenever GCHQ analysts conduct a query of bulk data, they are required to draft a statement explaining why their query is necessary and proportionate. Overall, we concluded that these justifications were meeting the required standard and analysts were accounting for the proportionality of their queries of bulk data in sufficient detail. GCHQ has responded to recommendations made by IPCO in this area and has a plan in place to improve standards across the board. We had begun to observe improvements towards the end of 2018. This work is particularly important, because GCHQ's ability to use powers in bulk relies on having a robust and accountable internal approval and documentation structure in place.

Operational Purposes

- 8.23 The IPA established defined operational purposes for bulk interception and bulk equipment interference. These are recorded in a list approved annually by the Prime Minister.
- 8.24 An agency can only select for examination product from bulk interception (content or secondary data) or from bulk equipment interference for a purpose listed on the warrant under which the product was obtained.

- 8.25 In 2018 GCHQ sought approval in every instance to use warranted bulk equipment interference warrants for the full range of operational purposes. For bulk interception GCHQ felt it appropriate to limit the operational purposes for a number of warrants.
- 8.26 This is consistent with the strategic nature of bulk intercept and bulk equipment interference, reflects the broad range of targets that GCHQ may need to work against under these warrants and is consistent with the relevant Codes of Practice. Sections 145 and 186 of the IPA provide for the modification of bulk interception and bulk equipment interference warrants respectively. Under a modification agencies can add, vary or remove an operational purpose as specified in the warrant as a purpose for which any intercepted content or secondary data or EI material obtained may be selected for examination. During 2018 GCHQ did not modify any bulk interception or bulk equipment interference warrants in this way.
- 8.27 The system used by GCHQ to effect selection for examination of product obtained under their bulk interception and bulk equipment interference warrants require an operational purpose to be recorded before access is granted to the product, along with a necessity and proportionality justification.

Bulk Communications Data

- 8.28 Extant section 94 directions were replaced by bulk acquisition warrants commenced in February 2019 and do not, therefore, form part of our report of GCHQ's activities in 2018. We reviewed all of the section 94 directions during our inspections and found them to be of a high standard, including clear detail of the expected value from the proposed action. We have previously provided a statistic for the percentage of end product reports which include material acquired under section 94. In view of the transition to the IPA, and an evolution of how intelligence is analysed and reported at GCHQ, we no longer believe that this statistic is meaningful. There is no question of the ongoing value of bulk communications data (BCD) to GCHQ's operational output, but we are currently unable to provide any statistics to quantify that value.
- 8.29 The Foreign Secretary requires GCHQ to carry out a review every six months and share these reviews with the Foreign and Commonwealth Office (FCO). We scrutinised the review documentation at GCHQ and were satisfied that all were comprehensive, containing a summary of the data that had been retained and how the BCD was to be handled, analysed and accessed. The reviews included the operational justification and legal basis for continued retention and use and set out the value to relevant operations. The reviews documented an assessment of the collateral intrusion and set out consideration of the issues and consequences of alternative forms of acquisition and the potential contingencies involved.
- 8.30 As at MI5, we review acquisition, retention, use and disclosure arrangements for all data obtained under a section 94 notice. In 2018, we interviewed officers responsible for authorising access, as well as analysts and staff responsible for auditing access to the data.
- 8.31 During our inspections, GCHQ and MI5 both demonstrated the value of BCD to recent operations. The critical role of BCD to the range of activities conducted at GCHQ was well articulated in the casework we inspected. We were satisfied that the submissions to the Foreign Secretary explicitly set out why the acquisition, retention, access to and analysis of the data was necessary to GCHQ's statutory functions and specifically to the stated operational requirements. We considered the nature of the requested data and the stated

intelligence requirements and were satisfied that the documentation demonstrated that their approach was necessary and proportionate.

- 8.32 We inspected GCHQ's review records, which was a requirement of the section 94 direction. The reviews summarised how the data to be retained was being handled and analysed. Our conversations with analysts and officers responsible for protective monitoring gave us a high level of confidence that these were being adhered to. We have inspected the front-end analytical tools used to access BCD and were satisfied by the access control mechanisms in place. GCHQ's reviews documented the operational advantages of accessing BCD and how this would progress the relevant operations and investigations. The reviews additionally included the operational justification and legal basis for continued retention and use.
- 8.33 During inspections into the selection of BCD for examination by analysts at GCHQ, we reviewed the breadth and depth of the internal procedures and audited a number of individual requests made by analysts. We concluded that the analysts had justified in each case properly why it was necessary and proportionate to access the communications data (CD).
- 8.34 GCHQ carries out robust retrospective audit checks. The senior managers we interviewed explained and demonstrated in some detail how the audit processes work and the function of GCHQ's Internal Compliance Team, who carry out random retrospective audit checks of the analysts' justifications for the selection of BCD. Some system changes were undertaken in early 2018 and this enables the IPCO Inspectors, working with GCHQ's Internal Compliance Team, to select and review the analysts' necessity and proportionality justifications for the selection of BCD. The changes have much improved the capabilities of the retrospective audit checks. Importantly, GCHQ were able to demonstrate how deficiencies are remedied when submissions fall short of the required standard. When the internal audit team identify that necessity or proportionality justifications recorded by particular analysts are below the minimum requirements, the Policy and Compliance Lead is responsible for ensuring that the analyst is made aware. The Policy and Compliance Network is a network of staff distributed throughout GCHQ and who are responsible for compliance in their areas. This includes working with analysts to ensure their justifications are up to standard and providing additional training when audit has found justifications which fall below requirement.
- 8.35 We made recommendations as to how the training and guidance provided to analysts could be delivered to highlight the requirement for clarity within their justifications (for example, simple text setting out what operational benefit is sought when undertaking the queries).
- 8.36 In addition, GCHQ's IT Security Team conducts technical audits to identify and further investigate any areas of concern (for example, activity that may be a breach of the operational requirements). The senior managers we interviewed as part of the inspection process explained and demonstrated in some detail how the audit processes work and the function of the team. We were satisfied with the thorough overall approach.

Bulk Personal Data (BPD)

- 8.37 As detailed above, we worked with UKIC in anticipation of the implementation of the IPA to ensure that records in relation to their bulk data holdings complied with the requirements of the IPA. In preparation for commencement of Part 7 of the IPA, GCHQ conducted a detailed review of all of its BPDs to ensure they were all transitioned into appropriate warrants under the Act. This review involved determining which holdings should be authorised under specific or class warrants. GCHQ applied for a number of class

BPD warrants, which authorise the retention and examination of the majority of its BPD holdings, and a number of specific BPD warrants to authorise the minority of datasets. Many of GCHQ's holdings are technically complex and so GCHQ have worked closely with the JCs and the TAP so that the judges considering the warrant applications have a clear understanding of the technical issues involved.

- 8.38 GCHQ briefed us on how sensitive personal data would be managed in accordance with the requirements of the IPA. We are content that relevant data would be identified during the examination and ingestion phase and that only data necessary for the stated operational purposes would be retained.
- 8.39 GCHQ holds a large number of datasets outside of the BPD regime, usually because these datasets do not contain personal data. In some cases, it is not immediately apparent whether a given dataset constitutes a BPD and GCHQ errs on the side of caution. For example, a dataset containing Internet Protocol (IP) addresses which may or may not relate to individuals could be classed as personal data. In some cases, GCHQ identified that any personal data which a dataset may contain is *de minimis*. In this scenario, we agreed with GCHQ that it would be reasonable not to seek a BPD warrant to authorise retention of the dataset. However, we noted that GCHQ did not have a process in place to record centrally any decisions it took on whether or not datasets were BPDs. In response to a recommendation from us, GCHQ is now implementing a process which we will inspect in 2019.
- 8.40 Internally, GCHQ reviews the necessity and proportionality case for retaining BPDs under class warrants or acquiring new ones through its BPD Review Panel. Overall, we were satisfied that the panel is effectively overseeing the acquisition, retention and deletion of GCHQ's BPDs, although we made a small number of recommendations to improve the clarity of the paperwork put before the panel and the extent to which the panel's decisions are subject to challenge.
- 8.41 During our inspections, as at SIS, we received demonstrations on how GCHQ's BPDs are accessed and used. This included a spot-check review of internal justification records used by analysts to document what they are looking for and why. We were not satisfied by the standard of these records, although interviews with staff demonstrated a high level of consideration and understanding of the relevant principles. We recommended that GCHQ should refresh staff training to address this shortfall and, in particular, should focus on the issue of intrusion and the proportionality of interrogating BPD in relation to a particular intelligence requirement. We will follow this up at inspections in 2019.

Operational purposes

- 8.42 Like MI5 and SIS, in most cases GCHQ seeks approval to use warranted BPD for all operational purposes in accordance with the CoP. There are some specific datasets which GCHQ assesses to be necessary to retain and examine only in relation to a subset of operational purposes. In those instances, GCHQ will apply for a warrant which names a subset of operational purposes. We have not seen any modifications from GCHQ although they have applied to the FCO in one instance to remove operational purposes that were not necessary.
- 8.43 As noted for the other agencies, we did not scrutinise the records relating to selection for examination of BPD material during 2018. We will review these records in 2019 and will examine whether data is being appropriately accessed, including by an individual with a clear operational need in line with an authorised operational purpose.

Challenge to the lawfulness of GCHQ's use of bulk data

- 8.44 As noted in chapter 2, in *Privacy International v GCHQ & Others* IPT/15/110/CH, the IPT considered the lawfulness of GCHQ's use of bulk data. The IPT judgment called for "*a review of existing procedures at GCHQ in relation to sharing of intelligence and of bulk datasets... under the supervision of IPCO*". In response, GCHQ is conducting a detailed review of the processes and procedures governing decisions to share data in bulk with foreign partners. This review is ongoing and we are receiving regular updates. We will report in full on the outcome of the review in our 2019 Annual Report.

Intelligence Services Act Section 7

- 8.45 In previous reports we have explained that GCHQ conducts a range of activities overseas relying on authorisations obtained under section 7 of the Intelligence Services Act (ISA). GCHQ sometimes relies on class authorisations to authorise a set of activities, which are managed internally using approval documentation. We have scrutinised this paperwork and interviewed analysts and approving officers. As with other areas of internal documentation, we have recommended that GCHQ should ensure that these records demonstrate adequate consideration of proportionality and intrusion in each case.
- 8.46 GCHQ's work on equipment interference, formerly conducted under section 7, is now conducted under Parts 5 and 6 of the IPA. In some instances, GCHQ will conduct operations which do not acquire communications, equipment data or other relevant information protected under the IPA, but which would still be an offence under the Computer Misuse Act 1990. These operations continue to be authorised under section 7 of the ISA. Our priority in this area is to work with GCHQ to ensure that our Inspectors and JCs understand the types of data involved during all phases of a relevant operation and scrutinise whether the correct authorisation(s) are in place.
- 8.47 We have reviewed a sample of the relevant casework and are satisfied that these operations are appropriately authorised under the ISA and IPA. Many of GCHQ's internal processes and safeguards do not take into account the method of authorisation and will ensure that data obtained is handled to meet stringent safeguards, irrespective of how the operation is authorised. Given the sensitivity of that work, we are not able to disclose details of the specific operations.
- 8.48 In 2017, we stated that we were not satisfied that GCHQ were properly capturing the likelihood of obtaining legal professional privilege (LPP) material. The IPA implements specific safeguards in relation to the handling and retention of LPP material, which must be approved by the IPC. We are confident that GCHQ have put processes in place to meet the requirements of the Act and to ensure that warrantry accurately represents the likelihood that LPP material will be obtained. We are satisfied that GCHQ are identifying LPP material and handling it in accordance with those safeguards.

9. Ministry of Defence

Overview

- 9.1 We conduct oversight of the Ministry of Defence's (MOD) use of the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 (IPA) powers in the UK, and non-statutory oversight of the MOD's agent running and surveillance activities overseas.

Findings

- 9.2 In line with previous years, the MOD continues to make limited use of investigatory powers in the UK, with good consideration of the level of intrusion conducted and thorough internal documentation of planned activities on the small number of occasions when they do. We were satisfied that the records examined, supplemented by interviews with officers responsible for the application, authorisation and management of covert activity, demonstrated a high standard of compliance with RIPA and the Surveillance and Covert Human Intelligence Sources (CHIS) Codes of Practice for activities both within the UK and overseas.

Covert Human Intelligence Sources (CHIS)

- 9.3 In our 2017 report, we noted that the MOD had started using online CHIS and had introduced guidance for officers involved in this activity. We inspected one online case this year in particular and the MOD's casework demonstrated a clear record of activity and mechanisms for internal oversight.
- 9.4 We inspected the internal review mechanisms for agent running activity in place at the MOD and were pleased to note a regular, centralised process was in place. This is used by the MOD to oversee the ongoing necessity of their use of covert powers in relation to a range of missions. Our inspection noted good consideration of the proportionality of conducting each action authorised and of the likely collateral intrusion.

Surveillance

- 9.5 Authorisations for directed surveillance were supported by comprehensive intelligence cases and the covert activity to be undertaken was clearly and unambiguously described by the Authorising Officers. Of particular note was the quality of assessment and supporting observations provided to authorising officers by the legal and policy advisors. The MOD consider it important to engrain in their personnel the discipline of recording RIPA considerations for all surveillance activity and a strong culture of compliance was evident throughout the inspection.

Interception and Equipment Interference

- 9.6 The MOD may apply to the Secretary of State for Defence to conduct activities in the UK which fall under the IPA, such as interception or equipment interference.

Additional targeted interception and targeted examination provisions s17(2)

- 9.7 As detailed in chapter 2, the IPA sets out provisions to obtain warrants to intercept communications for a group of persons or more than one organisation or set of premises. Under section 17(2)(c) the MOD may apply for a warrant to intercept communications for the purposes of training and testing in the UK. Our inspection of the MOD fell during the transition period as the IPA was being introduced and so we did not inspect any reliance on this provision in 2018.
- 9.8 With regard to activity authorised under RIPA, our inspection noted that the MOD has good internal authorisation processes. There is a good audit trail which details what equipment is used and when and what if any collateral intrusion occurred.

Targeted equipment interference warrants s 101(1) and (2)

- 9.9 We discussed the provisions for thematic warrants in relation to training and testing equipment with elements of the MOD during the process of transition to the IPA. We will inspect any reliance on these provisions at future inspections.

10. Consolidated Guidance

Overview

- 10.1 In accordance with a direction from the Prime Minister made under Section 230 of the IPA on 22 August 2017, we inspected the UK Intelligence Community (UKIC) and the Ministry of Defence (MOD) to examine their compliance with the requirements of the Consolidated Guidance. Many decisions engaging the Consolidated Guidance cut across the work of more than one organisation and accordingly our findings are presented thematically in this section.
- 10.2 The Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) often use section 7 of the Intelligence Services Act (ISA) to authorise activities overseas which will involve continued consideration of the risk of torture or cruel, inhumane or degrading treatment (CIDT). The existence of a section 7 authorisation does not remove the obligation for officers to apply the Consolidated Guidance and to continue to inform senior officers and/or Ministers, as appropriate, in the event of changes to the risk assessment as an operation is progressed. It should not be necessary to state that section 7 authorisations cannot be used to authorise internationally unlawful acts.
- 10.3 In 2017, we stated our intention to obtain statistics in relation to the use of assurances by the intelligence agencies and the MOD. This intention was expressed in IPCO's evidence to the Intelligence and Security Committee (ISC) inquiry into detainee mistreatment and rendition. We have worked with UKIC to understand how they use assurances and how the credibility of specific assurances is assessed and continually monitored. It is clear that assurances are sought both verbally and in writing and, on reflection, we judge that the way that assurances are obtained and relied upon renders this a pure statistic of limited value. In our view, having written assurances in place cannot be considered to be a single factor enabling UKIC officers to pursue a course of action where the Consolidated Guidance is engaged. We have not, therefore, collected figures for assurances in 2018. This is not to under-estimate the importance of assurances when assessing risk and we cover this in more detail below.

Findings

- 10.4 Overall, we are satisfied that UKIC and the MOD consistently ensure that decisions taken which engage the Consolidated Guidance are subject to detailed and careful scrutiny. This is especially the case in complex counter-terrorism cases, which sometimes involve both serious human rights risks and imminent threat to life. In many cases put before Ministers, bespoke and detailed legal advice was included, setting out the legal basis for the proposed course of action under domestic and international law.
- 10.5 UKIC and the MOD all have robust processes for ensuring decisions which engage the Consolidated Guidance are brought to the attention of policy and legal experts for review, even in what they might consider to be fairly routine cases. However, each agency does this

differently and we have suggested that more could be done to join up the process where a decision engages more than one organisation. A considerable amount of work has now been done to achieve this.

- 10.6 In 2017, we noted that the MOD were not recording the matters taken into consideration in relation to the risk of a lack of due process on their Consolidated Guidance documentation. Our recent inspection confirmed that the internal guidance has been updated to prompt the assessing officer to set down any relevant points. We are satisfied that the MOD's approach meets the requirements of the Consolidated Guidance.

Assessing Risk

- 10.7 Frequently, UKIC and the MOD must decide whether to pass intelligence to a foreign liaison partner, or to cooperate with them in a joint operation. In any circumstances where Her Majesty's Government (HMG) is not able directly to control the circumstances of detention, the officers involved must assess the risk that suspects or detainees could be mistreated. This assessment will rely on a range of factors, including HMG's knowledge of the liaison partner's human rights record and their conduct in similar operations, and the specifics of the particular case. The Consolidated Guidance provides a framework for officers to escalate any case where there is assessed to be a risk of mistreatment.
- 10.8 We welcomed UKIC's decision to set up a central team to draft objective summaries of liaison partners' compliance status to inform decisions under the Consolidated Guidance. We were impressed by the quality of the assessments it has produced to date. However, a number of more challenging priority countries have not yet been assessed. We have made several recommendations to UKIC which focus on ensuring all relevant staff have access to these assessments and take these into account when making decisions under the Consolidated Guidance.
- 10.9 In cases where the risks are assessed to be serious, UKIC and the MOD submit to Ministers for a decision. In this scenario it is vital that assessments about the risks and national security benefits of proceeding are presented in an objective and balanced manner. This was overwhelmingly the case in submissions we reviewed, although we noted one case at SIS where uncertainties about the reliability of the underlying intelligence case were not articulated as clearly as they should have been.
- 10.10 In a small number of cases at SIS and the MOD, we observed officers recording the level of risk as 'unknown' or referring to a 'generic risk of mistreatment'. We have recommended to SIS and the MOD that risks must be quantified as either above or below the 'serious risk' threshold; uncertainty is a key factor in the decision before Ministers, but officers should not fall back on 'unknown risk'.

Assurances

- 10.11 Assurances are an important mitigation which can be relied upon by HMG to prevent mistreatment occurring at the hands of a liaison service. Assurances are typically sought from a senior figure who can guarantee that an individual will be detained in a specific and compliant facility and that local officers will not engage in unacceptable behaviour. The logic in most of the records we reviewed was that, amongst other things, by engaging with a senior and credible figure in the organisation in question, HMG can rely on the assurances obtained and can continue to rely on those assurances because of the strength

of a sustained personal relationship. Whilst this is usually the case, we identified some important exceptions during our inspections in 2018.

- 10.12 In some cases, the assurances relied upon are dependent on a specific individual and their ability to ensure their organisation complies with the assurances. Should the political context change, or should key personnel leave post, assurances could become unreliable. SIS keeps this risk under very careful and continuous review and updates the Foreign and Commonwealth Office (FCO) in the event that the circumstances materially changed. We have recommended that SIS ensure they make clear in submissions to Ministers any cases where they judge assurances to be particularly fragile.
- 10.13 In other cases, a material change to SIS's understanding of a liaison partner's behaviour necessitates a review of the assurances which are in place. We are satisfied that UKIC's working practices are sufficiently agile to adapt their assessment as new information or intelligence comes to light.

Caveats

- 10.14 When UKIC or the MOD pass intelligence to a liaison partner in writing, it is common practice to attach a caveat setting out how this intelligence is to be used. Typically, the caveat would instruct that no action (such as arrests and detention) should take place on the basis of the intelligence without first consulting the UK. This is an internationally accepted practice which HMG can expect to be respected. As such, caveats can be an important mitigation of compliance risk associated with sharing intelligence.
- 10.15 Having reviewed the caveats in use across UKIC, we concluded that they are being used inconsistently and risk being counter-productive in some cases. For example:
- GCHQ used some caveats which were not appropriate or not relevant to the liaison partner in question;
 - SIS routinely attached caveats to formal notes passed to liaison partners but these are not always worded in clear English or comprehensible to a non-native speaker, they are translated into the local language in some but not all cases;
 - MI5 has a range of different caveats in use and sometimes applies the incorrect caveat to material passed to liaison partners.
- 10.16 We have recommended that UKIC ensures that any caveats attached to intelligence and passed to liaison are correct and are simple and comprehensible to the recipient, translating these into the local language wherever possible.

Allegations of Mistreatment

- 10.17 On a small number of occasions, UKIC and the MOD were made aware of allegations of mistreatment by a liaison partner in circumstances which engage paragraph 6 of the Consolidated Guidance. In every case, we were satisfied that these allegations were effectively and comprehensively investigated. There were no cases where the investigation concluded that HMG had made a material contribution to any mistreatment which had occurred. In some cases, cooperation with the liaison service was paused whilst an investigation took place; the thorough, impartial nature of the investigation which was conducted in these cases formed a strong evidence base on which to take the decision to resume cooperation with the liaison service in question.

Case study: allegations of mistreatment

In the course of an investigation, MI5 passed intelligence to a liaison partner via SIS. The subject of the intelligence was arrested by the liaison partner in their country. The individual told the British Consular Official that he had been tortured.

The FCO led the response to this allegation and lobbied for further access to the detainee. The FCO continue to regularly access the individual throughout his detention.

With the detainee's consent, the matter was raised with the local law enforcement and relevant government departments in country. The FCO requested an independent and impartial investigation. The issue was also raised at a bilateral meeting by the Prime Minister.

Following a suggestion from the local government, consular staff have also made the individual and his family and legal representatives aware of how they could initiate a formal human rights complaint.

Unsolicited Intelligence

- 10.18 Paragraphs 27 and 28 of the Consolidated Guidance set out the requirements to be followed should UKIC or the MOD receive unsolicited intelligence from a liaison partner where they know or believe that intelligence originates from a detainee and where they believe the standards to which that detainee has been or will be subject are unacceptable. Whilst not formally required to do so by the Consolidated Guidance, UKIC has also considered how to manage the *indirect* receipt of unsolicited intelligence in similar circumstances. We have commended this approach and are pleased that this is another example of where departments have applied the spirit of the guidance to different operational challenges.

Methodology

- 10.19 Following our 2017 report, and in light of the ISC's detainee report, Reprieve, a human rights charity, asked us to clarify our thinking around the details we publish in relation to the Consolidated Guidance. Reprieve asked for additional information and statistics which we are unable to provide because of the sensitivity of this area. The following explanation sets out our response to Reprieve's questions and clarifies our methodology for Consolidated Guidance inspections, which has evolved in recent years and will continue to change in response to the implementation of The Principles, outlined in chapter 2, in 2020.

Q1: Figures for the number of times the Consolidated Guidance was considered, broken down by agency

The Intelligence Services Commissioner previously published statistics for the number of times that the Consolidated Guidance was considered. In reality, this related to the number of times administrative processes relating to the internal policies for applying the Consolidated Guidance had been exercised. The resultant statistics are an unhelpful matrix, further impacted because internal processes have changed substantially in recent years meaning that it is not possible to analyse trends on the basis of these figures. We do not, therefore, believe that publishing these figures would enable the public to understand the level of use of the Consolidated Guidance by the agencies.

We have found that the application of the Consolidated Guidance, and internal policies relevant to detention, are one of the areas of our oversight where UKIC is most collaborative. Because of this, providing individual figures for each agency would be misleading as a representation of how UKIC is working. It is also worth noting that these figures would likely double-count instances of consideration.

Q2: Statistics, per agency, for the number of breaches, or failures to apply, the Guidance

The Consolidated Guidance does not include a requirement to report breaches. The agencies have therefore introduced different methods for identifying and recording instances where they believe the Consolidated Guidance has not been adhered to. These methods have largely related to failures to apply internal guidance and policies, and not to the application of Consolidated Guidance principles in scenarios where there is any assessed risk to a detainee.

Although we have previously received briefings on instances where there has been a failure to act in accordance with the Consolidated Guidance, and at times have noted these in our report, we have not collected statistics in this regard and do not believe that it would be appropriate to do so. In previous reports, we have noted our view that this is a flaw in the Consolidated Guidance and are pleased that this has been rectified in The Principles. We will, therefore, consider how this should now be reported from 2020 onwards.

Q3: Details of each agency's procedures for applying the Guidance (including checking whether it does apply) and escalating decision making to senior officers and Ministers

We have encouraged each agency to publish details of their internal policies and procedures. It would not be appropriate for the Investigatory Powers Commissioner's Office (IPCO) to publish this material while it remains classified.

Q4: The number of times a case considered under the Guidance was referred to a Minister, for each agency, and the number of subsequent Ministerial authorisations, in respect of each agency

This question takes a simplistic view of the authorisation process which would not be borne out through the provision of statistics. In many cases, submissions to a Minister will refer to a programme of work and these may be supplementary to, or combined with, a section 7 authorisation. On selection, we are provided with details on which casework has been referred to a Minister for a decision, and which relate to an existing section 7 submission. In many cases, the submission will be made by SIS, or in tandem by SIS and the MOD such that both Ministers are consulted before action is taken.

IPCO has not, to date, collected figures centrally for this. This reflects the risk-based approach to Consolidated Guidance oversight, which examines submissions to Ministers in the wider context of operational activity and decision making both in country and in the UK. As we discuss the implementation of The Principles, we will consider whether it would be useful to collect these figures. However, we believe that absent detail of the relevant casework, these statistics would not enable members of the public to improve their understanding of HMG's work in this area.

Q5: The number of assurances sourced and received from liaison services, in respect of each agency

We have reconsidered our position in relation to the collection of statistics on assurances and wrote to the ISC in 2019 to clarify that we did not intend to collect or publish details of written and verbal assurances.

Our rationale for this change was based on the following: assurances (whether written or verbal) provided to UKIC by a liaison service are regularly revisited and refreshed. In some cases, UKIC may 're-invoke' verbal assurances with a liaison partner in advance of any operation involving a detention. In others, written assurance may remain in place, unchanged, with a liaison partner for a number of years, save that they are re-sent to relevant senior personnel as their roles change. The existence of assurances is not an automatic 'green light' to progress; rather, the decision to proceed with an operation depends on the considered judgement of officers working with liaison.

Collating the total number of verbal and written assurances UKIC has in place during any given year is not a meaningful measure of UKIC's reliance on assurances as a means of mitigating detainee-related risks. If, as a hypothetical example, SIS involved verbal assurances with a specific liaison ten times in a given year because of a spike in operational activity, including this in an overall figure would risk giving the misleading impression that SIS's reliance on assurance and/or the number of liaisons with whom the operative might have increased, when in fact that was not the case. Furthermore, UKIC have been clear that disclosing the existence of specific liaison relationships would damage national security; this means that it is not possible to publish a statistic which can be broken down to show the extent of UKIC's use of assurances with particular liaison partners.

Q6: The number of authorisations under section 7 of the Intelligence Services Act (1994) made in tandem with cases considered under the Guidance

As noted above in relation to Ministerial considerations, figures in this area risk oversimplifying and therefore misleading the public in the absence of proper context. In particular many section 7 authorisations provide authority to conduct a suite of actions, and conversely section 7 authorisations may be used collectively and in tandem with other authorisations such that one operation of activity may be authorised by multiple authorisations. It is worth noting additionally that the existence of a section 7 authorisation does not discharge the officer's obligations with respect of the Consolidated Guidance, and the officer in the field must be expected to continue to assess and make judgements in relation to the assessment of the risk of mistreatment or torture as the operation continues. Details of how section 7 is used in relation to the Consolidated Guidance are published in the ISC's report following the Detainee Inquiry.

It is worth commenting on the misapprehension that section 7 is used to authorise unlawful acts, including torture and CIDT. IPCO has previously noted that these acts are contrary to International, European and UK law.

Q7: Details of the statistical sampling process, and IPCO's rationale for statistical significance

Previous Commissioners alluded to a sampling process through which a proportion of the 'Detainee Grid' were examined. IPCO's oversight of the Consolidated Guidance does not follow this model and does not seek to review a statistically representative sample of activity relevant to the Consolidated Guidance. IPCO's oversight in this area is risk-based and covers a greater depth of information than was available to previous Commissioners. We have developed a cross-UKIC inspection model which allows us to track through casework between the agencies and to inspect companion documentation at the MOD.

Given the comments above about the inaccuracy of statistics in this area, it would be impossible to set out our oversight as a proportion of the whole. We seek to develop a high level of confidence in the methodology applied in relation to the Guidance, including by challenging the central legal and compliance teams, and at times conduct 'deep dive' reviews of particular cases or stations. We believe that this process gives us a more robust oversight model than would be possible through attempting to identify and examine a statistically representative sample.

11. Law Enforcement Agencies

Overview: Implementation of the Investigatory Powers Act 2016

- 11.1 Throughout 2018 Law Enforcement Agencies (LEAs) were making arrangements for the transition from using Regulation of Investigatory Powers Act 2000 (RIPA) to acquire communications data (CD) and intercept communications, and the Police Act 1997 to conduct equipment interference, over to the Investigatory Powers Act 2016 (IPA). This transition does not introduce new powers but implements safeguards to protect sensitive data and ensure that applications to conduct covert operations are reviewed impartially and independently. This transition has been accompanied by the introduction of new Codes of Practice (CoP), which go further than previous iterations to set out in full how authorities should use their powers and how material should be handled. Our inspections of LEAs have the dual function of ensuring compliance with the legislative framework and providing guidance to users to ensure that best practice is maintained across the UK. This particularly helps smaller users benefit from lessons learnt by larger forces.
- 11.2 The most significant change for LEAs has come in relation to CD, with the creation of the Office for Communications Data Authorisations (OCDA) as set out at paragraph 2.39. Under the guidance of the Investigatory Powers Commissioner (IPC), our Inspectors have been assisting with the training of OCDA authorisers in the run-up to the office taking applications from early 2019. We will cover the implications and first months of OCDA in more detail in the 2019 report.
- 11.3 The IPA also introduces specific safeguards to protect journalistic confidentiality, which means that a Judicial Commissioner (JC) must pre-authorise any application seeking to identify a journalistic source. Additionally, from February 2019 there has been a requirement for LEAs to demonstrate that an investigation for which CD “events” (for example, itemised billing) is being sought meets a new definition of serious crime.²⁸ Our inspections in 2019 will consider whether this definition is being met in all authorised cases.
- 11.4 It is worth noting that two new criminal offences have been introduced by the IPA. The first (section 11) applies to anyone in a public authority who intentionally or recklessly acquires CD without lawful authority; the second (section 82) prohibits anyone working for a telecommunications operator from disclosing the existence of an application to acquire CD. We did not investigate any activity in relation to these offences in 2018.

28 As defined at s.263(1) of the IPA and amended by s.86(2A).

Inspections

- 11.5 Our intention is to inspect all UK LEAs annually,²⁹ and 39 authorities were inspected in 2018. There are two visits to each authority, the first looking at the acquisition of CD and the second looking at property interference under the Police Act, along with Covert Human Intelligence Sources (CHIS) and surveillance activities under RIPA. Where possible, we carry out both inspections at the same time.
- 11.6 In addition, we conducted 46 inspections of renewal of authorisations in respect of 76 relevant sources (undercover operatives) under the enhanced oversight and authorisation regime in Statutory Instrument 2013/2788.

Findings

- 11.7 With regard to CHIS and surveillance under RIPA, we noted, in general, that the existence of experienced and specialist teams is important to establishing and maintaining a good level of compliance. Although standards vary across law enforcement, we are content that appropriate processes are in place and that cases are handled in compliance with the new (CoP).
- 11.8 We have continued to note a good level of compliance across law enforcement in relation to property interference. We made no substantial recommendations in this area in 2018.
- 11.9 We made several recommendations to the intercepting agencies to support the transition to the IPA so that, while maintaining the current high standards, they would be compliant with the new CoP. The majority of our recommendations related to administrative processes and all have now been implemented. There were no themes that caused us particular concern.
- 11.10 We were generally satisfied with the methodology applied across LEAs in relation to CD. We note that the workflow systems currently available should decrease the likelihood of manual errors occurring and have encouraged forces to use these to improve the clarity of their records. In particular, where possible, we encourage Single Points of Contact (SPoCs) to use workflow system functionality to make explicit which data lines will be renewed. It is also reassuring that workflow systems are being used to record urgent oral authorisations; we believe that this approach to maintaining comprehensive records represents best practice.
- 11.11 We have seen some forces introduce a validation check via a second SPoC for applications to resolve Internet Protocol Addresses; given the higher number of recordable errors in this area, we would encourage this practice.
- 11.12 As well as a summary of our findings, the below includes examples of some more specific recommendations to highlight some of the key outcomes from our inspections.

²⁹ Certain inspections were postponed in 2018 owing to: the involvement of Inspectors in the evolution of IPCO; a large number of vacant positions; and the need to train Inspectors in the new Investigatory Powers Act 2016. We deferred inspections which we judged to be lower risk. Those inspections were completed in 2019.

Covert Human Intelligence Sources (CHIS) and Surveillance

11.13 We are content that the standard of compliance with the letter and spirit of the legislation and the CoP is generally good. In recent years, there has been a reduction in the number of authorisations granted in property interference, covert surveillance and CHIS; this has been commensurate with the reduction in the number of staff in proactive and covert units.

11.14 We note that the number of authorised CHIS has declined gradually over the last ten years.

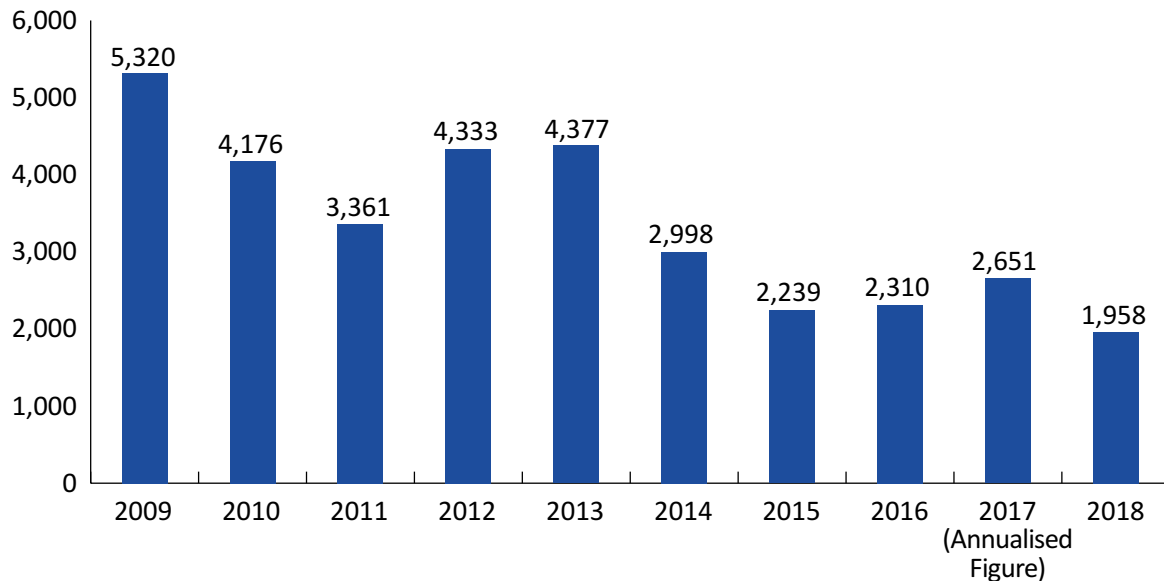


Figure 1: CHIS authorisations made by law enforcement over 10 years

11.15 Information obtained from CHIS is highly sensitive and can be invaluable to law enforcement investigations by providing information that cannot be obtained using other covert tactics.

Example: use of CHIS to progress a criminal investigation

A 'County Line' drugs distribution network was established in a town. An authorised CHIS knew of vulnerable persons being used to sell the drugs on behalf of the organised crime group and was able to provide vital intelligence enabling the police to target the offenders and the premises they were using. Along with the assistance of other covert techniques, the police were able to gather evidence of the drug dealing, safeguard vulnerable young persons being exploited by the gang and successfully prosecute the offenders.

11.16 At each authority, the Central Authorities Bureau (CAB) oversees and quality assures applications, authorisations and associated processes. We found that there is often a lack of consistent standards, or a reduction in standards, at authorities where the CAB experiences more frequent instances of staff change. Similarly, we have seen that the key roles of Operational Security Officers (OpSy), who carry out structured audits and reviews of covert operations and units conducting covert activity, and Senior Responsible Officers (SROs), who act as a strategic compliance lead, can be instrumental to establishing best practice environments. In some agencies, however, staff carrying out these roles also fulfil other duties, which detracts from their positive impact on compliance.

- 11.17 Training is an important foundation for compliance and is often a first step in response to our recommendations. We would encourage a more proactive approach to training, including refresher training for staff in key roles.
- 11.18 As we have mentioned elsewhere in this report, the growth of online activity, particularly in relation to social media, has been reflected in updates to the Covert Surveillance and CHIS Codes of Practice. We have been pleased to note that LEAs have introduced a range of training to allow staff lawfully to exploit this source of information and that this training is available to staff including researchers, analysts, Cyber Crime Units and relevant sources.
- 11.19 Naturally, some agencies have been slower than others in establishing a well-structured, trained, online capability, and in recognising how the use of open source material may meet the criteria for authorisation as directed surveillance or CHIS. We will continue to examine whether the appropriate training and authorisations are in place. In this respect we interview staff involved in online surveillance activity, as well as those in public-facing roles which might incidentally become involved in surveillance.
- 11.20 We have previously made recommendations at specific LEAs seeking to improve the bespoke nature of applications. We are pleased that these have generally been discharged and that applications scrutinised in 2018 did not rely, as before, on generic templates. We have also seen examples of good practice in some LEAs with consistently high standards of record keeping.
- 11.21 We have seen examples of improvements in the documentation of welfare concerns in relation to CHIS in LEAs where this had previously been of concern. With one organisation, where we had previously considered whether the risks to a CHIS from the individuals they were tasked to interact with were adequately considered and documented, we found improvements during recent inspections. However, we still believe there could be greater consistency; this would raise our level of confidence that this matter is considered fully in all cases by those responsible for the CHIS' welfare. We have also noted inconsistencies in other areas, including how contact notes are completed and policy logs used, and we have identified where improvements could be made.
- 11.22 Similarly, our inspection at another LEA addressed the issue of risk assessments for CHIS authorisations. We had previously raised concerns and were impressed by the approach taken to remedy these shortcomings. The authority has standardised its approach, introducing a risk-assessment questionnaire to prompt consideration of specific risks in each case. New methodology for logging and reviewing risks has now been introduced, supported by new guidance for staff involved in overseeing this process.
- 11.23 We previously recommended that one authority should review their processes for oral authorisation of urgent applications. We were concerned that contemporaneous records did not fully capture the required detail and that these were not retained consistently and centrally. The organisation has now established a mechanism for centrally recording and monitoring all urgent authorisations. The records we subsequently reviewed demonstrated that the necessary considerations, including the scope and nature of the planned activity and related intrusion considerations, are now well documented.
- 11.24 We have previously raised some concerns about 'status drift' and suggested that CHIS should be authorised at the earliest opportunity once they have met the statutory criteria. We note that this is at the discretion of the relevant authority but we would expect to see a documented rationale for any prolonged recruitment. In 2018, one authority demonstrated that this question had been thoroughly considered internally and had been the subject of a specific internal programme of work to ensure that officers working within the organisation

are consistent in their thinking and approach. This comprehensive response has given us a high level of confidence in the organisation's compliance with the letter and the spirit of the CoP.

Directed Surveillance

11.25 Directed surveillance covers a range of covert techniques which are commonly used in combination with other tactics. Directed surveillance is used by law enforcement agencies across the range of operations they conduct. Figure 2 shows that there has been an increase in the authorisation of directed surveillance tactics from 2017, reflecting the vital role of surveillance for police across the country.

Example: use of directed surveillance in relation to the investigation of crime within a residential premises with consent from the owner

An elderly person had been the victim of theft of a large amount of money from their home by a 'bogus caller'. It was suspected that the offender may call again at the address, so a covert camera was installed. When the offender did attend the property again, officers recognised the images and arrested him.

11.26 Our inspection of surveillance documentation at one LEA demonstrated a clear and robust authorisation process where all surveillance operations were carefully planned and authorised at the appropriate level. We have commented on an over-reliance on formulaic text, as with CHIS authorisations, but have seen a general improvement and expect this to continue. We have also recommended that surveillance applications ensure that each requested tactic is justified operationally to ensure that all actions authorised are necessary and proportionate.

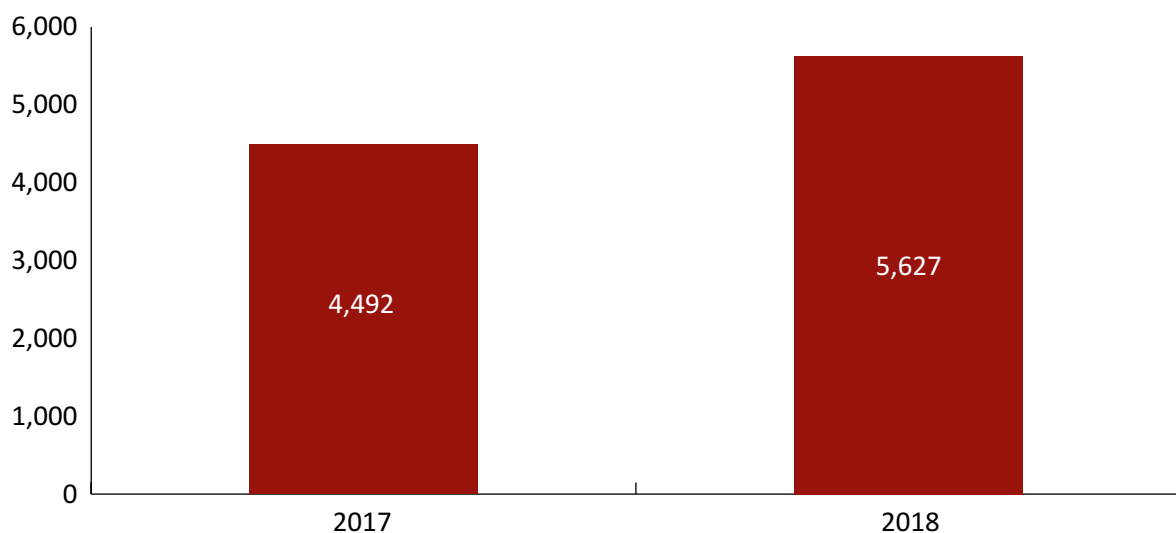


Figure 2: Law enforcement directed surveillance authorisations 2017 and 2018

- 11.27 LEAs currently use a variety of IT systems and hard copy documents to maintain records of applications and authorisations for surveillance. At the time of our inspection, one authority was procuring a new covert management system. We expect to see a reduction in the number of administrative errors in 2019 once this new system is in place.
- 11.28 The standard of compliance in both the applications and authorisations for directed surveillance at one organisation was very good. In particular, we found that Authorising Officers (AOs) made pertinent entries regarding their considerations of necessity and proportionality and made each case bespoke to the crime and subjects in question. However, our inspection at this organisation identified that internal oversight of open source activity was inadequate. We would expect to see significant improvements in this area, including the introduction of internal auditing policies, before the next inspection.
- 11.29 At one LEA, where we had previously expressed concerns that officers were not fully documenting the actions authorised, we found a significant improvement in records kept for urgent oral authorisations. We examined a range of relevant paperwork and we have a high level of confidence that use of the urgency procedures are appropriate and compliant with the CoP. This reflected a significant effort by the force to improve officer training. By contrast, we found shortcomings on another inspection, where the LEA was falling short of the required standard, relying heavily on formulaic text and insufficient proportionality statements. We have recommended that AOs should ensure that the points to cover in the CoP are adequately addressed in each case.
- 11.30 In 2018, Her Majesty's Revenue and Customs (HMRC) informed us of some significant errors, where individuals had been used as CHIS without appropriate authorisation under RIPA and other cases where there had been inappropriate disclosure to defendants regarding persons being authorised as CHIS during prosecution proceedings. We responded to HMRC's reports by conducting a detailed inspection of these cases to ensure that appropriate remedial action was being taken. This inspection, which took place in 2019, noted substantial progress in this area since the error had been identified. We will continue to keep this issue under close review.

Property Interference

- 11.31 Property interference, conducted under Part 3 of the Police Act, includes any interference with property which does not fall under the definition of equipment interference in the IPA. In many cases, the police will conduct these actions overtly under different powers, which IPCO does not oversee.

Example: use of property interference when monitoring a private property or vehicle

A covert listening device was installed in a van belonging to a person suspected of being involved in the importation of counterfeit cigarettes using the cover of a legitimate business. The device gathered evidence of the subject arranging the importation of the cigarettes and the distribution of them within the UK. Evidence from the device allowed the police to confirm that two members of the business were involved in coordinating distribution and were able to use this to progress an investigation into both parties.

11.32 We inspect property interference alongside RIPA powers and generally find a good level of compliance with the CoP. These powers are used less commonly than RIPA techniques but remain a central pillar of our inspection programme. Broadly, the use of property interference authorisations has decreased over the past decade, but it has remained at a similar level in recent years. We would expect this to continue despite the introduction of the IPA, which will include some activities which would previously have been authorised under the Police Act.

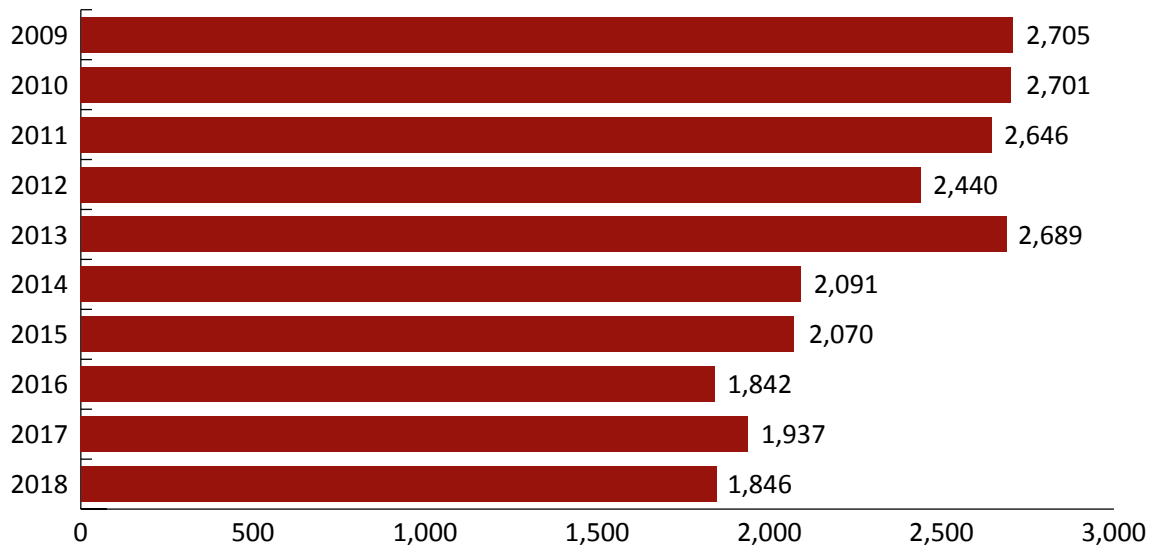


Figure 3: Property interference applications since 2009

11.33 Applications to conduct property interference are routinely reviewed internally by the CAB and the AO, who will be of Superintendent rank, before being presented to the Senior Authorising Officer (SAO), the Chief Constable or Deputy Chief Constable. The quality of documentation is therefore usually consistent and of a high standard.

11.34 Non-urgent authorisations are notified to a Judicial Commissioner (JC) who will, on occasion, raise questions or concerns. We have found through inspections that the SAO and CAB will initiate lessons learnt from any comments they receive and so we have found the judicial review process to be successful in identifying and eliminating minor issues.

11.35 During our inspections, we examine a selection of property interference applications and authorisations. Due to the low volume at smaller authorities, we will often review all such applications on an inspection. This gives the opportunity to discuss issues that may be novel to the authority in question but which we have seen regularly at larger-volume users. This process establishes consistency in approach across law enforcement and gives us a high level of confidence in the level of compliance in place.

11.36 We inspect urgent authorisations, which are normally documented within the LEAs using an urgent oral booklet or similar manual system. We inspect whether the contemporary notes address the necessary statutory considerations, including to document the nature of the interference and the case for urgency.

- 11.37 In an increasing number of authorities, an on-call CAB officer is responsible for documenting the conversation in relation to the authorisation. The SAO will independently take notes of their approval. We have concluded that this approach provides a full and accurate record of the relevant considerations.
- 11.38 We continue to see applications in some authorities that are overly lengthy and will continue to make recommendations in this area. In relation to cancellations we, and our predecessors, have advised many public authorities that a simple confirmation of cancellation is not sufficient and we continue to recommend that further notes should be made on conclusion of any interference, particularly with regard to the product obtained.
- 11.39 We advised one LEA that they should consider conducting more frequent reviews of the use of intrusive surveillance techniques. This would reflect the high level of intrusion resulting from the use of these techniques, as required by the CoP.

Legally privileged material (LPP)

- 11.40 During one inspection, we found processes for identifying and handling LPP material that were particularly notable and gave us a high level of confidence that this sensitive material will be handled appropriately. However, we did note that an AO's comment at review in one particular case was lacking; we would expect the AO to comment on the continuing necessity of obtaining any confidential material. We have recommended that AOs must comment timeously on the acquisition of confidential information, providing their reasons for allowing the continuation of the relevant activity, and that any such acquisition should be notified to IPCO at the start of the next inspection.

Equipment Interference

- 11.41 The IPA introduces the ability for LEAs to obtain a warrant to conduct equipment interference (EI) operations. EI might include obtaining data covertly from a computer or mobile phone, such as the unique identifier for that or other systems data, but cannot include the interception of 'live' communications. This capability is not new to law enforcement and would previously have been authorised as property interference. Since implementation on 5 December 2018, we have seen a small number of applications to conduct EI, which is in line with our previous oversight in this area. The intrusive and technically complex nature of EI means that it is predominately used by the larger LEAs; our oversight of these organisations has demonstrated the success of these techniques, which we are satisfied are being used appropriately. We will inspect the use of EI at the relevant authorities in 2019, focusing on their use of new techniques and on how the safeguards introduced by the IPA have been implemented.

Targeted Interception

- 11.42 Much of our focus in 2018 was to assist and prepare the intercepting agencies³⁰ for the introduction of IPA and transition from RIPA to IPA. Our objective here was to ensure that standards of compliance did not slip during the transition and that the approach taken to IPA warrantry was common across the agencies. The IPA presented an opportunity for us to work closely with the intercepting agencies to make sure key themes of our inspection and previous recommendations were adequately addressed from the outset. This included intrusion into privacy, in particular, and we also focused on the implementation of the

³⁰ As well as MI5, GCHQ, SIS and the MOD, the intercepting agencies are Her Majesty's Revenue and Customs, Metropolitan Police Service, National Crime Agency, Police Scotland, Police Service of Northern Ireland.

enhanced safeguards for sensitive material. We were satisfied that the proposals for new processes were sufficient to comply with the new CoP.

- 11.43 Before the IPA came into force, we reviewed all RIPA documentation at the intercepting agencies. We oversaw the transition process to new warrants with no major issues. In the wake of the transition, we have re-evaluated our inspection model for interception. We have previously scrutinised a high proportion of casework, often significantly higher than other areas of IPCO oversight. With the double lock now in place, however, we do not judge that this is necessary to ensure the basic level of compliance. This has created capacity for us to conduct more probing and broader-scoped inspections, including a more practical in-depth examination of systems and how interception material is used within each agency.

Example: LEAs use of targeted interception in the course of their investigation:

An LEA becomes aware that an organised crime group is importing drugs to the UK via a European port. The investigation identifies some members of the group based in Europe and their contact in the UK. The law enforcement officers discover that this individual is planning to bring a shipment of drugs into the UK over the weekend and identify a mobile telephone number for him. The officers are aiming to identify the group's plans to move the drug shipment, so that they can seize the load before it comes into the UK and is sold on illegally.

The mobile number is placed on targeted intercept cover by way of urgent authorisation. As a result of this, and other covert tactics, the location of the illegal operation is identified. Law enforcement officers take action and the drugs are seized. The officers are able to make a number of arrests. The operation stopped the drugs from being sold in the UK and a number of dangerous individuals are now subject to criminal justice outcomes.

- 11.44 During our inspections, we examined modifications and cancellation documentation and processes. This enabled us to confirm whether interception was concluded when the intelligence obtained was no longer necessary and proportionate. There are new processes under IPA here and this is an area of work in progress, although we have not identified any issues for concern. We also inspect documentation in relation to urgent applications. Although these applications are reviewed retrospectively by the JCs, we consider whether the current records were adequate and test whether the case for applying urgent procedures is appropriate.

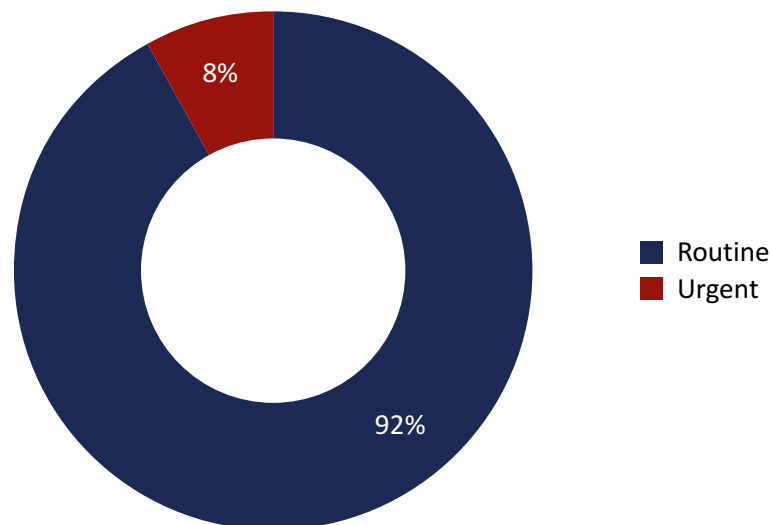


Figure 4: Proportion of urgent and routine interception authorisations, LEAs, 2018

- 11.45 The records scrutinised at each agency were of a high standard. However, we have continued to make recommendations in relation to the articulation of collateral intrusion. Our inspections have previously noted that intrusion, and particularly collateral intrusion, can change during the life of a warrant, but that this change is not always well articulated on the casework. As an example, we questioned the language used to characterise intrusion, which we were concerned might be formulaic and did not always demonstrate the necessary consideration of the intrusion likely to occur in the case to be authorised. We have recommended that bespoke considerations should be recorded in every case.
- 11.46 During previous inspections at one organisation, we raised concerns about delays in suspension of interception of specific communications. We saw significant improvement in this area and were pleased to examine records demonstrating timely and appropriate cessation of interception. However, we still identified a small number of instances where interception has continued for longer than was necessary. We expect to see further improvement in this area in 2019.
- 11.47 The transition to the IPA, and technical developments in recent years, have complicated the landscape for interception, placing an obligation on each agency to update policies, processes and systems to meet changing requirements. We have been impressed by the proactive approach taken by the intercepting agencies to meet this challenge and have a great deal of confidence that the new processes will ensure a high degree of compliance with the IPA once warrants are transitioned and the new Act is in force.

Legally privileged material

- 11.48 The IPA introduces the requirement for the requesting agency to assess the likelihood of obtaining legally privileged (LPP) or confidential material, and to state if this is the purpose of the operation. Our inspections scrutinise whether the basis of these assessments is appropriate and whether the likelihood of obtaining LPP or confidential material is being accurately described to the Secretary of State and JC considering the warrant. In general, we have found that the assessments made were accurate and thorough.
- 11.49 On inspections, we conducted searches on workflow systems, which are used to track and retain interception material, to identify the existence of LPP and confidential material.

At each agency we confirmed that this sensitive material is appropriately handled and that staff are knowledgeable in relation to the requirements and restrictions under the IPA. One agency has implemented a new process of regularly reviewing the presence of potentially privileged material across all live operations. We noted that this comprehensive approach established a high level of confidence that all relevant material is being identified and handled appropriately. We have highlighted this approach as best practice to other agencies.

- 11.50 Conversely, one of our other inspections found processes that could be developed further with regards to identifying and tagging LPP material and which would benefit from a more refined monitoring process. In general, intercepting agencies take a cautious approach to LPP material, including reviewing any material which has the potential of including privileged material. However, we did find some instances which did not appear to have been identified and recommended a review of the system used for highlighting potentially relevant material. The authority concerned has demonstrated significant improvement in relation to our recommendations and we do not expect to see these shortcomings at our inspection in 2019.
- 11.51 We noted that each agency took a thoughtful and appropriate approach to handling LPP material. During one inspection, we discussed the definition of individuals working within the legal profession, which is set out by the IPA and the CoP, to ensure that the scope is taken to include those working in a legal capacity alongside advocates, solicitors and barristers. We agreed with the approach taken, which is to treat communications to and from paralegals, and others working at the direction of and under the supervision of an advocate, solicitor or barrister, as potentially privileged too.

Additional targeted interception and targeted examination provisions s17(2)

- 11.52 As detailed in chapter 2, the IPA sets out provisions to obtain warrants to interception communications for a group of persons, more than one organisation or a set of premises. The transition from RIPA to IPA was late in the year for LEAs; we intend to inspect their internal processes and reliance on this provision in 2019.

Communications Data

- 11.53 Communication data (CD) is used by police and law enforcement agencies across a wide range of investigations. The majority of applications to acquire CD are made for the prevention and detection of crime, with the second largest category being in life at risk situations, such as high-risk missing persons. In more straightforward cases, a single item of CD may be all that is required, for example to corroborate the account of a witness who has been sent a malicious or threatening communication. In more complex investigations, multiple strands of communications data need to be acquired and analysed to establish patterns of contact and movements between groups of organised criminals or terrorists, identify potential suspects in a murder or kidnap, or quickly to locate dangerous and violent offenders.
- 11.54 The term 'communications data' refers to the 'who', 'where', 'when' and 'how' of a communication. It does not include any of the content within a communication such as text, audio, video or other images and therefore cannot establish what was actually said or written. Most requests for CD relate to information held by telecommunications operators (for example, Vodafone, BT and O2), including the time and duration of a communication, the telephone number or email address of the originator and recipient, or the location of the device on which the communication was made or received. CD covers electronic

communications including internet access, internet telephony (for example, a Skype call), instant messaging and the use of applications, but also includes communications sent through postal services such as the Royal Mail.

Case study: how CD can be used

Counter Terrorism Police were engaged in an investigation into the transporting of individuals into the UK who were believed to be linked to terrorism. A team were tasked with locating a particularly dangerous individual believed to be at large. He was suspected as having links to a proscribed organisation and his current address and location were unknown. Work with the NCA and Interpol showed that this male was wanted for a grievous bodily harm (GBH) with intent offence (stabbing) overseas.

Internet and intelligence investigations identified online accounts that were suspected of being used by the suspect. A communications data investigation was then used to identify a number of means of communication used by the suspect in the UK. As a result of communications data analysis, used in conjunction with other digital opportunities, a lifestyle pattern was produced and a number of addresses were identified.

Utilising the data available, the subject was located, arrested and extradited to face trial.

11.55 As the figures in this section demonstrate, the vast majority of CD requests are made in relation to suspects of an investigation, but there are occasions where an LEA will seek data relating to a victim, witness or vulnerable person. The highest proportion of CD requests relate to telephony. The data obtained by law enforcement related to subscriber details and traffic data in most cases.

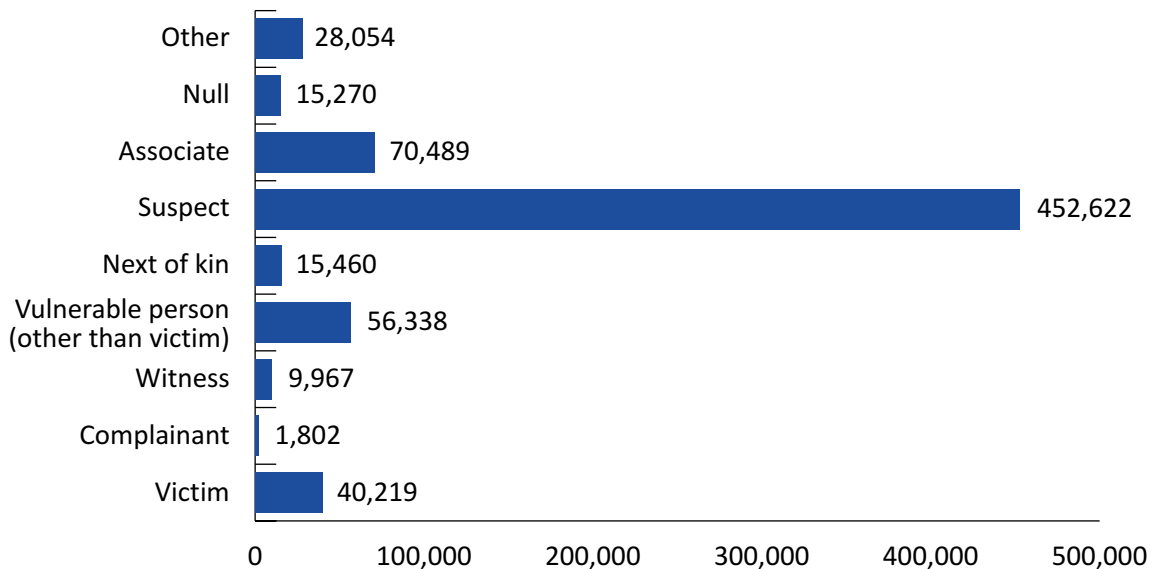


Figure 5: Communications data items by relevant individual, 2018

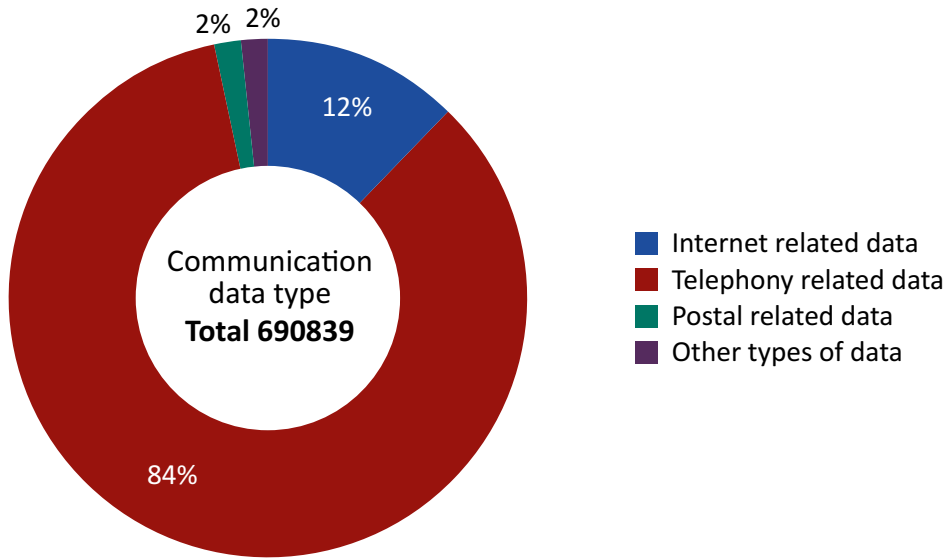


Figure 6: Communications data by communication type, 2018

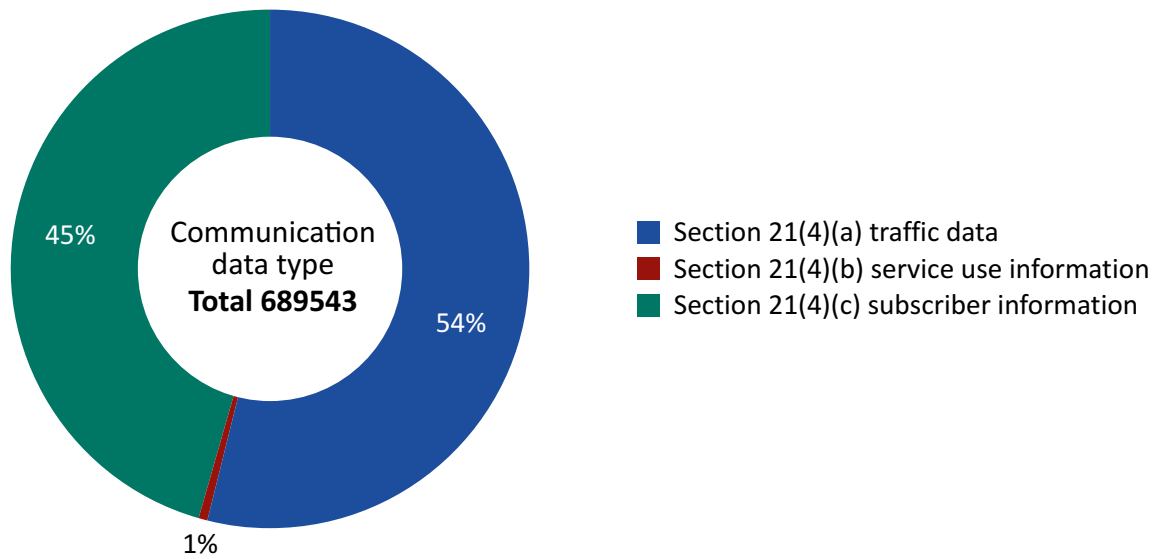


Figure 7: Communications data by data type, 2018

- 11.56 In advance of the transition to independent authorisation by OCDA in 2019, we made several recommendations to ensure that the requirement for independent scrutiny of authorisations was upheld and that an independent designated person reviewed all applications for CD. This was to ensure compliance with the relevant CoP.
- 11.57 We inspect Professional Standards Departments and Counter-Corruption Units within police forces in relation to their use of CD. These units are unique in their role and it is essential that this is recognised when applications are made to obtain intelligence for the purpose of progressing internal, non-criminal, investigations. We recommended that applications from the Counter-Corruption Unit or Professional Standards Department must be explicit as to the nature of criminal conduct under investigation, acknowledging CD can only be acquired for the core function of prevention and detection of crime, and not for the ordinary function of discipline. In some cases, we were concerned that forces were

obtaining data otherwise than for the purposes made available to them by the CoP. We will monitor whether any further instances of this activity occur in 2019.

- 11.58 Another focus of interest during our inspections is the application of emergency provisions. We scrutinise a higher proportion of urgent casework processed at LEAs, to ensure that the requirements of the CoP are met and, specifically, that the exceptional nature of the urgent requirement is clearly articulated on the current records. Because urgent applications will continue to be conducted independently of OCDA, we will again review a high proportion of urgent authorisations in 2019. We have recommended that steps should be taken to ensure all applications submitted as National Priority Grading Scheme 2 comply with the CoP and provide a clear explanation of the exceptionally urgent operational requirement.
- 11.59 We also considered the adequacy of provisions to ensure that the minimum necessary intrusion is made into a target's privacy and made a number of recommendations in this regard. We have suggested that applications seeking data over an extended date range, such as those targeting organised crime groups, should set out how the data will be used and why a shorter period would not meet this requirement.
- 11.60 In one instance, we made a recommendation in relation to the articulation of statutory purpose. The IPA introduces an increased focus on the purpose of obtaining intelligence, which is a means of safeguarding data from misuse or use other than the intended purpose. In some cases, we judge that additional training for staff would improve the consistency and accuracy of records. We believe in this case that the training or guidance given to applicants should be reviewed to ensure the distinction between the statutory purposes of applicable crime, non-crime emergency welfare provisions, and that for identifying persons who have died or are incapacitated, is properly understood.
- 11.61 Our inspections seek to confirm that the AO in each case is independent from the operation. This is a requirement of the CoP intended to ensure that the authorising individual's scrutiny is objective. We have seen good evidence of this practice on our inspections but, at one authority, we made the specific recommendation that the authorising individuals should give greater consideration to the specific details of the application at hand when completing their comments.
- 11.62 We noted at a different authority that applicants were able to select an AO when submitting their application. This gives the option, technically, for the application to be considered by one involved in the case. The applications selected for examination did not identify any examples where this system has been abused but we have recommended that the SRO must ensure that processes are followed to eliminate this possibility.
- 11.63 We saw good practices in the casework we scrutinised at one interception agency, which documented bespoke considerations of the relevant details in each case. They demonstrated well established practices for ensuring the independence of the AO but, at some points, this has resulted in significant delays in obtaining the required data. We advised that they could consider a more flexible approach without compromising independence. In previous years, we have made recommendations to this topic at other organisations and have seen improvements in efficiency as a result.

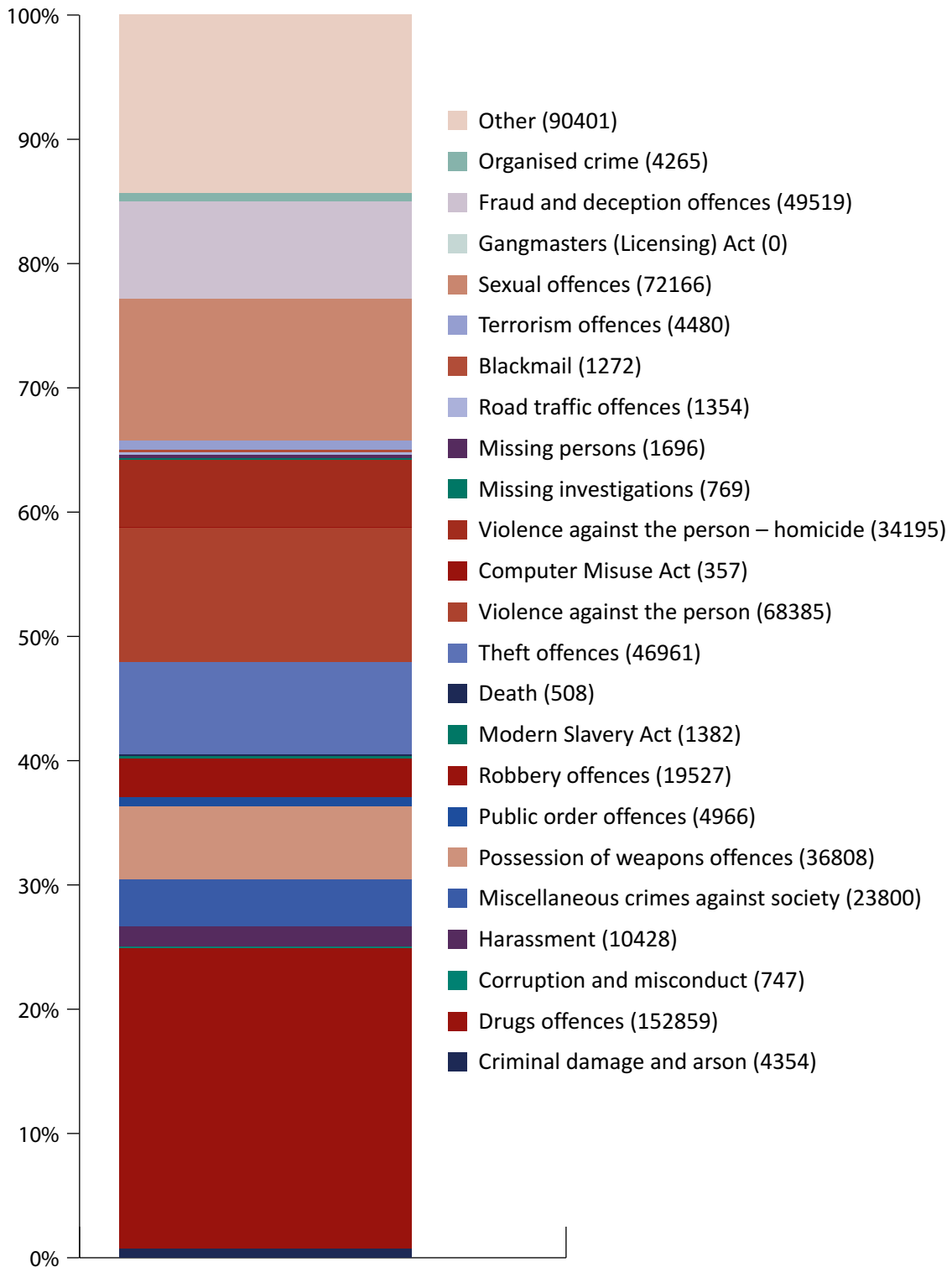


Figure 8: Communications data applications by offence, 2018

11.64 We found a small number of instances of non-compliance with independence on another inspection. We expect that changes in policy and process, together with the implementation of OCDA, will see this practice eliminated.

- 11.65 We found exemplary practice in relation to sensitive professions in two agencies. The SPoCs conduct regular audits of all relevant applications to ensure that sensitive casework is properly identified and set out in applications. We reviewed results from these audits and found them to mirror our own processes and considerations.
- 11.66 In those organisations where CD is acquired in support of warranted investigations, it was apparent that confusion has arisen from historical practices as to whether, and in what circumstances, such data should be acquired under Part I RIPA (Section 20), or by way of an application under Part I Chapter 2 RIPA. We made a recommendation for one organisation to tighten processes and assist the public authority to achieve the best possible level of compliance with RIPA and the CoP. This issue has also been the subject of further discussions with the Home Office Policy Unit to ensure that the guidance in this area is clear and compliant and revised legislation, with appropriate interpretation, is to be introduced under the IPA in 2019.

Sensitive Professions

- 11.67 During our inspections, we review applications relating to individuals of sensitive professions and consider whether the relevant safeguards are being applied appropriately. We had no concerns that the relevant data was being obtained unnecessarily but in some cases the records did not fully reflect the sensitivity of this data. We recommended that within all applications linked to sensitive professions, the applicant, the SPoC processing the application and the Designated Person granting the authorisation, must include an assessment of whether the data being sought is likely to involve a higher degree of interference with an individual's human rights, whether there might be any unintended consequences, or whether the public interest is best served in the application.
- 11.68 On previous inspections at two agencies, for example, we had noted shortcomings in relation to the enhanced considerations of privacy that are required when dealing with applications relating to certain sensitive professions (such as lawyers and doctors). Our 2018 inspection found a good level of compliance with the provisions of the CoP in this area, resulting from improved internal processes.
- 11.69 We conducted two inspections of one agency in 2018. Our first inspection similarly identified shortcomings in relation to sensitive professions. The CoP requires that the application should state if the data requested is relevant to a sensitive profession, if known, and that the person granting the authorisation should consider whether the request is appropriate given the sensitivity of the material intended to be acquired. We have seen some progress in this area, although we found that the depth of considerations offered were inconsistent. This is not to say, however, that this sensitive material is not lawfully obtained nor appropriately safeguarded upon receipt. We expect to see further improvements in this area in 2019.

Protected Information

- 11.70 LEAs may require the disclosure of the protected information, which they have lawfully obtained or are likely to obtain lawfully, in an intelligible form or to acquire the means to access the information. The National Technical Assistance Centre (NTAC) is the lead national authority in relation to this form of activity and approval must be granted by NTAC to any LEA seeking to obtain to exercise these powers. The usage of the powers is infrequent, with 66 approvals granted in 2018.

12. Public Authorities

Overview

- 12.1 A number of public authorities, in addition to Law Enforcement Agencies (LEAs) and local councils, have the statutory power to use covert tactics. We refer to these authorities as Other Public Authorities (OPAs) and include a list at Annex A. Their powers vary according to the relevant Acts in which they are named.
- 12.2 OPAs are able to authorise the use of directed surveillance and communications data (CD) and many can also authorise the use of Covert Human Intelligence Sources (CHIS). A small number may also apply to conduct property interference³¹ and intrusive surveillance.³² As with all authorities, the regularity and pattern of use varies dependent on the powers available and the investigatory function of the relevant authority.
- 12.3 Examples of the investigatory functions of these public authorities include: to investigate and prosecute breaches of company and insolvency legislation; fraudulent benefit claims; preventing immigration abuse; regulating activities that can cause harmful pollution; the regulation of medicines, medical devices and equipment used in healthcare; and investigation of unregistered schools.
- 12.4 In 2018, we inspected nine public authorities: the Department for Work and Pensions (DWP); the Home Office Immigration and Enforcement Directorate (HOIE); the Department of Health and Social Care – Medicines and Healthcare Products Regulatory Agency (MHRA); the Office of The Police Ombudsman for Northern Ireland (PONI); the Insolvency Service; the Scottish Environmental Protection Agency (SEPA); Transport Scotland; the Competition and Markets Authority (previously the Office of Fair Trading); and Her Majesty's Chief Inspector of Education, Children's Services and Skills (OFSTED).

Findings

- 12.5 In general, we found the level of compliance to be good at the public authorities who had used their powers. We noted that the officers involved in this work were experienced, often taking up these posts following careers in law enforcement. However, we commonly made two recommendations: first, to ensure that the activities to be conducted were clearly and explicitly set out and, secondly, that records of meetings with CHIS should be better. We will keep both of these issues under close review in 2019.

31 Property interference can only be authorised by the Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), Police Investigations and Review Commissioner, or Home Office.

32 Intrusive surveillance can only be used by the Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), Home Office (for customs and immigration matters only) and the Ministry of Justice and Northern Ireland Office (in both the latter cases, for activity in prisons only)

Covert Human Intelligence Sources (CHIS) and Surveillance

- 12.6 The powers available to each authority have been determined by a careful process of analysis and consideration before ratification by Parliament. However, there are some instances where changes in culture, technology, trends in illicit behaviours, or reallocation of public responsibility, will mean that the available powers do not necessarily align with an authority’s investigative requirements.

- 12.7 In some cases, we have been persuaded that it would be appropriate for specific authorities to have wider powers, for example to allow them to conduct property interference operations to support an existing investigative function. We have recommended that one organisation, the MHRA, should discuss this issue further with the Home Office, who are responsible for reviewing the function of the legislation and may be in the position to recommend an amendment to the legislation to support this change.

- 12.8 Another organisation, OFSTED, which had not made use of its directed surveillance powers for many years, had been considering seeking its removal from the Regulation of Investigatory Powers Act 2000 (RIPA) schedule following its last inspection. However, a surge in the type of activity, which it is there to protect against, prompted a change in view. We were pleased to see that OFSTED had invested in training and updated policies, despite the lack of use, leaving them prepared for the surge.

- 12.9 In general, however, we have seen an increase in the use of directed surveillance powers on 2017.

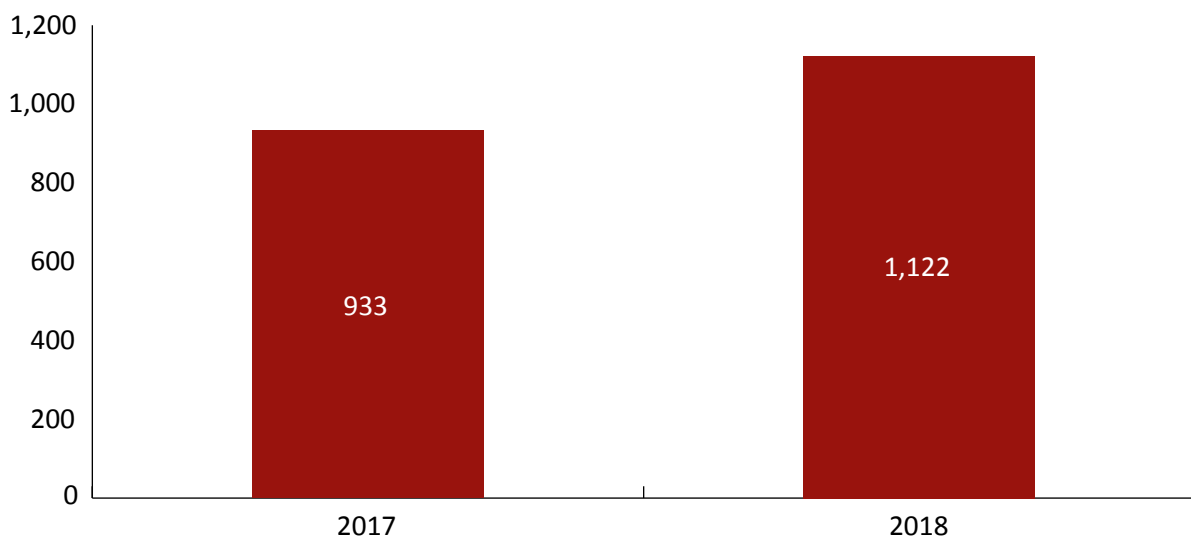


Figure 9: Directed Surveillance Authorisations (DSAs) 2017-2018

- 12.10 At our inspection of one public authority in 2018, we saw a particularly good demonstration of necessity and proportionality consideration in the use of DSAs. We did not inspect any renewal documentation, because the authority had ceased surveillance in each case at the earliest appropriate opportunity. They have worked to raise the level of awareness and communication as part of an ongoing compliance strategy; notably, they have introduced a monthly newsletter from the Covert Authorities Bureau (CAB) to keep colleagues updated on RIPA issues and help raise the profile and availability of the CAB for internal advice. We are encouraged by this approach to compliance culture and would encourage similar initiatives to be introduced elsewhere. Our inspection found that management of online research into suspected fraudulent activity, undertaken by a dedicated team of trained

officers, demonstrated the success of previous training programmes; officers were well aware of when a RIPA authorisation might become necessary and how to authorise their actions. Elsewhere, we have commonly made recommendations that all staff should receive enhanced training so that they recognise when online activities, particularly social media research, would constitute surveillance.

- 12.11 We were impressed with the RIPA and open source training programmes undertaken by a number of organisations in response to previous recommendations.
- 12.12 We have often found applications and review casework in public authorities to be long-winded, and not focused clearly on the central considerations. We have continued to see casework that is often formulaic and does not pay sufficient regard to the specifics of the case being considered. We have recommended that documentation should be succinct and bespoke, which would give us a higher level of confidence that the Authorising Officer (AO) has considered the key elements and has an accurate understanding of the anticipated level of interference with privacy.
- 12.13 However, we have also seen evidence of high standards of compliance in the management of CHIS and undercover officers in certain organisations. However, we were concerned that some public authorities showed a lack of understanding of when a member of the public or other informant should be considered a CHIS. We believe that this is particularly important for organisations that do not have the power to authorise use of CHIS and must therefore not establish covert reporting relationships. We have suggested that, irrespective of their power, a public authority has a duty of care towards any individual that provides them with information on which they might later act, and therefore ought to have in place a system of recording such details as would enable them to assess whether the status of the informant has drifted. We were pleased to see that some authorities had established a system to regularly review the status of individuals providing information.
- 12.14 At the end of 2018 we received a report of a potential error which we investigated and will therefore report in more detail in 2019. An authority reported that they had been receiving intelligence from an individual, who had not been authorised as a CHIS, since 2017. While there is no obligation, legally, to authorise an individual as a CHIS, in this case the nature of the relationship was such that we would have expected the activity to have been authorised and managed under RIPA. Our inspection raised wider concerns, which we expect to be remedied over the coming year.
- 12.15 As shown in figure 23, use of CHIS has generally fluctuated in recent years, but we saw little change from 2017. The public authorities continue to be relatively low users of this tactic and we expect this to continue over the coming years.

Communications Data

- 12.16 These public authorities are generally low users of communications data (CD) powers. The processes they follow are the same as those undertaken by local authorities. Some authorities have their own staff trained as accredited Single Points of Contact (SPoC) to acquire data from telecommunications operators, whilst others utilise the centralised services of the National Anti-Fraud Network (NAFN), which is described further in the next chapter in line with others from 2019. Public authorities will be required to apply for communications data by independent authorisation via the Office for Communications Data Authorisations (ODCA).

12.17 Our inspections at the most common users of CD generally noted a high standard of compliance and we made no recommendations. In respect of the application records we sampled, we were satisfied that the documentation reflects the complexities of their investigations and justifies the principles of necessity, proportionality and collateral intrusion. We were similarly satisfied that the appropriate threshold was maintained in relation to investigating criminal activity, as distinct from internal disciplinary matters.

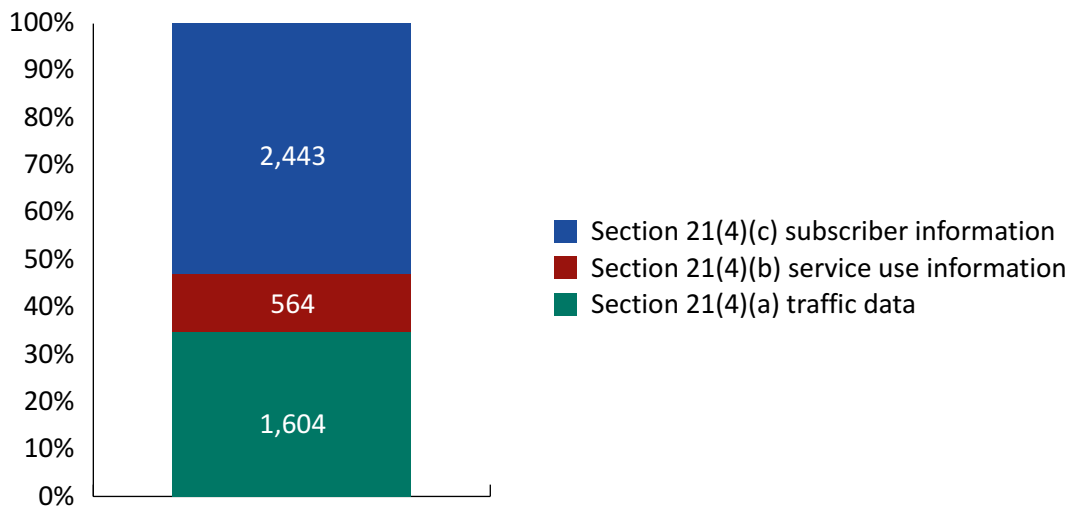


Figure 10: Communications data by type for Other Public Authorities (OPAs), 2018

12.18 The majority of communications data requests from public authorities were for subscriber information. This request would seek to identify the user of a telephone or email address, for example. The statistics show that 89% of communications data items obtained related to telephony and that in 96% of cases, the applicant identified the subject of the request as the suspect of their investigation.

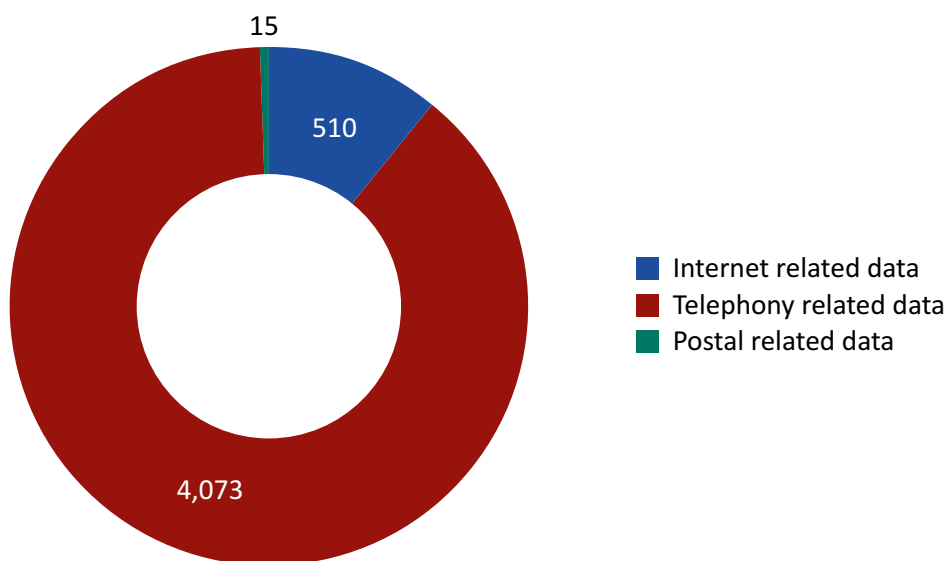


Figure 11: Communications data items by communications type, 2018

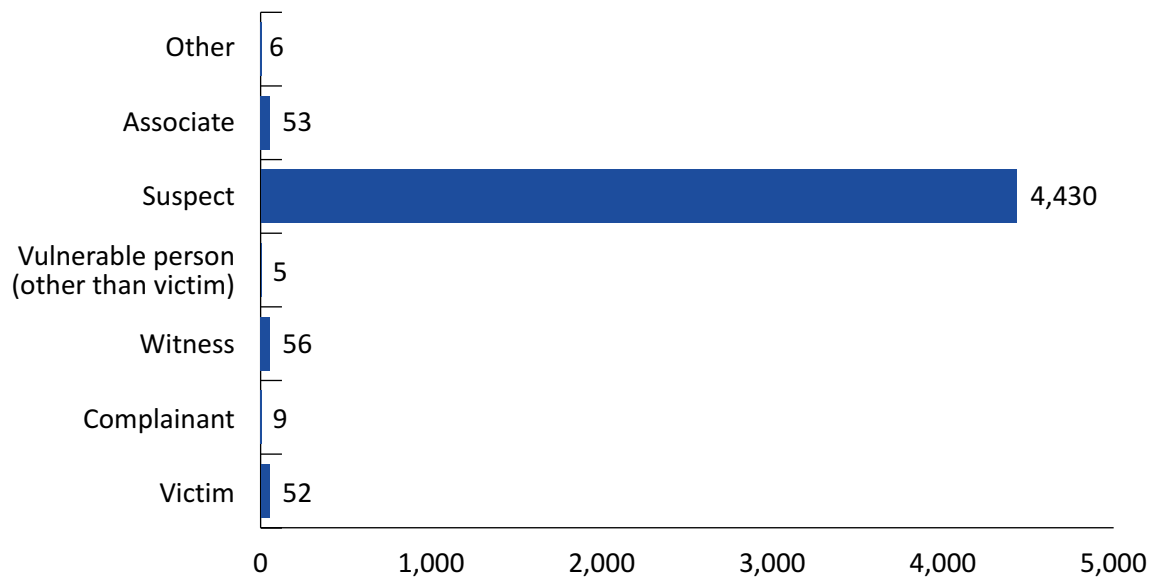


Figure 12: Communications data items by relevant person, 2018

13. Local authorities

Overview

13.1 Our work with local authorities differs from that with other public bodies and law enforcement because of the infrequent use of powers. While there is little risk of any large-scale abuse, which we work to prevent through our oversight of more regular and bulk users, there is a substantially higher risk of inadvertent unlawful activity. At local councils, workers are routinely engaged in activities which look into the lives of the public, increasingly via social media interactions. This means that part of our role is to ensure that these everyday interactions are appropriate and are compliant with the legal framework. For this reason, we carry out a dual function with regard to local authorities: first, inspecting the recorded use of covert powers and, secondly, investigating the culture and practice across the organisation to establish a level of confidence that any who need to use covert powers would be recognised by staff and would be properly authorised.

13.2 In 2018 we conducted:

- 90 local authority inspections, 35 on site and 54 remotely (in one instance, a remote inspection was followed up by a visit);
- 1 extraordinary inspection where we had previously noted poor compliance; and
- 5 Fire and Rescue Services inspections, 4 on site and 1 remotely.

In 2018, 42 local authority inspections were postponed until 2019 due to a scarcity of Inspector resources while the focus was on transitioning to the Investigatory Powers Act 2016 (IPA). We are increasing this work again during 2019 and hope to get back on schedule by 2020.

13.3 In recent years, our inspections at Fire and Rescue Services have confirmed that they are not using covert powers. This reflects a change in the nature of their work and collaborative approach with other organisations which renders it unnecessary for Fire and Rescue Services to use these powers. We do not expect this to change in the future. The Home Office is currently reviewing whether it would be appropriate to revoke their inclusion on the Regulation of Investigatory Powers Act 2000 (RIPA) schedule, effectively removing those powers. Until this issue is resolved, or we are notified of a change in practice, the Investigatory Powers Commissioner (IPC) has decided that we will not conduct further inspections of Fire and Rescue Services.

Findings

13.4 We have continued to see a decline in the use of covert powers by local authorities. At one end, we inspected one council which had approved 56 directed surveillance authorisations and 26 Covert Human Intelligence Sources (CHIS) authorisations in the period between their previous inspection and the 2018 inspection. However, at most there had been no

use of covert powers during that three-year period. We have identified several causes for this decline including, but not limited to, benefit fraud now being investigated centrally by the Department for Work and Pensions (DWP), and councils favouring overt investigations and/or working with local police forces to investigate criminality. In addition to this, we believe that resource limitations are impacting the use of covert powers and several councils have suggested that the introduction of the Protection of Freedoms Act 2012 has been a contributing factor. We have heard that the requirement to obtain the approval of a magistrate can be seen as a hurdle, rather than an appropriate safeguard. We are concerned that councils have found these changes in culture and legislation to be prohibitive and the IPC has been keen to encourage the continued use of covert powers which have been placed on statute to enable public authorities to undertake surveillance to fulfil their civic responsibilities for the local community in this context, it is worth noting that our findings in Scotland, where sheriff approval is only necessary for communications data applications (see below), show more regular use of RIPA powers by all five councils we inspected in 2018.

- 13.5 We examined the RIPA records in place at each of the authorities we inspected. The most common recommendations were that Authorising Officers (AOs) should clearly articulate their considerations in relation to necessity, proportionality and collateral intrusion and that any CHIS application should be accompanied by an appropriate risk assessment. A risk assessment should allow the AO a clear route to assess the risk in relation to deploying that particular individual as a CHIS. This was not always possible from the casework we reviewed. We also often recommended that councils should remove any remaining references in their policy documents to use of the urgency provisions where these were no longer available; this provision was removed by The Protection of Freedoms Act 2012. In general, however, we were satisfied that records were well kept and that the necessity of conducting the proposed action was clear.
- 13.6 We identified a handful of examples where records were inadequate but do not meet the threshold for an error.³³ By way of example, these included:
- In one case, the identity of an authorised CHIS had been changed during a review (because the activity had been undertaken at different times by two members of the council's relevant department). A CHIS authorisation relates to a specific individual source who may only be changed by a process of cancellation and fresh authorisation; and
 - In a second example, an authorisation was granted for the investigation of offending which failed to meet the penal threshold for directed surveillance. This meant that the activity did not carry the protection afforded by RIPA. This highlighted a requirement to identify clearly the offence being investigated and its maximum penalties in each application.
- 13.7 We concluded that the standard of CD applications being produced by local authorities was good, despite Special Points of Contact (SPoCs) returning 91% of all applications on at least one occasion for further development or additional information. We are content that this process demonstrates a conscientious approach and reflects the infrequent use of CD applications by local authorities.
- 13.8 We made no recommendations in relation to the use of CD by local authorities in 2018.

³³ Note that Section 80 of RIPA sets out that authorities are not required to obtain authorisations under RIPA to make these activities lawful.

Covert Human Intelligence Sources (CHIS) and Surveillance

13.9 Local authorities are able to authorise the use of directed surveillance and CHIS under RIPA for a range of purposes. These can include: to identify those responsible for environmentally damaging fly-tipping; to identify those who may be causing major criminal damage to council property or that of local residents; the unlawful sale of alcohol or tobacco to minors; or to detect serious fraudulent activity.

Example: use of CHIS and surveillance

A local authority was experiencing a spate of thefts from pay and display parking meters and after some initial analysis of the crimes installed covert CCTV cameras at locations where it was believed the offenders may strike again. Within a week images of the offenders and the vehicle they were using were captured. The evidence was passed to the police who arrested and prosecuted the offenders.

13.10 In Scotland, which has additional grounds available to local authorities, directed surveillance could be used to detect the sale or preparation of meat unfit for human consumption, or practices by landlords that place tenants at risk in terms of their safety.³⁴

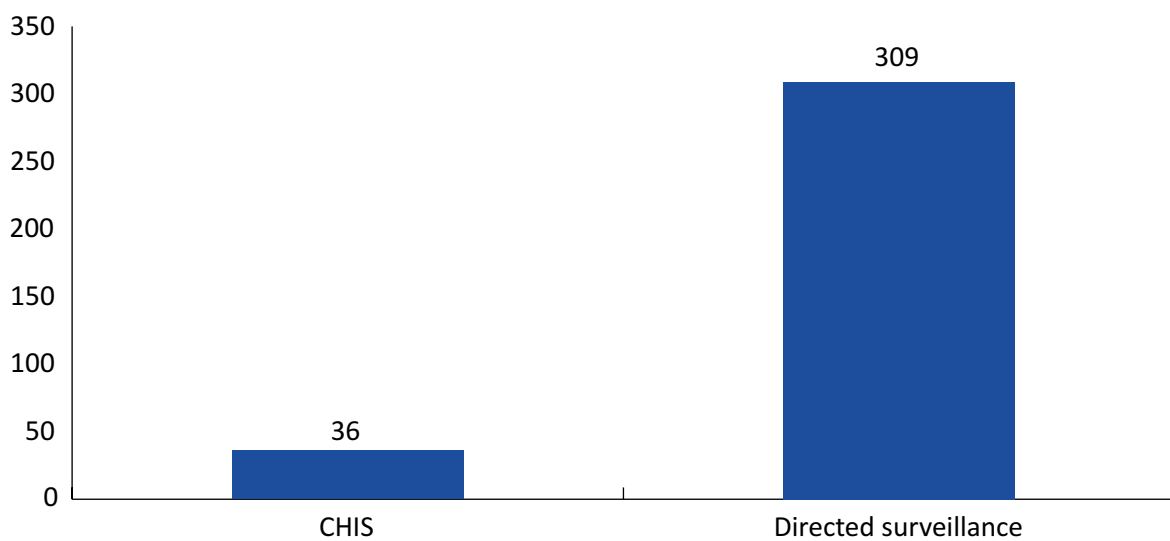


Figure 13: CHIS and directed surveillance authorisations by local authorities in the UK in 2018

³⁴ These scenarios are by example only.

Case study: inspection

We had noted poor compliance standards in a local authority. In this case, the recommendations from our previous inspection had not been discharged appropriately. We noted that the corporate oversight was almost non-existent. From our initial inspection, we were not confident that covert tactics ought to have been used in certain scenarios, or that they had been properly authorised.

Our second inspection, however, found a refreshed approach to the management, training and ongoing oversight of the RIPA processes. We examined a new authorisation, which we judged to demonstrate the council's confidence to appropriately and compliantly use RIPA powers. The authorisation was for a Trading Standards officer to act as a CHIS.

We made suggestions for improvement in relation to the casework but were satisfied that the investigation was appropriate and that the CHIS was properly authorised.

13.11 We have been disappointed that responses to desktop inspections have occasionally been late or incomplete. Perhaps unsurprisingly, we have found that respondents who are newer in role, and those working at authorities which use the powers infrequently, typically provide less clear and comprehensive responses than others. However, this limits the level of confidence we have in those authorities; we believe that those authorities that do not regularly engage with oversight are more likely to establish poor or inefficient compliance practices in the future. In 2018, we conducted one physical follow up to a remote (desktop) inspection because we were not satisfied that the response given demonstrated adequate compliance.

13.12 The use of directed surveillance has increased marginally in 2018 across local authorities, as shown at figure 14.

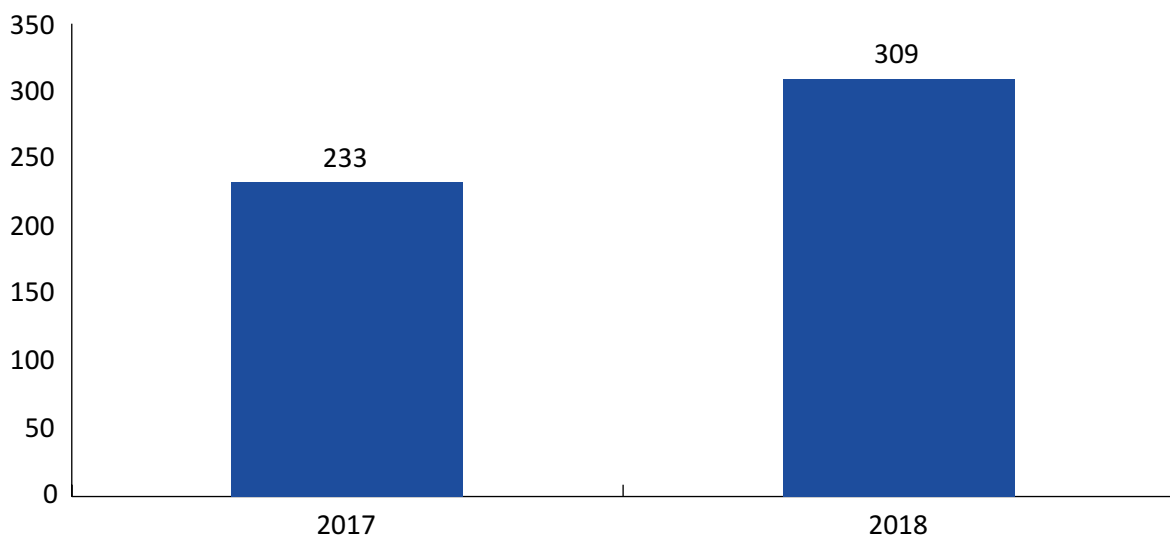


Figure 14: Directed surveillance applications made by local authorities in 2017 and 2018

- 13.13 In 2018, we focused on the use of social media as part of investigative or enforcement activities. We have found that some councils have updated their RIPA or Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) policies to include sections on social media, whilst others have added an annex. In many cases, this has reflected the text of the August 2018 Code of Practice (CoP), which we encourage. We have commended programmes to raise awareness of the challenges of working with social media; these have variously included intranet information bulletins and internal training updates. However, we have seen that this approach is not universal and some authorities are yet to recognise the implications of social media for their work, both in terms of opportunities and limitations. We are also concerned that awareness programmes and policies can sometimes only consider 'key departments' and do not consider the less obvious ways in which their staff may interact with social media. For example, officers working in the areas of childcare, school exclusions, elderly and social care provision and human resources can inadvertently become involved in activities which constitute surveillance. This means they need to be clear on the legal frameworks which govern their work. We will continue to focus on this area in 2019, to ensure that councils are adhering to the relevant guidelines and are considering the implications of retention for any data they obtain in the context of increased public interest and concern about access to private data.
- 13.14 We are conscious that providing training for staff not directly involved in surveillance or CHIS activities may appear to be an unnecessary cost for councils. However, we have noted that inexperienced staff who have not been trained are vulnerable to inadvertently straying into activities which may not properly be authorised. We recommend that councils invest in training staff to understand the potential for any actions requiring authorisation, and that there are policies and key people in place within the public authority to which they can turn for further advice. We commonly recommended that individuals who had not received RIPA training since our last inspection should be provided with appropriate refresher training on changes that have come into force in recent years.
- 13.15 We inspected one council, in particular, that benefited from this approach in 2018; they were able to respond in a compliant manner using surveillance tactics to an increase in waste tipping. Our inspection noted that the authorisation records were well-kept and the powers used appropriately. We also inspected several authorities which demonstrated good training provision and policies despite limited use of covert powers.
- 13.16 We were particularly impressed by one council's comprehensive approach to policy and guidance. This included a RIPA policy; Social Networking Site Guidance; a CCTV Code of Practice; CCTV Procedural Guidelines; and separate Codes of Practice for CCTV in Council Run Buildings, the use of Body Worn Video Cameras and Public Space Surveillance Cameras. We were pleased to note that some of these had been drafted in collaboration with local police, demonstrating a thoughtful approach to covert investigations in the area. This practice gives us a high level of confidence in how these powers are being considered and used and we would hope to see this sort of approach replicated elsewhere.
- 13.17 The CoP requires local authorities to report the fact of its use of surveillance powers to elected council Members.³⁵ We identified that some councils had failed to comply with this practice requirement and that Members were not being updated on a regular basis of any usage, or not, of the relevant powers. This is essential to enable the Members to determine the RIPA/RIP(S)A policy each year. We have recommended that this should be remedied immediately, such that councils are making regular and accurate reports of usage.

35 Paragraph 4.47, and paragraph 3.30 in the CHIS Code of Practice.

- 13.18 We identified that several councils have set up working groups to discuss emergent issues and provide updates on changes in national or local RIPA/RIP(S)A policy. We were pleased that this approach enables the Senior Responsible Officer (SRO) to comply with their responsibilities under the CoP, and to establish an environment of preparedness and awareness.

Communications Data (CD)

- 13.19 Local authorities can only apply for subscriber information, which may identify the registered user of a telephone number or email service. Consequently, the use of CD in local authorities has been of limited use and, during 2018, across the 400 plus local authorities that were listed under RIPA, only 147 applications were made from just 68 authorities. Examples of when they have been used are for investigations into offences under Trading Standards legislation of selling dangerous, illicit or counterfeit goods, or to help identify persons responsible for illegal industrial waste disposal. However, we believe that the small numbers of applications sought under RIPA are indicative of the often bureaucratic process of authorisation.

Case study: how CD is used by local authorities

A local authority investigated the activities of a suspected organised crime gang (OCG) believed to be operating a “rogue trader” scam contrary to the Fraud Act 2006 and the Consumer Protection from Unfair Trading Regulations 2008. Analysis of communications data allowed the authority to identify and prove links between the group.

Initial evidence identified five victims who had paid for unnecessary or overpriced roofing repair work, and a sixth who had paid into a financial investment scam. The payments totalled £887,500.

Each victim provided a telephone number from which they had received communication in relation to the work and investment scam. The council used communications requests and analysis to confirm other communication sources related to signatories for the bank accounts into which the money was paid.

Five defendants were charged with money laundering and conspiracy to defraud. The evidence obtained via NAFN communication data requests was admissible in evidence, demonstrating relationships between the defendants. Communication analysis was also able to rule out other individuals and potential lines of enquiry.

- 13.20 Local authorities request communications data via a SPoC at NAFN. Judicial approval must then be granted under sections 23A and 23B of RIPA (as amended by The Protection of Freedoms Act 2012). In England, Wales and Northern Ireland, applications are considered by a magistrate and in Scotland a sheriff. The accredited SPoCs at NAFN scrutinise the applications independently, providing advice and guidance to applicants and designated persons ensuring the local authority acts in an informed and lawful manner, and will acquire the data from the provider once the application has been approved.
- 13.21 Of those applications, the majority related to requests for subscriber information in relation to telephones which were identified by the applicant as relating to the suspect of their investigation.

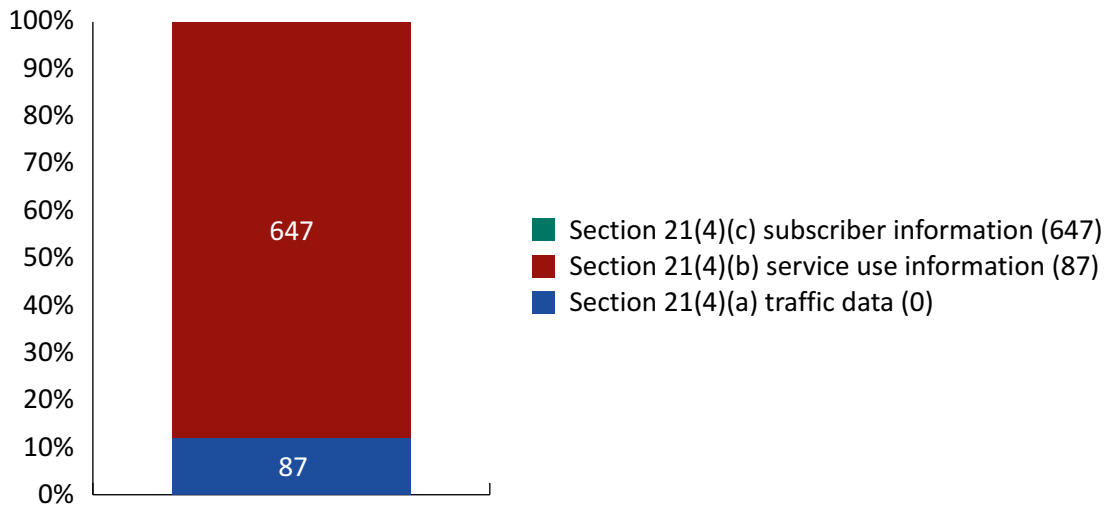


Figure 15: Communications data requests by data type for local authorities in 2018

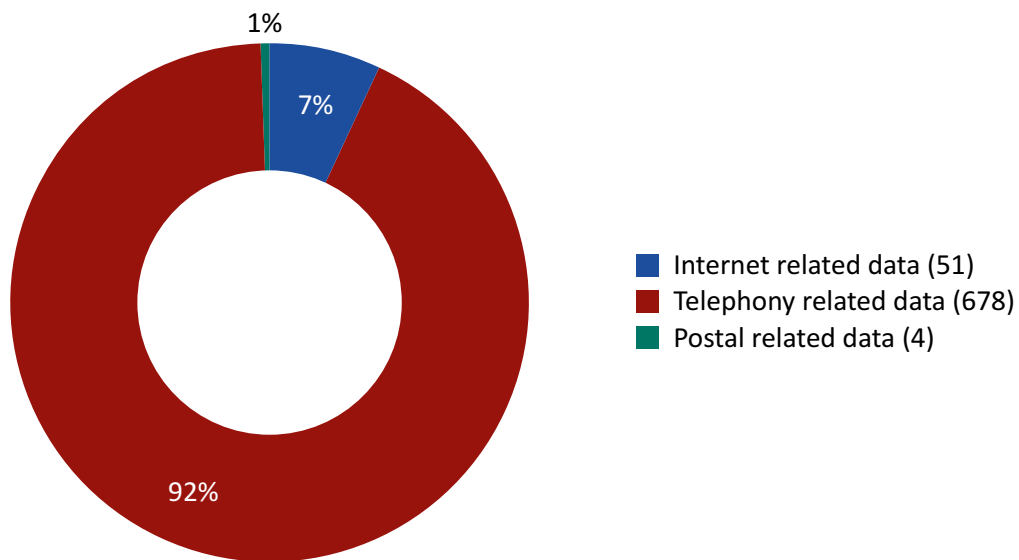


Figure 16: Communications data by communications type for local authorities in 2018

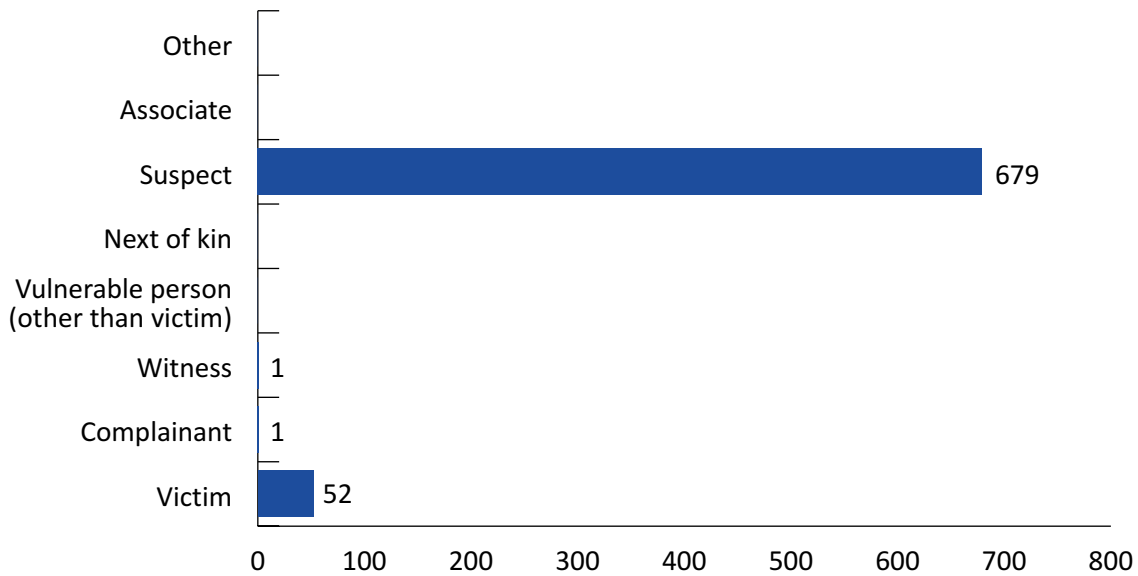


Figure 17: Communications data by relevant person, 2018

- 13.22 Throughout 2018, NAFN and local authorities prepared for the transition to Parts 3 and 4 of the IPA. This brought the introduction of new systems, processes and a training and awareness programme rolled out across the UK at regional seminars. Under the IPA, applications will be sent via the NAFN SPoC to an independent officer at the Office for Communications Data Authorisations (ODCA). We anticipate that this process will maintain independent scrutiny and oversight, while increasing efficiency.
- 13.23 Our inspection at NAFN confirmed that the system in place for acquiring communications data is compliant with the legislation. We were satisfied that the SPoCs ensured requesting authorities acted lawfully when acquiring communications data, providing designated persons with sound advice on which to consider an authorisation and apply their statutory considerations, and that staff processing the requests were appropriately trained.
- 13.24 During our inspection, we also considered whether errors have been correctly reported or recorded and whether practices are reviewed and adapted in light of any exposed weaknesses or faults. We were satisfied that errors were being identified and remedied appropriately.

14. Prisons

Overview

- 14.1 In England and Wales, the interception of prisoners' communications (telephone calls and mail) is governed by Prison Rules 1999 (as amended), which are made under the Prison Act 1952. Scottish Prisons use the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and prisons in Northern Ireland are governed by the Northern Ireland Prisons Act 1953. In each country, Prison Governors can authorise a wide range of intrusive conduct if they consider it necessary and proportionate for the purposes of:
- National Security;
 - Prevention and detection of crime;
 - Public safety;
 - Securing prison security;
 - Protection of health or morals; and/or
 - Protection of others' freedoms.
- 14.2 Other legislation available to Governors includes the Regulation of Investigatory Powers Act 2000 (RIPA) for authorising covert surveillance and management of covert human intelligence sources (CHIS) or the Serious Crime Act 2015, which allows the removal of illegal handsets from communication networks and the interference with Wireless Telegraphy Act 2012 to identify illicitly held mobile phones.
- 14.3 We have seen many examples where the use of covert tactics has led to the recovery of illicit items being taken into establishments by visitors, the identification and confirmation of corrupt relationships between staff and prisoners and the recovery of many illicit items from within the prison such as phones, SIM cards and homemade weapons.
- 14.4 We inspect the use of these powers at the individual prisons and centrally at Her Majesty's Prison and Probation Service (HMPPS). In 2018, we conducted 88 prisons inspections.

Findings

- 14.5 Overall, we are satisfied that the level of compliance in relation to the use of covert powers under RIPA is slowly improving. However, there is still much work to be done and the methodologies are not generally compliant with the requirements of the relevant Codes of Practice (CoP). We anticipate that the planned structural and procedural changes, if implemented, together with our recommendations below, will go a long way to establishing a compliant regime.

- 14.6 In addition to our standard approach to reports and recommendations, in 2018 we gave prisons an overall grading which reflects the standard of the approach overall to the management of investigatory powers, along with the establishment's progress in implementing previous recommendations. The ratings for this year were:
- 61% were good
 - 26% were satisfactory
 - 13% were poor.
- 14.7 The strategic responsibility for the management and delivery of covert tactics across the HMPPS estate falls to the Executive Director for Security, Order and Counter Terrorism (SOCT), who is also the HMPPS RIPA Senior Responsible Officer (SRO). This is the reason for our annual inspection at HMPPS. HMPPS have initiated work to rectify weaknesses in their intelligence management structures and processes, including the way authorised activity is managed and monitored. Progress on this work has been slow but we anticipate significant benefits to compliance across the estate as this work progresses. At the time of the most recent inspections many of these changes were still in their early stages and therefore had little or no impact on our findings.
- 14.8 We similarly conducted an inspection of the Northern Ireland Prison Service (NIPS). NIPS operate three establishments, one of which manages young offenders and female prisoners. We were satisfied that NIPS had made improvements based on our previous recommendations, in particular in relation to training.
- 14.9 The Investigatory Powers Commissioner (IPC) and Dame Linda Dobbs met with the Cabinet Secretary for Justice for Scotland to agree an approach for the statutory inspection process of prison interception in Scotland. We agreed that inspections of Scottish detention facilities will mirror the rest of the United Kingdom. Our previous inspections of the Scottish Prison Service (SPS), which operates 15 establishments, focussed on directed surveillance and the management of CHIS and our inspections have identified a strong cooperative relationship between the SPS and Police Scotland. This enables a significant exchange of intelligence to the benefit of both organisations. We are working with the SPS to establish an appropriate inspection model, which will scrutinise the use of all investigatory powers in the 15 Scottish prisons.

Covert Human Intelligence Sources (CHIS) and Surveillance

- 14.10 We noted a decrease in activities involving CHIS and surveillance techniques in 2018, despite the increased presence of psychoactive drugs, illegally-held mobile phones and other items in prisons. We believe that this reduction might be attributed to the use of Prison Rule 50A, which allows for overt monitoring via CCTV, and the adoption of other overt tactics. Conversely, this could be a result of outdated structures and processes and a lack of confidence and understanding in staff, which is becoming an obstacle to legitimate investigation within prisons. We discussed this question with HMPPS and intend to keep this under review in 2019.

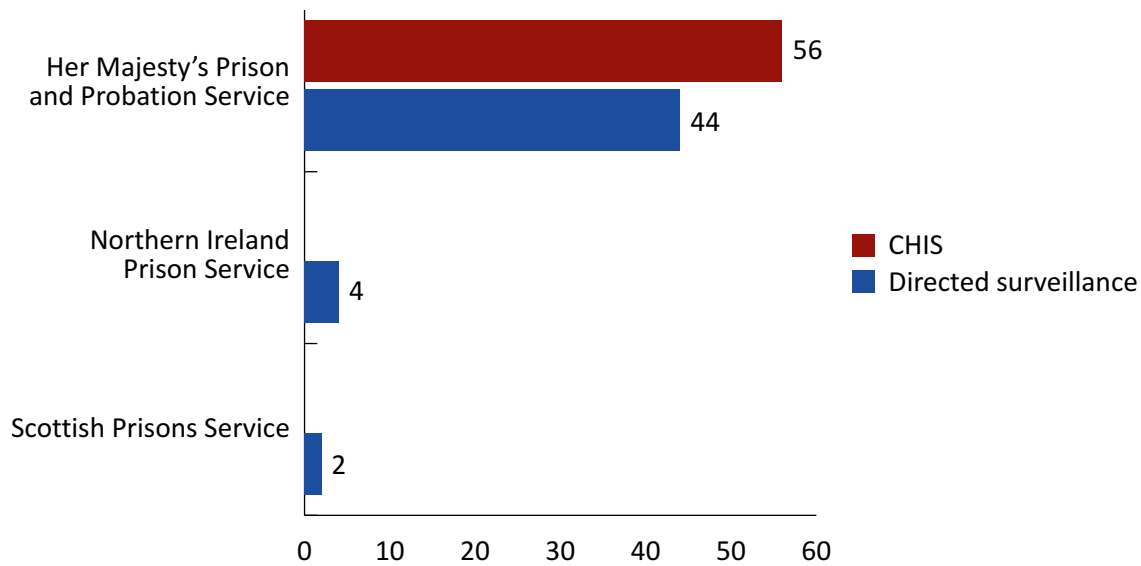


Figure 18: Use of CHIS and surveillance in prisons, 2018

- 14.11 During our inspection at HMPPS, we were pleased to note that many of our recommendations from 2017 had been discharged. However, we were disappointed that compliance levels remain low. We highlighted the need for a more rigorous process, particularly around the management of CHIS which are particularly high risk in this environment.
- 14.12 We continue to recommend that relevant and meaningful policies and Prison Service Instructions must be put in place to enable a more complaint culture across the service.
- 14.13 We were concerned about the operational competence of Authorising Officers (AOs), which appears to result from a lack of adequate training. We note that this is currently under review and look forward to seeing those carrying out this fundamental role being able to develop their competence within an improved structure with the right level of support.
- 14.14 HMPPS have developed their Digital Investigations Unit and have targeted the illegal use of social networking sites by prisoners. We were persuaded of the value of this work in preventing illegal activity but have requested assurance that this work is being conducted in a compliant manner. We will review this in 2019 and scrutinise whether appropriate internal oversight is being applied.

Interception

- 14.15 We inspect each prison's use of interception provisions, including how sensitive legally privileged conversations are safeguarded. To make an external phone call, prisoners use a pin-phone system that requires a unique pin number being entered prior to the call being made. The pin-phone system is controlled centrally in each prison by an electronic system, while the monitoring of letters and emails has to be done manually. Before issuing a pin code, prison staff will explain the interception process to new prisoners. Prisoners are responsible for recording their legal or confidential contacts, which allows the prison to filter and ensure that they do not monitor sensitive communications. In England and Wales, the Prison Service Instructions (PSIs), the National Security Framework and the Public Protection Manual provide detailed guidance on how interception should be carried out.

- 14.16 The decision to authorise the interception of a prisoner's communications is made by a Governor. The authorisation and its associated documents are stored in the establishment and any intelligence is recorded in the prisoner's file. We request the number of live authorisations at each prison on the day of inspection and do not collect statistics for interception of prisoners' communications. These figures are not centrally collected and we do not anticipate that this will change in the near future.
- 14.17 Under Prison Rules the raw intelligence cannot be stored for more than three months without an exceptional case for retention. The Governor may authorise prolonged retention of raw interception material for as long as is judged to be necessary, but this provision is rarely used in reality. We have inspected the necessity and proportionality records in relation to any prolonged retention and were satisfied that the cases were appropriate and the records adequate. Relevant circumstances might include material relating to a specific dispute or criminal act conducted within the prison, or where an individual within the prison has come to harm.
- 14.18 In England and Wales, Prison Rule 35A gives a prison Governor the authority to intercept any communications by a prisoner or a class of prisoners, if this step is necessary and proportionate. Prison Rule 81 allows Governors to delegate their powers to other officers. In practice, the responsibility to consider and authorise requests to intercept prisoners' communications is delegated to the Head of Offender Management or the Head of Prison Security. We were satisfied that these methodologies were being used appropriately.
- 14.19 An Interception Risk Assessment needs to be completed whenever there is a request to intercept a prisoner's communications. This document should explain the threat, the proposed course of action, the assessment of necessity and proportionality, the duration of the proposed monitoring and any other matters taken into consideration by the AO. The majority of our recommendations relating to interception focused on a failure sufficiently to set out in an application the necessity and proportionality considerations to a standard that would enable the Governor to make a lawful decision as to whether to authorise interception. We made this observation frequently, particularly with regard to prisoners who pose a risk to the public, such as those convicted of violent assaults, harassment or sexual offences. We have continued to see deficient paperwork, a general failure to include sufficient detail of the factors relevant to the particular case, an apparent disregard of any Human Rights issues that were engaged and an insufficient record of the matters the AO had taken into consideration.
- 14.20 We also noted that there was commonly a failure to carry out suitable reviews of the authorisations. We noted that this was particularly the case when staffing levels were low or those monitoring lacked appropriate supervision.
- 14.21 The increase in drug use within prisons is well documented; the posting of correspondence soaked in illegal psychoactive substances into establishments has risen sharply. In the disguise of a personal letter or legal correspondence, prisons receive drug impregnated paper that is subsequently consumed. We have highlighted the powers available to Governors to intercept suspicious correspondence in a proportionate and intelligence-led manner and welcome the use of testing equipment that reduces the level of intrusion into a prisoner's correspondence. Our inspections have focused on the testing and opening of mail suspected of containing drugs and overall the processes and procedures in place have been compliant with Prison Rules and are proportionate.

Communications Data

14.22 The ability to access communications data (CD) is limited to HMPPS Headquarters. We have inspected the acquisition of CD for the purposes of internal investigations, including corruption prevention. The methodology for obtaining CD has changed under the IPA: all requests for CD made by individual prisons are processed by the SPoC unit at HMPPS and, from 2019, are approved by the OCDA. From our inspections in 2018, we are satisfied that the applications being made are necessary and proportionate. In the future, the oversight function provided by OCDA will enable us to establish have a high level of confidence in the consistency of these requests.

Wireless telegraphy

14.23 Prisons also have the power to conduct operations under the Prisons (Interference with Wireless Telegraphy) Act 2012. This permits the interference with illicit communications equipment within prisons; this action would enable prisons to identify, and to some extent track the usage of, mobile phones used to support illicit and criminal activity within the prison. The objective is to identify and prevent illicit communications. HMPPS is progressing a programme of work to update the technologies used in this area, which will enable more efficient and proactive detection.

14.24 We have reviewed the use of these techniques and are satisfied that they are being used appropriately although, as in other areas, the standard of documentation across the prisons estate is inconsistent. Where the use of mobile phones is detected within an establishment but the device has not been seized, the prison may apply to a court under the Serious Crimes Act 2015 for a Telecommunications Restriction Order. A Telecommunications Restriction Order allows the prevention or restriction of use of communications devices in prisons by ordering mobile network operators to remotely blacklist handsets and disconnect SIM cards inside prisons. We inspect the records of this activity at each prison and are satisfied that this technique is being used appropriately.

15. Warrant Granting Departments

Overview

- 15.1 The introduction of the double lock has established a new working relationship with the departments of state. This moves the Investigatory Powers Commissioner's Office (IPCO) from simply conducting retrospective reviews to current scrutiny of the Secretary of State's decision making. Notably, this includes insight into the pre-authorisation challenge function provided by the Secretary of State and through the Warrant Granting Department (WGD). In many cases, and in the majority of novel and contentious cases, there is some additional dialogue between the WGD and the requesting agency to ensure that the requirement outlined is necessary and proportionate. Such scrutiny at this point in the process provides a granular challenge, whereby the WGD will review whether the proposed action meets the required operational or intelligence outcome. This is of particular note for thematic authorisations where, before submitting an application to the Secretary of State, the WGD will ensure that the scope of the warrant is the minimum necessary to meet the stated aims.
- 15.2 We inspect the Ministerial oversight of the use of bulk communications data (BCD) at the requesting agencies, rather than the WGD. This gives us oversight of the end-to-end process. In our consideration of the Secretary of State's role in this process, we consider the adequacy of documentation presented for authorisation and review and the clarity of directions provided to the relevant communications provider. For each section 94 direction, the direction supporting documentation made explicit that the relevant Secretary of State was giving the direction in person and each was signed. In each case, section 94 directions specified the communications data (CD) which was the subject of the direction by using terminology familiar to the communications service providers (CSPs). This methodology will change in 2019 to accommodate the changes resulting from the introduction of warrantry for the bulk acquisition of CD.
- 15.3 Our 2018 inspection of the Home Office's National Security Unit (NSU) focused on the scrutiny they provide throughout the lifespan of interception operations. The Home Secretary may impose conditions for review when approving any authorisation, for example, where it is judged that there may be an unusually high level of intrusion into the target's privacy. However, we noted a number of cases where the requirement for review was not enforced and MI5 did not provide a relevant update at the designated time. We support the Home Office's assertion that these reviews must be received, if requested, and our Judicial Commissioners (JCs) consider these to be an important condition of the authorisation.
- 15.4 We have worked closely with the National Security Unit (NSU) to establish processes to ensure that applications are progressed swiftly through the system without compromising the ability for the Senior Official, Secretary of State or JC to have adequate time to consider or challenge the application in hand. We believe that these processes have been well implemented.

- 15.5 Our inspection at the NSU fell before the Investigatory Powers Act 2016 (IPA) had been fully implemented and so we did not formally inspect the modification casework in 2018. However, our oversight via the double lock gives us a high level of confidence that these are being well handled. In 2019, our inspectors will review a sample of modification paperwork although, given the double lock, this is likely to be a lesser proportion than those reviewed in house at each agency.
- 15.6 In our 2017 report, we stated concerns that the Foreign and Commonwealth Office (FCO) in particular were not providing the expected level of oversight, or challenge, to the UK Intelligence Community (UKIC) when reviewing and authorising submissions. The introduction of the IPA, which has required significant resources from the FCO to manage the new authorisation regime, has delayed our assurance work in this area. This transition has included an overhaul of the department's central records system for warrantry and authorisations, which we expect to assist with our oversight in the future. We are continuing to work with the FCO on this and anticipate that we will be in a position to confirm a higher level of confidence in our 2019 Annual Report.
- 15.7 Our 2018 inspection of interception authorisations at the FCO noted good evidence that the Foreign Secretary and Senior Officials were providing appropriate challenge to the requesting agency. During this inspection, we scrutinised documented correspondence between the FCO and requesting agency, which recorded examples of the FCO challenging the scope and intrusiveness of proposed authorisations.
- 15.8 In addition, the introduction of the double lock has simultaneously established scrutiny of authorisations that have been approved by the Foreign Secretary. We have no concerns about the standard of scrutiny or challenge provided in those areas, specifically bulk personal data (BPD), interception and equipment interference, and all subject to judicial approval.
- 15.9 The WGDs of the Scottish Government (SG) and Northern Ireland Office (NIO) are providing a robust guardian and gatekeeper function with regard to interception applications and had a good level of compliance with the previous Regulation of Investigatory Powers 2000 (RIPA) regime and the Code of Practice.
- 15.10 We examined collateral intrusion statements made by Police Scotland and considered that there could be greater consistency in some applications. We suggested that this was an area the SG should focus on in the future.

16. Technology Advisory Panel

Overview

- 16.1 The Technology Advisory Panel (TAP) is required under the Investigatory Powers Act 2016 (IPA) to submit an Annual Report to the Investigatory Powers Commissioner (IPC). The IPC has agreed that he will make that report publicly available through his Annual Report.

The full text of the 2018 report is as follows:

The Technology Advisory Panel (TAP) was set up under the Investigatory Powers Act 2016 (“the Act”) (paras 246-247). Establishing and maintaining the TAP is a responsibility of the Commissioner but the TAP may also give advice to relevant Ministers. The TAP has a dual function under the Act: both to advise about the impact of changing technology, and also 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 Commissioner or of any part of the Government.

The Chair of the TAP, Sir Bernard Silverman FRS, formerly Chief Scientific Adviser to the Home Office and Emeritus Professor of Statistics at Oxford University, was appointed towards the end of 2017. During 2018 the Commissioner appointed the following three additional members: Professor 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, and John Davies, who has an extensive technical background in both government and private industry roles. A Secretary to the TAP was also appointed. This is the first Annual Report.

Activities undertaken by the TAP and its members during 2018 include:

- *A number of informal meetings during the year, leading to the first formal meeting in December 2018; the panel could not meet formally earlier, because of the need to complete processes required for the appointment of members.*
- *The co-hosting (with the Intellectual Forum based at Jesus College, Horizon Digital Economy Research and the EPSRC IoT Research Hub, PETRAS) of a day conference in November 2018 on the Metrics of Privacy. Delegates came from a mixture of backgrounds and experiences including statistics, computer science, privacy and open rights groups and other bodies with an interest in the topic. A formal report of the day is being prepared for publication.*
- *A study and report on a specific sensitive topic in order to give technical guidance to the members of the Inspectorate.*

- *Guidance on specific warrantry-related technical topics given to one of the Judicial Commissioners. This involved providing technical support in relation to Technical Capability Notices, National Security Notices and Communications Data Retention Notices.*
- *Work on the systematic planning of inspections using statistical quality inspection approaches.*
- *Attendance at an international oversight review committee meeting in Australia as other countries expressed an interest in creating similar organisations to the TAP.*
- *Attendance at several meetings and briefings jointly with Judicial Commissioners.*

17. Errors and breaches

Overview

- 17.1 For the first time, in 2018, all errors arising from the use of investigatory powers have been reported to, and investigated by, the same organisation (the 2017 Annual Report shows an amalgamation of reporting both to the Investigatory Powers Commissioner's Office, IPCO, and its predecessor organisations). The errors that we investigate range from small-scale human errors to broader systemic failings. Irrespective of the scale of the error, we consider the human impact in our assessment of its seriousness; in the majority of cases the subject of the error will be unaware that their right to privacy has been affected.
- 17.2 Section 231(9) of the Investigatory Powers Act 2016 (IPA) defines a 'relevant error' as an error:
- a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and
 - a) of a description identified for this purpose in a code of practice under Schedule 7.
- 17.3 Based on this description, IPCO has been preparing new guidance that will define 'relevant errors' and 'serious errors' more clearly for public authorities and those who may be affected. This guidance should shortly be available on the IPCO website; it will include some examples of the types of activity in each category and is intended to help to ensure that reporting is consistent across all public authorities.

Reporting and investigation

- 17.4 When a relevant error has occurred, the public authority must notify the Investigatory Powers Commissioner (IPC) as soon as reasonably practicable and no later than ten working days (or as agreed with the Commissioner) after it has been established that a relevant error has occurred. The overwhelming majority of errors are reported timeously by members of staff within the relevant authorities and most are dealt with quickly by the IPCO team. Where a matter is identified as potentially serious, the report will be assigned to one of the Inspectors for a detailed investigation for consideration by the IPC. Because of their sensitivity, all error reports of the UK Intelligence Community (UKIC), and those for the intercepting agencies, are handled individually by an Inspector.
- 17.5 There are occasions when unreported errors are identified during the course of an inspection but it is pleasing to note that the strong culture of self-reporting identified in previous Annual Reports continues. Given the nature of the recent MI5 IT compliance issue, which was reported to IPCO in February 2019 and is covered in more detail in paragraphs 6.44 -6.46, the IPC raised legitimate questions about whether IPCO should itself have identified the compliance risks earlier or whether the reliance on self-reporting puts the oversight regime at risk of manipulation by those we inspect. Having reviewed the matter

closely the IPC is satisfied that it is precisely the depth of our inspections, and the access to records given to IPCO Inspectors across all the organisations we oversee, which ensures that the culture of self-reporting works as effectively as it does. There is little doubt that unreported issues would emerge during the course of an inspection and so there is a clear understanding amongst all public authorities that errors should be reported as soon as possible.

- 17.6 The potential impact of errors on the rights of individuals can be grave. The prompt identification of errors is key to ensuring that problems do not become systemic and that individual failings are addressed. The onus is on the public authority to take the necessary steps, with the agreement of, or as mandated by, the IPC to prevent recurrence. All public authorities take errors seriously and the Inspectors keep a close check on remedial action at follow-up inspections.
- 17.7 The IPC has a duty to inform affected parties of a serious error under section 231 of the IPA, if he judges that this is in the public interest. A serious error is an instance of non-compliance which has resulted in significant prejudice or harm to the person concerned. During 2018 the IPC made eight determinations in relation to serious errors, as detailed at Annex C. In these cases, in accordance with section 231 (6) of the IPA, the Commissioner informed the affected person of their right to apply to the Investigatory Powers Tribunal (IPT) to seek redress.

Double lock error

- 17.8 The Home Office reported one instance where an administrative oversight meant that judicial approval was not retrospectively sought in the case of an urgent application. This was identified when the requesting agency sought to renew the warrant. The requesting agency, when notified of the error by the Home Office, ceased all activity and cancelled the original warrant, which had been active for five working days. The agency applied for a new authorisation to cover the activity: the case, and the error, were briefed to both the Home Secretary and a Judicial Commissioner (JC), who were satisfied that the requested action was necessary and proportionate and who both approved the new application.
- 17.9 The Home Office took several steps to prevent repetitions of this error by changing the process for handling urgent requests for warrants. We are confident that these processes eliminate the possibility of inadvertently failing to validate urgent applications via the double lock. We have seen no other instances where the double lock process has not been effective.

UK Intelligence Community (UKIC) Errors

- 17.10 To allow comparisons with statistics provided in previous years, the errors from UKIC and the Warrant Granting Departments (WGD) are broken down by agency and power as inspected by the previous oversight organisations. UKIC reported a total of 167 errors. Other than the Home Office error detailed above, there were no errors reported by the WGDs or the Ministry of Defence (MOD).
- 17.11 Of the UKIC errors, 20 errors related to activity other than interception and communications data (CD). There were 40 errors in this category reported in 2017 and 38 reported in 2016.
- 17.12 In addition, 40 interception errors and 107 CD related errors were reported by UKIC agencies in 2018, as detailed below. Of the CD related errors, 46 were reportable errors.

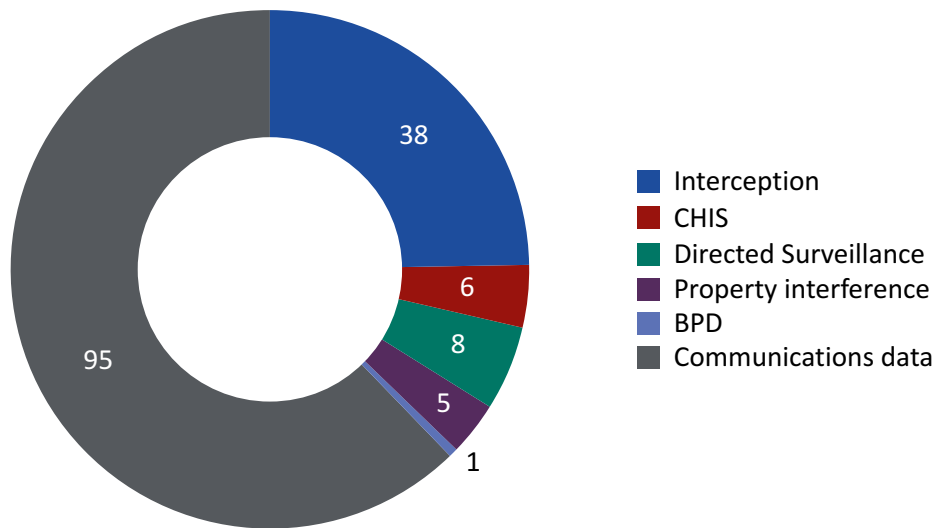


Figure 19: UKIC errors, 2018

| | MI5 | GCHQ | SIS |
|------------------------------|-----|------|-----|
| CHIS | 3 | 0 | 3 |
| Directed Surveillance | 8 | 0 | 0 |
| Property Interference | 4 | 1 | 0 |
| Bulk Personal Data | 1 | 0 | 0 |
| Section 7 | 0 | 0 | 0 |
| Interception | 22 | 15 | 1 |
| Communications data | 84 | 11 | 0 |
| Total | 122 | 27 | 4 |

Table 1: Breakdown of UKIC errors, 2018

17.13 As shown at figure 20, there is no pattern of errors from UKIC and we have not seen a repeat of common errors made in 2017. There is no pattern in the errors reported to us which would suggest any systematic failure of safeguards. The errors which resulted from human error showed no evidence of deliberate attempt to act unlawfully or circumvent safeguards.

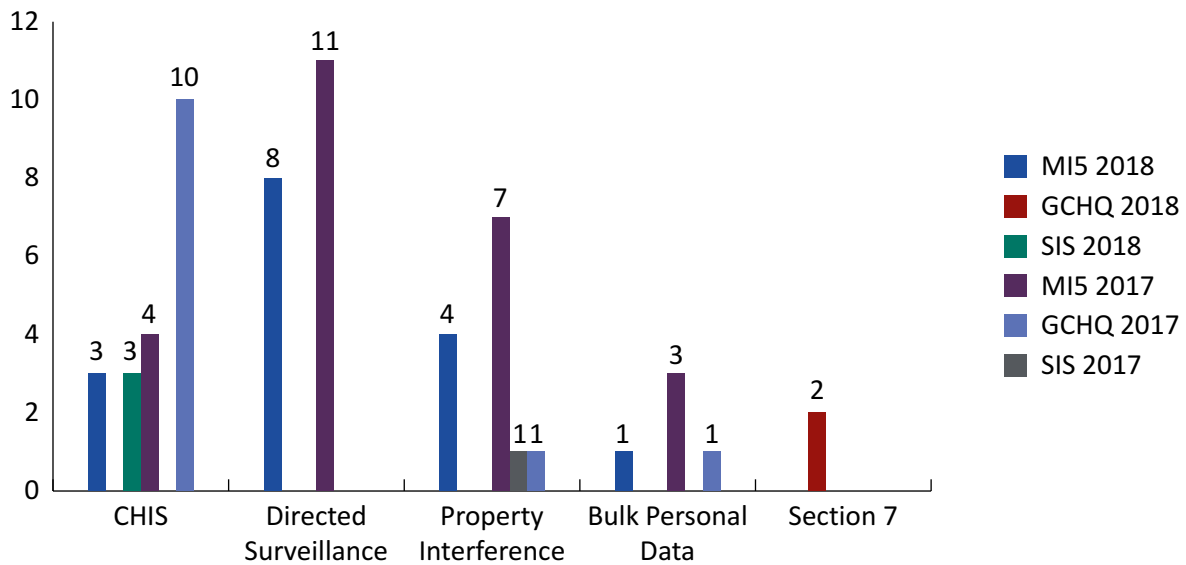


Figure 20: UKIC errors 2017 and 2018, excluding interception and communications data

17.14 In our 2017 report, we set out that MI5 had identified an error, in the way one of their systems was set up to handle data (as below). We have seen a growing understanding towards data handling systems in 2018, which may result in the identification of further errors in this area from MI5 and other bodies in the future.

17.15 In October 2017, MI5 reported an error relating to an intelligence platform. The system is used by MI5 officers to analyse a range of information from a variety of sources, including warranted data. An officer using the system might search data across a number of sources and save targeted results. The error, which was investigated by IPCO in 2018, was that there was no review, retention and deletion (RRD) policy in place for data saved by officers working on the system. This means that material, derived from targeted searches of warranted data, may have been unlawfully retained as there were no longer any authorised grounds under the relevant legislation to retain it. MI5 have now put in place an RRD policy for the platform and all data held in that area, that is assessed not to be necessary or proportionate to retain, has been deleted.

17.16 After reporting the error, MI5 also identified that this saved material had not been included in the search exercise that MI5 had previously carried out in relation to an ongoing IPT case. MI5 then carried out searches of the saved material using selectors previously provided by human rights charity, Privacy International. Material relating to Privacy International was found as a result of those searches, but this data was subsequently deleted.

17.17 Privacy International expressed concern to the IPC that this prevented IPCO from conducting an investigation into the issue. IPCO conducted an immediate inspection of MI5 in order to respond to the complaint from Privacy International. This showed that, whilst the data itself had been deleted, MI5 did hold a documentary record describing the data that they had held. In investigating this, the Deputy IPC and an Inspector visited MI5 to review the record of the data and concluded that there were no concerns about the necessity and proportionality of the actions taken by MI5.

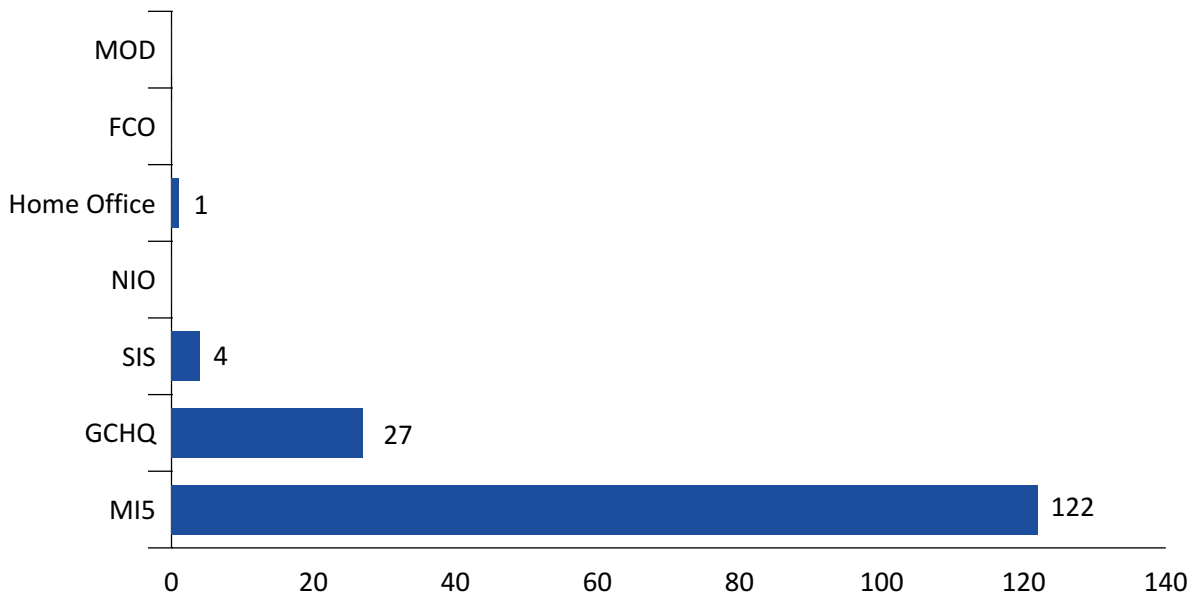


Figure 21: UKIC errors by department and agency, including interception and CD, 2018

UKIC Communications Data (CD) errors

17.18 The relevant Codes of Practice (CoP) outline the point at which errors occur and the actions required to be taken by an agency or a Telecommunications Operator (TO). When an approved application for targeted CD is initiated, or a notice served on a TO, there are two categories of error: recordable and reportable.

What is a recordable error?

A recordable error is one that has been identified by the agency without any data being incorrectly acquired or disclosed. A list of recordable errors is retained by an agency. The record explains how the error occurred and provides an indication of the steps taken to prevent a reoccurrence. At each inspection, the list of recordable errors is audited and, if necessary, observations or recommendations are made in inspection reports to tighten procedures or processes. An example of a recordable error is when an analyst manually transfers data to a system and inputs the information incorrectly, making a transposition error which does not result in the acquisition of incorrect data.

What is a reportable error?

A reportable error occurs when incorrect CD is acquired; such a disclosure to an agency could infringe on the rights of an individual unconnected to an operation or investigation. Reportable errors should be recorded within five working days of their discovery. The error report explains how the mistake occurred, indicates whether any unintended collateral intrusion has taken place, details and confirms the destruction of data and provides an indication of steps taken to ensure similar errors are not replicated. When a report is made, the appropriate Senior Responsible Officer (SRO) must be sighted on the error to enable, if necessary, any strategic changes to policy or procedures.

- 17.19 A strong culture of error reporting and subsequent management of errors runs through UKIC but, during the implementation of the IPA when agencies were focusing on numerous new compliance requirements, the delay in submitting reports did increase. Agencies did, during this reporting period, increase resources to their compliance teams, but often investigating the cause of a CD related error can be time consuming and complex. The reasons for these delays were clear and, when IPCO was notified, it was apparent that a thorough investigation had been conducted with, when necessary, action taken to prevent duplication.
- 17.20 No UKIC error reports were judged by the IPC to be serious.

| | Recordable Errors | Reportable Errors | Serious Errors |
|------|-------------------|-------------------|----------------|
| SIS | 0 | 0 | None |
| GCHQ | 11 | 9 | None |
| MI5 | 47 | 37 | None |

Table 2: UKIC communications error statistics, 2018

Interception

- 17.21 13 Interception errors were reported to us in 2018 by intercepting authorities other than UKIC. There were no errors reported by the WGDs. None of these errors were judged to be serious errors.
- 17.22 In 2018, 99 errors relating to surveillance, property interference and CHIS were reported by organisations other than UKIC. Errors in this area include failures to obtain the appropriate authorisation or failure to adhere to the relevant safeguards set out in the relevant CoP. This number is a slight increase from the 83 'breaches'³⁶ reported in 2017.

Surveillance, Property Interference and Covert Human Intelligence Sources (CHIS): Law enforcement, public and local authorities, and prisons

| Investigatory Power | Number of Errors |
|--------------------------------------|------------------|
| Directed Surveillance | 59 |
| Property Interference | 23 |
| Intrusive Surveillance | 3 |
| CHIS (including undercover officers) | 14 |

Table 3: Total surveillance, property interference and CHIS errors for LEAs, public and local authorities and prisons, 2018

- 17.23 We are satisfied that the number of errors is proportionately minimal. We have not noted any systematic failures to apply safeguards in any particular authority. The 59 directed surveillance errors vary significantly in seriousness but are most frequently the result of a simple human mistake. As reported in previous Annual Reports, examples include starting the surveillance before the authorisation has come into effect or continuing the activity

³⁶ There was no formal definition of an error provided by the Office of the Surveillance Commissioner (OSC) as the term was only defined with the advent of the IPA 2016. The terms 'error' and 'breach' were used interchangeably and section 79 of the OSC Procedures and Guidance 2016 outlined the circumstances when the then Chief Surveillance Commissioner expected to be notified of a breach and the procedures to be followed. We do not believe that the terms set out in the Code of Practice will have affected the working practice in relation to error reporting.

or leaving the equipment in situ after the authorisation has been cancelled. Any material obtained from unauthorised activity is handled with appropriate care and we ensure that destruction takes place.

- 17.24 We have noted, however, that errors have been reported in relation to the monitoring of social media sites without the requisite authorisation in place. This remains a relatively new investigative methodology. Many public authorities have embarked on training programmes to raise awareness amongst staff and have published guidance on the use of the internet on their own intranet sites to ensure that this resource is used in a controlled, auditable and compliant manner. We will keep a close review of this area and would expect to see report fall in errors of this kind in our 2019 Annual Report.

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

- 17.25 In 2018, 903 CD errors were reported to the Commissioner by relevant authorities, compared to 926 errors reported in 2017. The breakdown of errors is largely consistent with 2017 and we have noted that the most common error remains the submission of an incorrect communications address by an applicant. 42% of errors were made by Special Points of Contact (SPoCs), which is reflective of their role in the acquisition of CD. We have encouraged law enforcement to limit the impact of incidental errors through data validation and, in particular, suggested that internet-based CD should not be the sole basis for action. We believe that communications data errors should be identifiable before officers approach the wrong address or individual. We are encouraged that there have been numerous examples of where additional validation checks have identified errors before action was taken.

| | Reportable errors |
|----------------------------------|-------------------|
| Law Enforcement Agencies | 758 |
| Communications Service Providers | 126 |
| Others | 13 |
| Public Authorities | 6 |
| Total | 903* |

Table 4: Reportable errors in relation to law enforcement, 2018

** Five errors were identified during IPCO inspections and subsequently reported*

- 17.26 The majority of CD errors reported by law enforcement authorities and public bodies related to actions by the SPoC or applicant, as shown by the tables below.

17.27 A significant proportion of errors result from the applicant noting down incorrect details from the reporting person, such as victims or witnesses, or inaccurately transposing the communications address into their application. While this is inevitable, to some degree, it is essential that applicants are vigilant and that post-validation checks are used as much as possible.

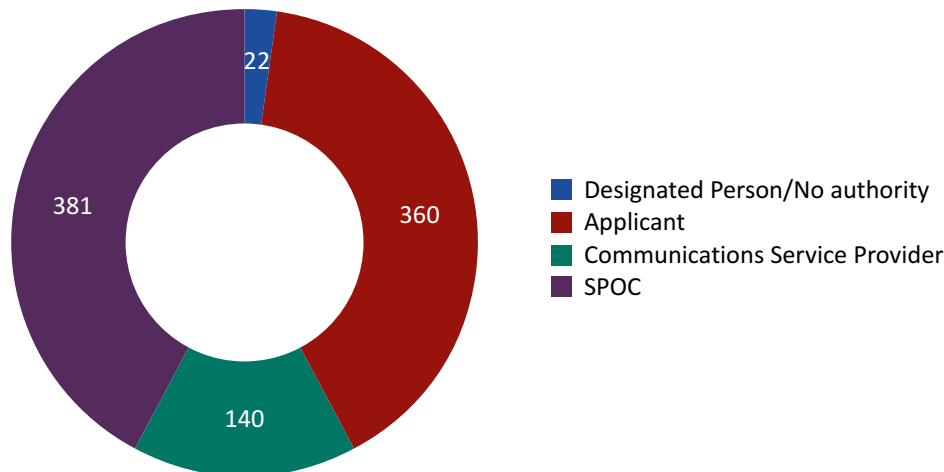


Figure 22: CD errors by user in law enforcement, public authorities and prisons, 2018

| | SPOC | Applicant | CSP | Designated Person (DP)/No authority |
|--|-------------|-------------|------------|-------------------------------------|
| | 81 (19 IP) | 309 (22 IP) | – | – |
| Incorrect time/date | 199 (66 IP) | 43 (12 IP) | 50 | – |
| Incorrect data type | 96 | – | 32 | – |
| Incorrect data | – | – | 27 | – |
| Excess data | – | – | 14 | – |
| Negative result when data was available | – | – | 14 | – |
| Data acquired without authority of DP | – | – | – | 14 |
| DP wrong rank | – | – | – | 8 |
| Other | 5 | 8 | 3 | – |
| Total | 381 | 360 | 140 | 22 |

Table 5: Breakdown of communications data errors by error type and individual responsible, 2018

Error reduction

17.28 Across public authorities, efforts to reduce the need for SPoCs to manually transpose data continue. We have encouraged public authorities to introduce technical means of minimising errors if possible and have seen the value of quality assurance and validations checks from SPoCs, which have shown a higher number of ‘near misses’ being recorded. These are particularly valuable in relation to comparison checks between the originating

document from which the number or identifier has been sourced and the number contained in the actual application.

- 17.29 Throughout 2018, we have focused during inspections on examining applications for internet related requests and the process by which they are acquired. We have continued to highlight the vulnerability of resolving Internet Protocol Address Resolutions (IPAR). Internet protocol (IP) addresses are dynamic and will appear in different date formats and time zones, all of which present challenges for officers and staff within public authorities to correctly interpret the returned data, and therefore pose a higher risk of an error occurring than with other formats of CD.
- 17.30 With the National Police Chiefs Council (NPCC), we supported the work of the Data Communications Group to produce a national 'Error Reduction Strategy'. Published in November 2018, the strategy is based on good practice and our inspection findings. The Strategy will be used as a baseline in our 2019 inspection programme when assessing the procedures in place to acquire internet data.
- 17.31 We note that incorrect time conversion is a persistent issue. This should be resolved with the roll-out of a tool designed by the Home Office National Communications Data Service (NCDS). Time conversion of IP activity from international timezones to GMT or BST has long been an issue. Many internet service providers are hosted outside the UK and data returned can, therefore, be in a variety of international time zone formats. With no bespoke tool available, SPoCs used various online tools to assist with this conversion and encountered a range of flaws. We have recommended that this tool, which was released in February 2019, should be used and, as a result, we expect to see a reduction of these errors in 2019.

Serious error investigations

- 17.32 We undertook 24 serious-error investigations in 2018 and determined that the 22 cases set out in Annex C were serious errors. In eight of those cases, the IPC wrote to the affected person informing them of the rights to apply to the IPT. Save for one historic error in the recording of a telephone number, all other notifications were in some way connected to the online sexual exploitation of children. We noted that in the case of investigation three, the affected person had already addressed concerns to the IPT; that meant our role in this case was to investigate and provide the IPT with our report.
- 17.33 Circumstances which we judge to be potentially serious are likely to include:
- Technical errors relating to the CSP secure-disclosure systems which result in a significant number of erroneous disclosures;
 - Errors when a public authority has initiated a course of action that has an adverse impact on someone (for example, sharing information with another public authority stating a person is suspected of a crime; when an individual is visited, or a search warrant is executed; or there is an arrest); and
 - Errors which result in the wrongful disclosure of a large volume of CD or a particularly sensitive data set.
- 17.34 We note that IPARs pose the most risk of error, although our recent investigations have identified a shift in that, in many cases, incorrect data was provided by the CSP or the results received were misinterpreted. The need for explicit attention to detail when

acquiring data in these cases will be ever present, especially as new technologies and means of communication evolve.

Prisons

- 17.35 Statistics for errors reported in relation to CHIS, surveillance and communications data are included in the chapter above. There is no formal process or obligation for prisons to record and report breaches of the Prison Rules. We would, however, expect any systemic failures in compliance to be notified to us at inspection.

18. Statistics

Overview

- 18.1 The Investigatory Powers Commissioner's Office (IPCO) collects a wide range of statistics on the use of investigatory powers, including those under the Investigatory Powers Act 2016 (IPA). These statistics help to inform our understanding of how those powers are being used and allow us to track the use of powers year on year. It is worth noting that changes in legislation and policy over the years necessitate the analysis of these statistics in combination with additional details about the use of powers, such as the way that different covert tactics, and operational activities, are authorised. The sensitivity of this work makes it impossible to publish the statistics we hold in full. Additionally, we believe that publishing some statistics would be unhelpful and, at times, misleading.
- 18.2 Section 234 of the IPA requests the publication of key statistics, including the number of warrants and authorisations issued, given, considered and approved during the year. In line with this requirement, this report includes the number of warrants and authorisations issued under the IPA, the Regulation of Investigatory Powers Act 2000 (RIPA), the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A), the Intelligence Services Act 1994 (ISA) and the Police Act 1997, and will include approvals given, such as the approval to retain and examine confidential or legal professional privilege (LPP) material. It is essential to note that these figures relate to a period of transition as the authorisation process for existing activities was implemented. For example, bulk personal dataset (BPD) holdings were not comprehensively authorised under the IPA from the date of implementation but were brought under the authorisation regime across a transition period. For this year, therefore, the statistics below will not necessarily reflect the totality of covert activity in some areas and it may be several years before full comparisons can be drawn.

Total number of applications made in 2018

- 18.3 The table below gives a total number of applications granted for the powers overseen by IPCO.
- 18.4 We have included details of the number of applications considered by the Judicial Commissioners (JCs) for those powers where the double lock has been introduced solely under the Act. We have not, however, included these figures for those powers where there has been a transition from a previous warrant regime; for example, the targeted interception figures therefore do not include the number of authorisations considered by the JCs as we believe that this would be misleading. However, we intend that this will be included in future years when all applications are made and considered under the IPA.

| | Considered by a JC | Approved, issued or given |
|--|--------------------|---------------------------|
| Covert human intelligence sources (CHIS) & Juvenile CHIS | – | 2,378 |
| Directed surveillance | – | 7,774 |
| Intrusive surveillance | – | 536 |
| Property interference under ISA section 5 | – | 594 |
| Property interference under Police Act 1997 | – | 1,735 |
| Bulk personal datasets – class warrant | 28 ³⁷ | 27 |
| Bulk personal datasets – specific warrant | 16 | 16 |
| Directions under section 219 | – | 0 |
| Directions under section 225 | – | 1 |
| Bulk communications data acquisition warrant | 1 | 1 |
| Communications data authorisation | – | 210,755 |
| Bulk interception warrants | 16 | 16 |
| Targeted examination interception warrant | 59 | 59 |
| Targeted interception warrant (including RIPA warrants) | – | 3,765 |
| Bulk equipment interference warrants | 3 | 3 |
| Targeted examination equipment interference warrants | 52 | 52 |
| Mutual assistance warrant | 0 | 0 |
| Targeted equipment interference warrants | 1,249 | 1,246 |
| Relevant sources | – | 735 |
| Request to retain LPP | 77 | 76 |

Table 6: Breakdown of authorisations, including those considered by a JC, 2018

Breakdown of the use of powers throughout 2018

18.5 The charts included in this chapter are intended to demonstrate trends in the use of investigatory powers across all of the authorities we oversee. Where it has been possible to do so, we have included individual details in the relevant chapter.

Covert Human Intelligence Sources (CHIS)

18.6 Use of a CHIS has broadly declined over the last decade for law enforcement, public authorities and local authorities (we do not have comparable statistics for prisons or the UK Intelligence Community, UKIC).

37 One application was rejected by the JC and was subject to an appeal as described in paragraphs 2.9-2.12.

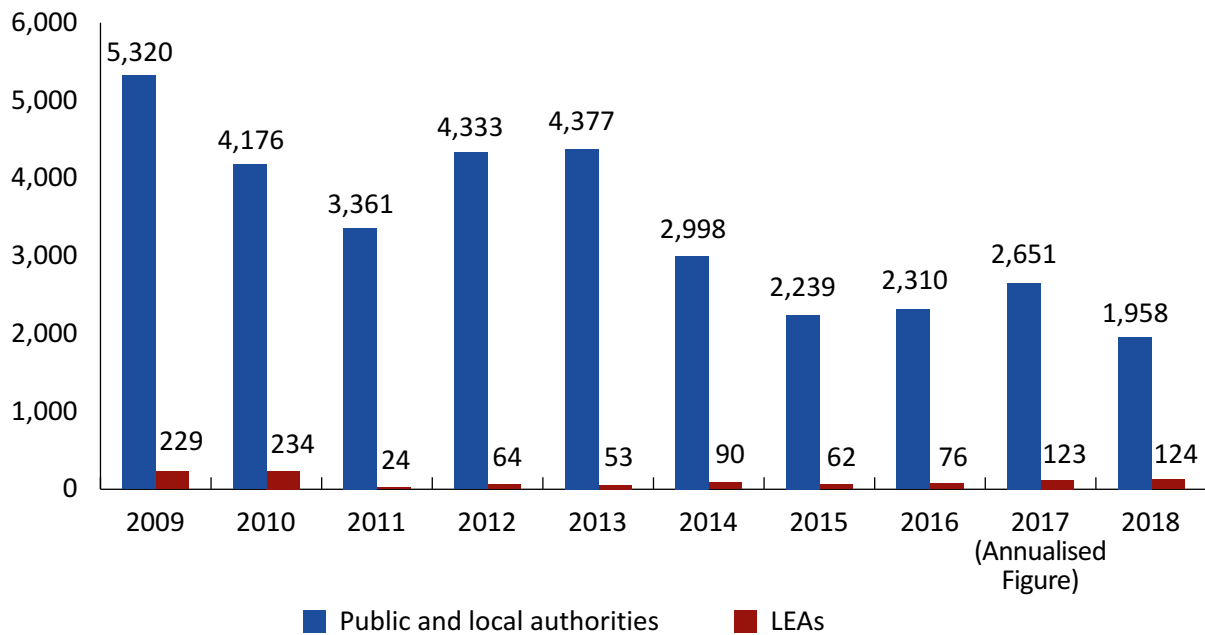


Figure 23: CHIS authorisations, law enforcement agencies and public and local authorities

18.7 For the use of relevant sources,³⁸ there has been little change from 2017 in the total number of undercover officer authorisations and the number of those renewed. Taking a longer-term view, the total number of authorisations has decreased from levels in excess of 1,000 each year between April 2014 to April 2016, which may be due to reduced availability of resources, or agencies finding alternative ways to tackle the criminality.

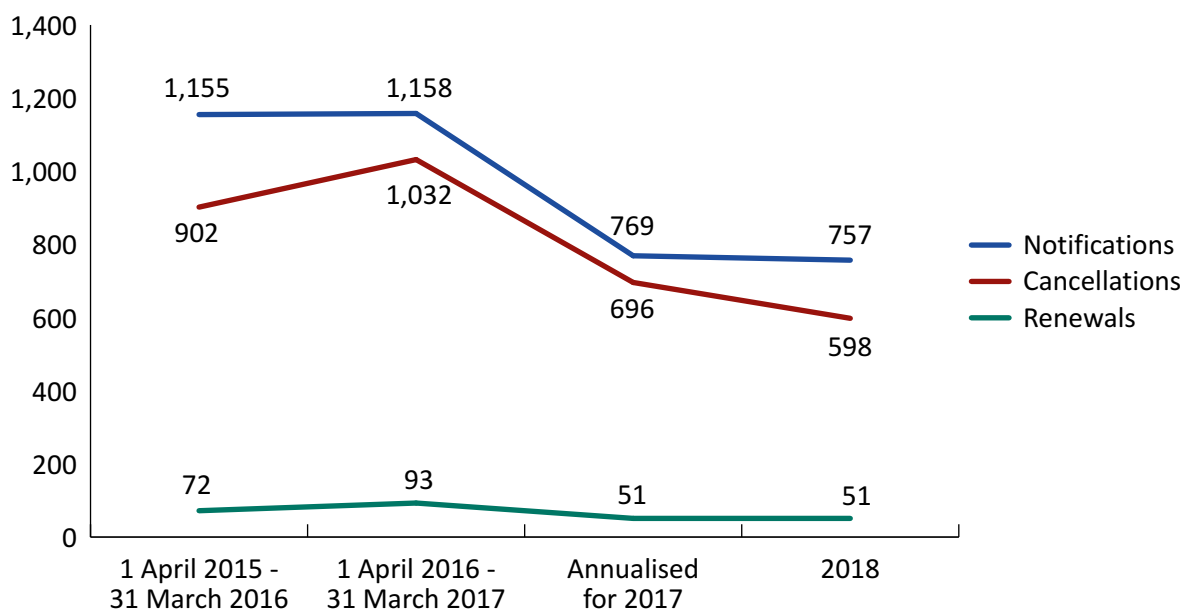


Figure 24: Relevant sources

³⁸ The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 (“the 2013 Relevant Sources Order”) further defines a particular type of CHIS as a ‘relevant source’. This is a source holding an office, rank or position with the public authorities listed in the Order and Annex B to the code. Enhanced authorisation arrangements are in place for this type of CHIS as detailed in the code.

Directed surveillance

18.8 The use of directed surveillance powers has been broadly consistent with 2017.

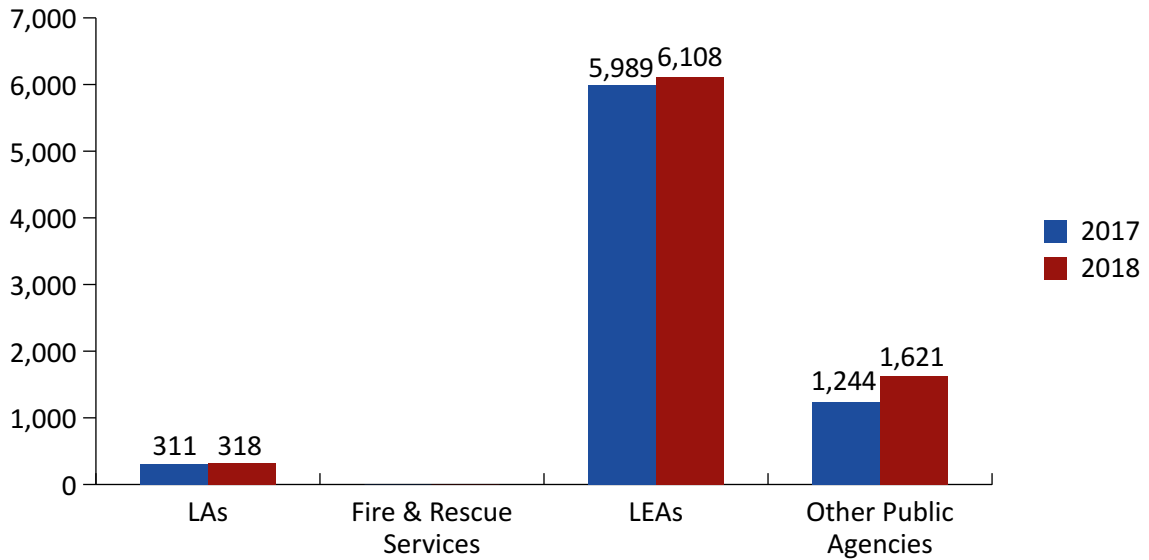


Figure 25: Directed surveillance across Law Enforcement Agencies and Public and Local Authorities in 2017 and 2018

Targeted Interception

18.9 Targeted interception authorisations have gradually increased in number since 2014. These figures include totals for law enforcement, UKIC and the Ministry of Defence (MOD). Of those, overall 6% of applications have been made under urgent provisions.

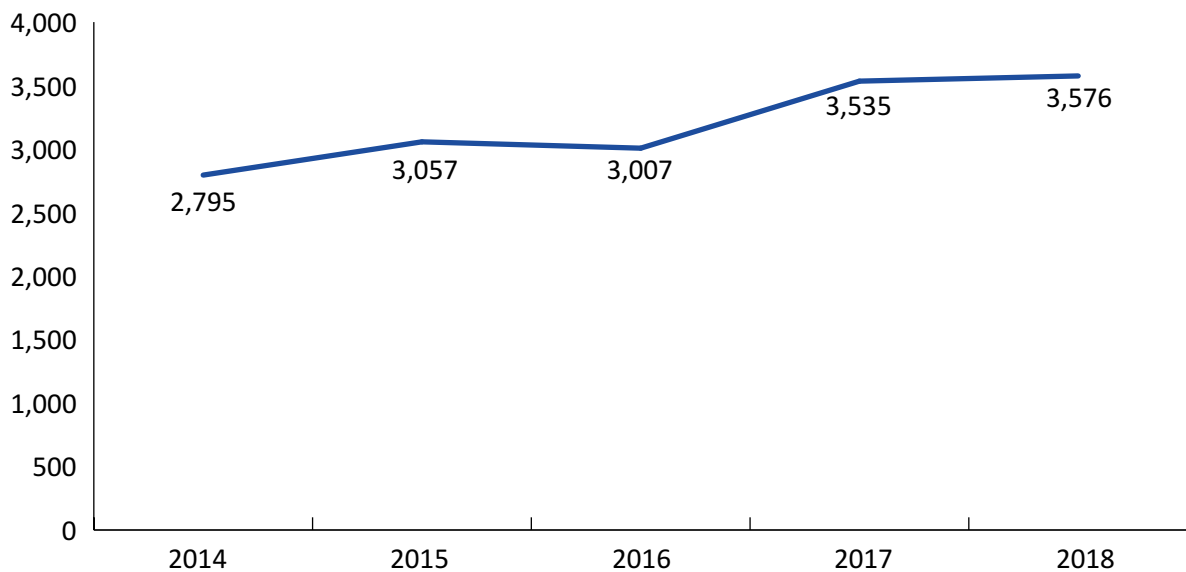


Figure 26: Targeted Interception authorisations, UKIC, MOD and LEAs 2014-2018

18.10 Retrospective oversight via the double lock has demonstrated that these provisions are being used appropriately, and we have found that, with the exception of the error identified at paragraphs 17.8-17.9, all urgent applications have been referred to JCs within the relevant timescale.

Communications Data (CD)

18.11 Details on targeted communications data (CD) applications, including the proportion of applications by data type and communications type are given in Chapters 12, 13 and 14. These figures cannot be provided for UKIC for national security reasons, although we can give a general overview of the extent of activity in this area. The greatest proportion of CD requests were made by law enforcement agencies, followed by UKIC.

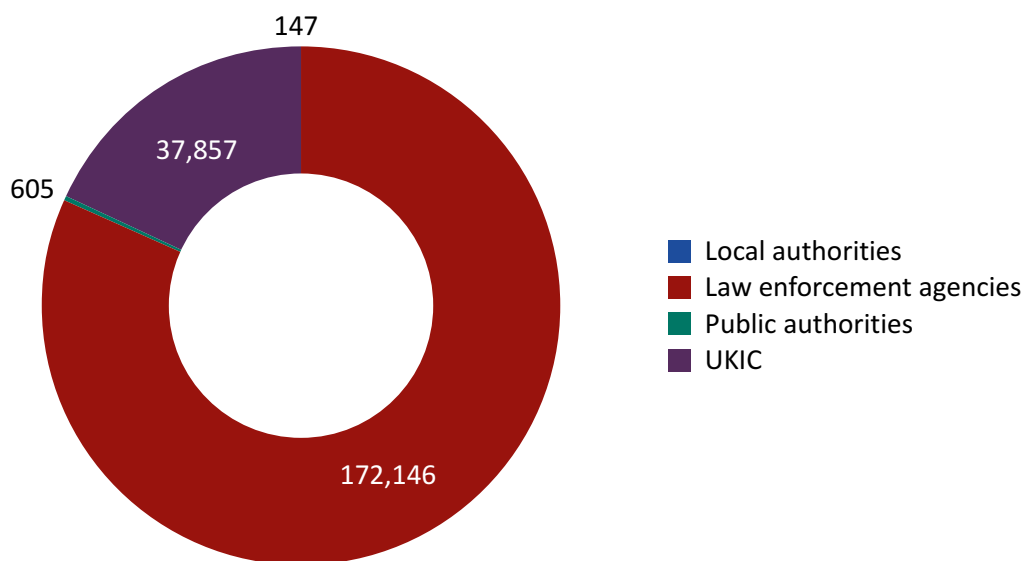


Figure 27: Targeted communications data applications by type of organisation, 2018

Bulk authorisations

18.12 We are unable to publish a full breakdown of bulk warrantry but, again, can give a general overview of the types of information collected. As this power was introduced under the IPA, there is no ability to compare authorisation figures with previous years.

18.13 Although oversight of bulk powers is not a new process, we have worked closely with the agencies to ensure that this is rigorous and effective. We have also worked with the JCs to ensure that the activities conducted under bulk warrants are those foreseen at the point of approval. By this means, we have been satisfied that the use of bulk powers is appropriate.

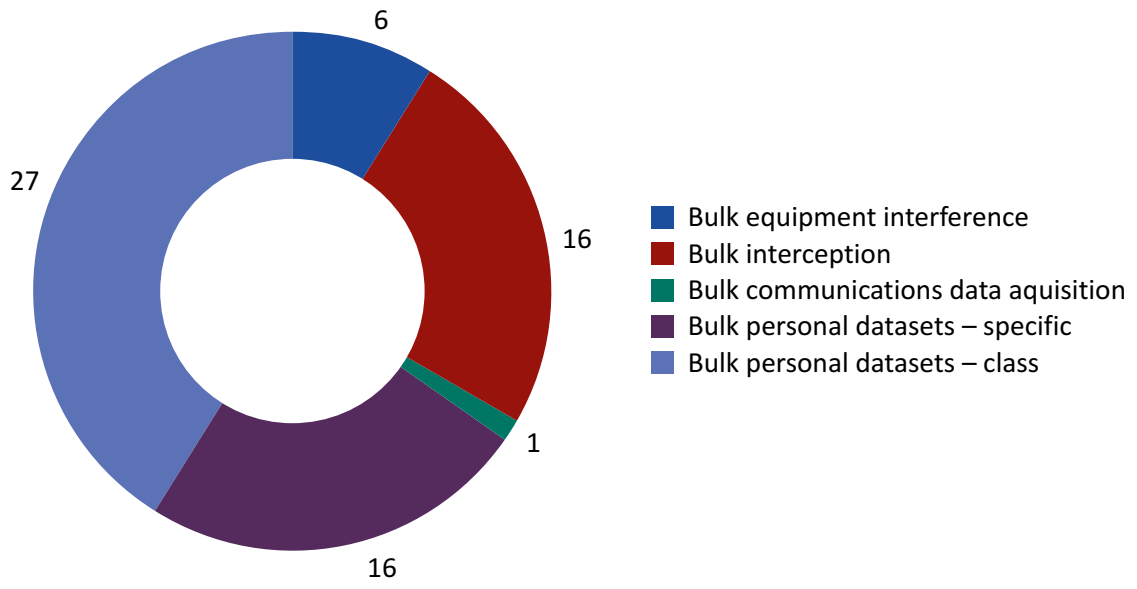


Figure 28: Bulk warrants requested, by type, 2018

Annex A: Glossary of Authorities

The following sets out how in this Annual Report has categorised the authorities we oversee.

| | |
|---------------------------------|--|
| Intelligence Agencies | <ul style="list-style-type: none"> • Secret Intelligence Service (SIS) • Security Service (MI5) • Government Communications Headquarters (GCHQ) <p>References to 'UKIC' mean the United Kingdom Intelligence Community. This may include Defence Intelligence. Note that Defence Intelligence do not have bulk powers under the Investigatory Powers Act 2016.</p> |
| Law Enforcement Agencies (LEAs) | <p>This refers to</p> <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) |
| Other Public Authorities (OPAs) | <ul style="list-style-type: none"> • British Broadcasting Corporation (BBC) • Care Quality Commission • Centre for Environment, Fisheries and Aquaculture Science (CEFAS) • Charity Commission • Competition and Markets Authority • Criminal Cases Review Commission • Department for Business Innovation and Skills (Insolvency Service) • Ministry for Housing, Communities and Local Government (MHCLG) • 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 Accident Investigation Branch (AAIB) • Department for Transport – Driver and Vehicle Standards Agency (DVSA) • Department for Transport – Marine Accident Investigation Branch (MAIB) |

| | |
|---|--|
| <p>Other Public Authorities (OPAs) <i>continued</i></p> | <ul style="list-style-type: none"> • Department for Transport – Maritime and Coastguard Agency (MCA) • Department for Transport – Rail Accident Investigation Branch (RAIB) • Environment Agency/Natural Resources Wales • 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, Childrens Services and Skills (OFSTED) • Her Majesty’s Prison and Probation Service (HMPPS) • Home Office Immigration & Enforcement and Border Force • Independent Office for Police Conduct (IOPC) • Information Commissioner’s Office (ICO) • 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 • Northern Ireland Office (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 • 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 • Welsh Assembly Government |
| <p>Local Authorities</p> | <p>All UK local authorities</p> |
| <p>Fire and Rescue Services</p> | <p>All separately constituted Fire and Rescue services in the UK</p> |
| <p>Ambulance Services</p> | <p>All UK Ambulance Services</p> |

Annex B: Budget

This table gives a breakdown of the Investigatory Powers Commissioner's Office's (IPCO) financial statement for the financial year for 2018/2019. This shows the first full year since IPCO's inception and shows an increased cost from previous years. This reflects the increase in staff, the recruitment of Judicial Commissioners (JCs), and the provision of independent accommodation. The financial statements from 2017, detailed in our Annual Report for IPCO and the three predecessor organisations, combined at £4,109,935.67.

| IPCO (Period 1/04/18 – 31/03/19) | |
|---|----------------------|
| Staff costs | £3,881,054.07 |
| Travel and subsistence | £363,788.93 |
| IT and Telecoms | £133,633.60 |
| Training and recruitment | £414.80 |
| Accommodation | £801,216.94 |
| Conferences and meetings | £21,552.98 |
| Office supplies, services and other costs | £112,165.34 |
| Legal | £56,242.67 |
| Total | £5,370,069.33 |

Annex C: Serious Errors

The Investigatory Powers Commissioner decided that this error amounted to a serious error (within the meaning of section 231 of the Investigatory Powers Act 2016). Accordingly, the Investigatory Powers Commissioner's Office (IPCO) notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal (IPT).

Error Investigation 1

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Special Point of Contact, SPoC) |
| Classification: | Transposition of Data |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Officers investigating the upload of indecent images of children to the internet had sought to identify the customer details of 14 separate IP (internet protocol) addresses used to commit the offences. An authorisation to acquire the information was granted, however whilst acquiring the data a wrong month was entered for one of the 14 addresses into the system portal used to collect the relevant details from Internet Service Provider. Despite an evident anomaly with the returned data, police officers still visited the address supplied to establish if there was any connection to the suspect. |
| Consequence: | Innocent person spoken to and eliminated from inquiries. |

Error Investigation 2

| | |
|----------------------------|--|
| | Police Force |
| Human or Technical: | Human (Special Point of Contact, SPoC) |
| Classification: | Transposition of Data |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers investigating the hacking of two email addresses and a file sharing application sought to identify the customer details of seven IP (internet protocol) addresses believed to have been used to commit the offences. After an authorisation to acquire the information had been granted, a series of errors were made when entering the data request into the system portal of the Internet Service Provider. As a result, erroneous information was returned and police visited three addresses to establish if there were any connections with the victim or suspected hacker. The proximity of one address visited to that of a potential suspect led officers to make an arrest of a person who was subsequently eliminated. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 3

| | |
|----------------------------|--|
| | Police Force |
| Human or Technical: | Human (Applicant/Special Point of Contact, SPoC) |
| Classification: | Misinterpretation of data |
| Data Acquired: | Email address – subscriber details |
| Description: | Following an arrest, a forensic examination of a seized computer was carried out. An email address was found on the device that was linked to a file sharing account on which a number of indecent images of children had been discovered. Police officers applied to acquire CD that would attribute this email address to the offending account. However, officers failed recognise that there was no process to verify identification when a person sets up this particular type of email address and that further checks and safeguards should have been applied. The name and address linked to this unverified email address led officers to arrest an innocent man. |
| Consequence: | The individual who was subject to this error made a complaint to the Investigatory Powers Tribunal (IPT). The IPT referred the case to IPCO for investigation. |

Error Investigation 4

| | |
|----------------------------|--|
| | Police Force |
| Human or Technical: | Human (Record Keeping) |
| Classification: | Incorrect Business Records |
| Data Acquired: | Location information |
| Description: | Police trying to locate a missing person who had indicated they intended to take their own life applied to acquire CD that could be used to identify a general location in which to focus their search. The telephone number used on the application had been associated to the missing person from an historic police record. The data returned related to an unconnected address and failed to assist in locating the missing person. The police reviewed the source record and after further enquiries established that when the record was created in 2015, an incorrect digit had been used when entering the telephone number. The missing person was later found deceased resulting in a referral to the Independent Office for Police Conduct and a subsequent investigation into potential police failings. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 5

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Applicant) |
| Classification: | Misinterpretation of data (Facebook Profile). |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police Officers trying to locate a person for whom welfare concerns had been raised, identified what they believed was their Facebook profile and as this was an urgent request, no verification of the profile identification was carried out. Data was sought to identify addresses from which this Facebook account had been accessed using the internet. The data returned identified an address that was visited by officers. On arrival it was established the person living at the address had the same name as the missing person but was not involved. It transpired that the two Facebook profiles were identical in name, but separated by a numerical suffix. |
| Consequence: | Police visited the premise of an individual unconnected to their search which delayed the welfare check. The missing person was subsequently found safe and well. |

Error Investigation 6

| | |
|----------------------------|--|
| | Police Force |
| Human or Technical: | Human (Applicant/Special Point of Contact, SPoC) |
| Classification: | Misinterpretation of data (Billing Address) |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers investigating the upload and sharing of indecent images of children identified three internet addresses used by the suspect and submitted an application seeking the customer details associated to these identifiers by the internet service provider. The application was authorised and data identifying the same customer address was received against all three transactions. Police officers attended the address and seized all internet enabled equipment but a subsequent forensic examination found nothing untoward. It transpired the data returned by the service provider related to the billing address only, and officers incorrectly assumed this was the installation address from where the internet service used would have been accessed. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 7

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Special Point of Contact, SPoC) |
| Classification: | Incorrect time conversion |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers investigating the upload and sharing of indecent images of children over a public WIFI service applied to obtain communication data that would assist to identify the offender. As the ability to acquire public WIFI data was a relatively new service, confusion arose when trying to determine the relevant time zone. The application was submitted in Greenwich Mean Time, when it should have been in British Summer Time, meaning the subsequent result was out by one hour. This led to police executing a warrant at the home of an innocent family. A re-examination of all similar service requests identified a second case where, although a warrant was not executed, all internet enabled devices were seized. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 8

| | |
|----------------------------|--|
| | Police Force |
| Human or Technical: | Human (Applicant) |
| Classification: | Transposition (Verbal) |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers trying to locate a vulnerable missing person applied using the urgency provisions for information that would identify a location from which an internet service had been accessed. During the urgent oral process the last digit of the internet address concerned was not given and as a result, the application returned data relating to a customer who had no connection to the incident. The correct internet details were subsequently identified and although a delay had been caused by the initial error, the person was found safe and well. |
| Consequence: | Police visited the premise of an individual unconnected to their search. |

Error Investigation 9

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Special Point of Contact, SPoC) |
| Classification: | Misinterpretation of data (Returned) |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers investigating defamatory posts over social media applied for data that would assist in identifying the users of relevant accounts through their profiles, and the locations from which they had accessed the internet. Misinterpretation of the data files returned led officers to execute a warrant on an innocent family with all internet devices seized. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 10

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Applicant) |
| Classification: | Transposition (Application) |
| Data Acquired: | Subscriber information relating to a mobile telephone number |
| Description: | Police officers trying to identify the vulnerable victim of a sexual grooming offence applied to acquire the subscriber details from a telephone number found during examination of the offender's telephone. When completing the application the officer made an error when entering the telephone number. The application was approved and a name and address for another number was obtained. The police made contact with this unconnected subscriber via a telephone call. |
| Consequence: | The Police made contact with a person unconnected to their search. |

Error Investigation 11

| | |
|----------------------------|--|
| | Police Force |
| Human or Technical: | Human (Special Point of Contact, SPoC) |
| Classification: | Incorrect Time Conversion |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers investigating the upload and sharing of indecent images of children applied for communication data to identify the address from which the offender had accessed the internet. At the point of application and approval the details of the information sought were accurate. However, when the request was submitted to the internet service provider, an incorrect time zone was entered and consequently the information returned by the service provider was out by one hour. Internet Protocol address used to access internet services are not fixed, and during that hour this identifier had passed on to another customer. As a result of the error an innocent person was subsequently arrested. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 12

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Applicant) |
| Classification: | Transposition (Reporting) |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers seeking to locate a vulnerable person had been supplied details of an internet address believed to have been used by this person for recent contact. Internet addresses are made up of eight separate groups of numbers separated by full stops. In the number taken down by the officers, no full stops were used. Unable to recontact the initial caller, the police with the help of the Internet Service Provider narrowed down the combination to two potential options. The first result identified a local address that was visited and transpired to be unconnected. The second result identified a further address 100 miles away in another force area at which the person was located safe and well. |
| Consequence: | Police made contact with a person unconnected to their search. |

Error Investigation 13

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Special Point of Contact, SPoC/Telecommunications Operator, TO) |
| Classification: | Transposition (Verbal) |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers seeking to locate a vulnerable person had been supplied details of an internet address believed to have been used for recent contact with the person raising the concern. Following a verbal authorisation and given the urgency, the Internet Service Provider was contacted to obtain the customer details. In the verbal transfer a two-digit house number was incorrectly recorded as a single digit house number. Officers attended this address and established there was no connection with the vulnerable person. The internet company was re-contacted, and the error was identified. Officers returned to the same street and located the person safe and well. |
| Consequence: | Contact made with a person unconnected to their search. |

Error Investigation 14

| | |
|----------------------------|---|
| | Police Force |
| Human or Technical: | Human (Applicant) |
| Classification: | Incorrect Time Conversion |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police Officers investigating sexual offences related to online grooming applied for communication data to identify all details and internet addresses associated to the offender's user name. Accurate data was provided by the service provider but when preparing applications to identify the location from which internet services had been accessed, a conversion to Greenwich Mean Time was required. In doing so, a period of 5 hours was subtracted instead of being added which led to incorrect information being obtained and a warrant was subsequently executed at an innocent's address. No arrests were made in this instance but devices were seized and examined. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 15

| | |
|----------------------------|---|
| | Telecommunications Operator (TO) |
| Human or Technical: | Human (TO) |
| Classification: | Incorrect Data |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution |
| Description: | Police officers investigating the sharing of indecent images of children via an online chat room sought communication data to identify the locations from which internet services had been accessed. The application submitted contained accurate information and following authorisation, a notice to supply the information was submitted to the internet service provider. The data returned identified the relevant location as a business address, however, after police visited this company it transpired the data supplied by the telecommunications operator had been incorrect. |
| Consequence: | Police made contact with a company unconnected to their investigation. |

Error Investigation 16

| | |
|----------------------------|---|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification | Shortfall Data |
| Data Acquired: | File sharing activity |
| Description: | A file sharing company based outside the UK reported a 'bug' in certain files that had impacted 57 sets of data provided to UK law enforcement agencies in response to applications for communication data. Urgent checks identified the software had returned a short fall of data for the period requested, but the data that had been returned was accurate. |
| Consequence: | Urgent checks were carried out revealing under-disclosure rather than inaccurate disclosure. |

Error Investigation 17

| | |
|----------------------------|--|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification: | Incorrect Data |
| Data Acquired: | Call records |
| Description: | Incorrect system coding led to call data records provided to a police force in response to an authorisation to obtain communication data being out by one hour in the supplied PDF document. A second file provided in Excel format however was accurate, and as this is the preferred file format for use by intelligence analysts, the error had no negative impact. |
| Consequence: | No impact as second file supplied (Excel) was accurate and is the preferred file used for analysis. |

Error Investigation 18

| | |
|----------------------------|--|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification: | Incorrect Data |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution (IPAR) |
| Description: | Police officers investigating sexual offences relating to online grooming, sought communication data connected to the suspect's username and internet addresses associated to the activity. The data returned was based on the same username but with a space between the name and a set of double digits (abc19 v abc 19). This error was not spotted and consequently further applications to identify the user of the internet address were flawed. Consequently, the information supplied in response to the further applications was erroneous and led to the arrest of an innocent person. |
| Consequence: | The IPC decided that this error amounted to serious error (within the meaning of section 231 IPA). Accordingly, IPCO notified the affected person of the fact of the serious error and of that person's right to apply to the Investigatory Powers Tribunal. |

Error Investigation 19

| | |
|----------------------------|--|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification: | Incorrect Data |
| Data Acquired: | Subscriber information relating to an Internet Protocol Address Resolution and associated email address |
| Description: | Police officers investigating the upload and sharing of indecent images of children applied for communications data to identify the location from which internet services were being accessed. A further application was submitted to identify the user of an associated email address. An inordinate delay in receiving this result from a service provider outside the UK led officers concerned for the welfare of children to execute a warrant based on the internet location result only. A short time after this warrant, the email result was returned and inexplicably identified a different address and person. This person was arrested however, no incriminating material was found in either case. From the enquiries conducted by IPCO to date it appears that the applications submitted by the police were accurate, and as yet a system fault has not been identified by the service provider. |
| Consequence: | The criminal investigation and the source of the potential error remain under investigation. |

Error Investigation 20

| | |
|----------------------------|---|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification: | Shortfall of Data |
| Data Acquired: | Subscriber information (email addresses). |
| Description: | As a result of an incorrect feed into the disclosure system that provides information from the telecommunications operator in response to authorisations granted to acquire communication data, negative returns were provided to police forces when relevant data was in fact available and should have been supplied. |
| Consequence: | For those where data was still available (18 out of 21) each police force was advised and invited to reapply. Just two eventually led to enforcement action. |

Error Investigation 21

| | |
|----------------------------|--|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification: | Shortfall Data |
| Data Acquired: | Cell site activity |
| Description: | Following a query by a law enforcement agency it was established that the results of 51 requests to acquire communications data associated to a specific cellular mast sites had certain data sets missing. The 51 requests related to 17 separate investigations from different police forces and agencies. |
| Consequence: | In three cases the missing data had no impact. In four further cases, where the missing data was subsequently acquired, no negative impact resulted. In the remaining 10 cases the missing data could not be acquired as the data retention period had expired and the information was no longer available. As such the authorities concerned could not provide an assessment as to whether or not the shortfall affected the overall outcome of the investigation |

Error Investigation 22

| | |
|----------------------------|--|
| | Telecommunications Operator (TO) |
| Human or Technical: | Technical |
| Classification: | Shortfall Data |
| Data Acquired: | Call records |
| Description: | <p>Following a query from a public authority as to the extent of data returned in response to an authorisation granted for a special service request, a telecommunications operator identified a system error that had resulted in a shortfall of information being supplied between August 2017 and August 2018. In total, 51 authorisations from 11 public authorities had been supplied with an incomplete range of data. The fault was identified and corrected within a few days of the anomaly being raised.</p> |
| Consequence: | <p>Where the data was still available and could be reapplied for, there was no discernible impact. For those cases where data retention schedules meant the data had been deleted and was therefore no longer available, the public authorities concerned have been unable to say whether or not the shortfall affected the overall outcome of the investigation.</p> |

Annex D: Communications Data

This annex details the use of communications data (CD) in 2018. The below tables give a breakdown of applications from each agency, and the number of applications made in relation to sensitive professions.

Sensitive professions

47 authorities applied for CD in relation to individuals of sensitive professions in 2018. These figures do not include any applications from local authorities as, in 2018, these authorities were not able to apply for events data or traffic data. It is worth noting that in the majority of these cases, the application related to the protection of a witness or victim, for example in the case of harassment of an individual who falls into one of these professions. Because of the sensitivity of these applications, we have not provided any real examples of use. The relevant applications break down as follows:

| Profession | |
|----------------------|--------------|
| Lawyer | 234 |
| Journalist | 203 |
| Member of Parliament | 113 |
| Minister of Religion | 272 |
| Medical Doctor | 498 |
| Total | 1,320 |

Applications by authorisation

The table below gives figures for the total number of items of CD sought within each notice given or authorisation granted, including those granted under the urgency provisions. In total, 808,214 items of CD were applied for and obtained in 2018. This is a slight increase from the 757,977 items acquired in 2017 and 754,559 in 2016. Unfortunately, because of difficulties in obtaining accurate statistics from CD workflow systems, and because of changes to new systems in a handful of cases, there is a small margin of error on this figure on those in the table below. In a small number of cases, we believe that these figures may be inaccurate to a degree of around 10%; we believe that is not likely to result in inaccuracies of more than 1% of our total figure.

| Name | Line Items | Type of Authority |
|--|------------|---------------------|
| Government Communications Head Quarters (GCHQ) | 24,047 | Intelligence Agency |
| MI5 | 82,060 | Intelligence Agency |
| Secret Intelligence Service (SIS) | 226 | Intelligence Agency |
| Air Accidents Investigation Branch (AAIB) – Department for Transport (DfT) | 0 | Public Authority |
| Child Maintenance Group (Department for Work and Pensions) | 0 | Public Authority |
| Competition and Markets Authority | 64 | Public Authority |
| Criminal Cases Review Commission | 3 | Public Authority |
| Department for the Economy for Northern Ireland | 51 | Public Authority |
| Financial Conduct Authority | 2,340 | Public Authority |
| Gambling Commission | 30 | Public Authority |
| Gangmasters and Labour Abuse Authority | 158 | Public Authority |
| Health & Safety Executive | 15 | Public Authority |
| Health & Social Care Northern Ireland | 0 | Public Authority |
| Her Majesty's Prison and Probation Service | 932 | Public Authority |
| Independent Office for Police Conduct | 84 | Public Authority |
| Information Commissioner's Office | 13 | Public Authority |
| Maritime & Coastguard Agency | 3 | Public Authority |
| Maritime Accident Investigation Branch | 0 | Public Authority |
| Maritime Management Organisation | 0 | Public Authority |
| Medicines and Healthcare Products Regulatory Agency | 170 | Public Authority |
| National Anti Fraud Network | 734 | Public Authority |
| Northern Ireland Prison Service | 0 | Public Authority |
| Office of Communications | 38 | Public Authority |
| Office of the Police Ombudsman for Northern Ireland | 45 | Public Authority |
| Police Investigations and Review Commissioner | 0 | Public Authority |
| Rail Accident Investigation Branch | 2 | Public Authority |
| Serious Fraud Office | 663 | Public Authority |
| Avon and Somerset Police | 15,033 | Police |
| Bedfordshire Police | 4,873 | Police |
| British Transport Police | 3,603 | Police |
| Cambridgeshire Constabulary | 3,215 | Police |
| Cheshire Constabulary | 12,531 | Police |
| City of London Police | 3,895 | Police |
| Cleveland Police | 4,317 | Police |
| Cumbria Constabulary | 5,449 | Police |
| Derbyshire Police | 7,053 | Police |
| Devon and Cornwall Police | 19,180 | Police |
| Dorset Police | 5,001 | Police |
| Durham Constabulary | 5,720 | Police |

| Name | Line Items | Type of Authority |
|---|------------|---------------------------|
| Dyfed Powys Police | 4,970 | Police |
| Gloucestershire Police | 2,147 | Police |
| Greater Manchester Police | 39,898 | Police |
| Gwent Police | 5,483 | Police |
| Hampshire Constabulary | 8,021 | Police |
| Hertfordshire Constabulary | 12,244 | Police |
| Her Majesty's Revenue & Customs | 18,263 | Law enforcement |
| Home Office Immigration Enforcement | 7,297 | Law enforcement |
| Humberside Police | 6,393 | Police |
| Kent and Essex Police | 22,321 | Police |
| Lancashire Constabulary | 15,993 | Police |
| Leicestershire Police | 10,969 | Police |
| Lincolnshire Police | 4,134 | Police |
| Merseyside Police | 22,022 | Police |
| Metropolitan Police Service Central Intelligence Unit (CIU) | 106,902 | Police |
| Metropolitan Police Service Department for Professional Standards (DPS) | 1,824 | Police |
| Metropolitan Police Service Counter Terrorism Command (SO15) | 3,891 | Police |
| Ministry of Defence | 117 | Defence |
| Ministry of Defence (Intel) | 0 | Intelligence – Defence |
| National Crime Agency | 48,175 | Law enforcement |
| Norfolk and Suffolk Constabulary | 5,619 | Police |
| North Wales Police | 7,245 | Police |
| North Yorkshire Police | 4,876 | Police |
| Northamptonshire Police | 12,280 | Police |
| Northumbria Police | 9,699 | Police |
| Nottinghamshire Police | 12,478 | Police |
| Police Scotland | 41,553 | Police |
| Police Service Northern Ireland | 8,632 | Police |
| Port of Dover Police | 0 | Police |
| Royal Air Force Police | 12 | Police |
| Royal Military Police | 439 | Police |
| South Wales Police | 11,833 | Police |
| South Yorkshire Police | 10,883 | Police |
| Staffordshire Police | 7,746 | Police |
| Surrey Police | 7,517 | Police |
| Sussex Police | 7,233 | Police |
| Thames Valley Police | 14,163 | Police |

| Name | Line Items | Type of Authority |
|-------------------------------------|------------|-------------------|
| West Mercia and Warwickshire Police | 18,327 | Police |
| West Midlands Police | 52,724 | Police |
| West Yorkshire Police | 26,852 | Police |
| Wiltshire Police | 5,473 | Police |

Annex E: Public Engagements

The Investigatory Powers Commissioner undertook several public engagements in 2018. Details of those engagements are given below.

The CEO of the Investigatory Powers Commissioner's Office (IPCO) engaged with Non-Governmental Organisations (NGOs) to discuss their interests in the use of investigatory powers and met representatives from Reprieve and Privacy International in July 2018.

Engagement with overseas bodies

- 6 April – CNCTR (International Oversight Bodies) Conference, Paris, France
- 25 April – G10 Control Commission/Chancery meeting, Berlin Germany
- 9 May – meeting with German Parliamentary Intelligence Oversight Committee (London, UK)
- 19 June – meeting with Joe Cannataci, UN Special Rapporteur on the Right to Privacy (London, UK)
- 25 June – meeting with the Canadian Child Sexual Exploitation (CSE) Commissioner (London, UK)
- 11 July – meeting with Georgian delegation (London, UK)
- 16 July – meeting with Dr James Renwick, Australia's Independent National Security Legislation Monitor (London, UK)
- 19 July – meeting with Christian Porter, Australian Attorney General (London, UK)
- 17 September – visit by Federal German Parliamentary 'G-10' control commission (London, UK)
- 20 September – meeting with German Independent Committee, Berlin, Germany
- 28 November – meeting with Dennis Richardson AC, Australia (London, UK)
- 7 December – CNCTR (International Oversight Bodies) Conference, Paris, France

Meetings with Ministers

- 24 April – meeting with the Home Secretary, Amber Rudd MP
- 19 June – meeting with Security Minister, Ben Wallace MP
- 25 July – meeting with the Home Secretary, Sajid Javid MP
- 15 November – meeting with Cabinet Secretary for Local Government and Public Services, Welsh Government, Alun Davies MP
- 29 November – meeting with the Foreign Secretary, Jeremy Hunt MP

Engagement with NGOs

- 12 December – Chatham House event on Consolidated Guidance

Engagement with the media

- 13 June – interview with Hayden Smith, Press Association
- 26 June – interview with Joshua Rozenberg

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

CCS0819890016
ISBN: 978-1-5286-1604-1