

IPCO

Investigatory Powers
Commissioner's Office

OCDA

Office for Communications
Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2020



Investigatory Powers
Commissioner's Office



Office for Communications
Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2020

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 6 January 2022

Laid before the Scottish Parliament by the Scottish Ministers 6 January 2022

HC 897

SG/2022/1



© Crown copyright 2022

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 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

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/government/publications

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

ISBN 978-1-5286-3008-5

E02694090 01/22

Printed on paper containing 75% recycled fibre content minimum.

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

Contents

	Letter to the Prime Minister	7
1	Introduction by the Investigatory Powers Commissioner, Sir Brian Leveson	8
2	IPCO operations and the impact of Covid-19	11
3	Legal and policy	16
4	Protecting confidential or privileged information	22
5	Communications and engagement	25
6	Technology Advisory Panel	29
7	Office for Communications Data Authorisations: operational developments	34
8	Office for Communications Data Authorisations: observations	37
9	MI5	39
10	Secret Intelligence Service	46
11	Government Communications Headquarters	51
12	The Ministry of Defence	62
13	The Principles	64
14	Law Enforcement Agencies and Police	73
15	Wider Public Authorities	100
16	Local Authorities	105
17	Prisons	111
18	Warrant Granting Departments	117
19	Errors	119

20	Statistics	131
Annex A	Definitions and glossary	147
Annex B	Budget	156
Annex C	Serious errors	157
Annex D	Public engagements	179

Letter to the Prime Minister

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

November 2021

Dear Prime Minister,

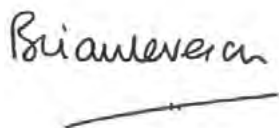
I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) from 1 January to 31 December 2020.

Although this is my third report to you as the Investigatory Powers Commissioner, it actually covers my first full year in the role. This report includes information on the use of covert powers by UK authorities and, specifically, the details required under section 234 of the Investigatory Powers Act 2016. For 2020, unlike previous years, I am pleased that we have been able to cover all relevant issues in this report; I have not, therefore, written to you separately about matters which should not be published for reasons of national security. I will, of course, continue to provide a confidential annex in future years when the need arises.

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.

Over the last year, the work of both IPCO and OCDA has been inevitably affected by the Covid-19 pandemic. Both offices have had to adapt their ways of working to ensure that we could maintain both our authorisation regimes and our oversight responsibilities. I am grateful to all for their exceptional dedication and professionalism during this challenging period.

Yours sincerely,



The Rt Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

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

This Annual Report covers my first full year as Investigatory Powers Commissioner (IPC) and presents the findings from a year that has been challenging both for my teams and all of the public authorities we work with. I am very pleased to say that, despite those challenges, both the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) have had a highly successful year and have maintained the strong and accountable oversight model we have worked hard to establish.

As required by section 234 of the Investigatory Powers Act 2016 (IPA), this Report sets out details of the how the functions of the Judicial Commissioners (JCs) were carried out during 2020. I have also chosen, although I am not obliged by legislation, to provide additional information on the activities of OCDA which also operates under my jurisdiction as the IPC.

We set out in Chapters 2 and 7 the particular issues faced by the two organisations as a result of the pandemic. I am very grateful to all of those in IPCO and OCDA who attended the office throughout 2020 to ensure that our critical work was done, as well as to those who adjusted their ways of working to ensure we have been able to continue to meet our statutory functions while working from home. I am confident that, for IPCO and OCDA, working through these challenges has helped us forge stronger relationships with those we oversee and identified more efficient practices which will improve our oversight far beyond the response to the Covid-19 restrictions.

I would like to express particular thanks for the contribution of the 10 temporary Judicial Commissioners, who were appointed in April 2020 under the terms of section 22 of the Coronavirus Act 2020, and for the exceptional efforts of Lord Justice Fulford, the previous IPC, who was appointed as a JC by the Prime Minister at the start of the March 2020 lockdown. All stepped in during the early stages of the pandemic to enable IPCO to continue its scrutiny of warrant applications while protecting those JCs considered to be at greater risk were they to contract Covid-19 due to their age. I also wish to thank the Lord Chief Justice of England and Wales, the Master of the Rolls and the President of the Queen's Bench Division for allowing and facilitating the loan of the temporary JCs, all of whom were serving judges, to assist IPCO during this challenging time. This was critical to enable IPCO to maintain the same standard of independent review throughout this period.

For 2020, in summary, it is clear that the public authorities I oversee continue to take seriously their duty to comply with the law when exercising investigatory powers. There are, however, a few issues I feel that I should highlight at this point. Inevitably, when undertaking an exercise such as this, one tends to focus on areas posing particular difficulties but I should stress that the list of issues that follows does not detract from the strong culture of compliance seen by my Inspectors on their visits. In any event, the concerns I set out below are directed towards problems of a more systemic nature and do not indicate any fault on the part of individual officers exercising the powers on a day-to-day basis:

- **Bulk interception:** the later sections of this report set out the legal position on bulk interception as it stood at the end of the year,¹ namely that the European Court of Human Rights had issued a first instance judgment on the compatibility of the UK's bulk interception regime with the Convention but that an appeal was outstanding. Judgment in that appeal was, in fact, handed down in May 2021 when the Grand Chamber identified a number of violations of the Convention in the way the bulk interception regime operated in 2017. Importantly for the work of IPCO, the Court decided that the selection for examination of bulk interception data must be subject to internal approval within the Government Communications Headquarters (GCHQ) and that, where it is highly likely that confidential journalistic material would be identified through that selection for examination, judicial approval must be sought. Discussions continue with the Government as to what changes will be implemented to comply with the judgment, all of which will have important implications for how this strategically significant investigatory power is overseen by IPCO in the future.
- **The Principles:** at the start of 2020, The Principles came into force, replacing the Consolidated Guidance as the policy governing the conduct of personnel exchanging intelligence relating to detainees overseas. This report outlines some of the challenges which arose when implementing the new policy; foremost among these was a lack of clarity about how personnel should proceed when there is a real risk a detainee has been, or will be, subject to mistreatment but there is no causal link between that mistreatment and the actions of UK personnel. In addressing this issue, the organisations subject to The Principles have agreed with the Cabinet Office a policy on 'no causal link' cases which addresses some of the ambiguities which have inadvertently crept in as a result of the transition from the Consolidated Guidance. We include more detail on this in Chapter 13 of this report.
- **Compliance of systems handling warranted data:** the problems experienced in MI5 in 2019 regarding the handling of warranted data, which are subject to ongoing litigation, were not unique. In 2020, through the continuation of IPCO's data assurance programme, we have looked in more detail at systems handling warranted data across the UK intelligence community (UKIC) and law enforcement. Given the pressure to introduce innovative systems and technologies in response to evolving threats, it is inevitable that compliance challenges will arise and I am pleased to see the growing understanding of the importance of this issue across the organisations we oversee. However, I remain highly reliant on public authorities raising with me, at a suitably early stage, any compliance problems which do arise. I am pleased that, for the most part, public authorities are doing so and am assured that the delays in disclosure, which are currently subject to the Investigatory Powers Tribunal case, are unlikely to arise again in the future.
- **Interception in prisons:** as is clear from Chapter 17, we are continuing to work with Her Majesty's Prisons and Probation Service on the arrangements for interception of communications in prisons. We are keen to ensure that the rules and arrangements underpinning the interception and monitoring of prisoners' communication are robust and that all authorisations meet the required necessity and proportionality thresholds.

These issues in themselves set 2021 up as another challenging year and we will continue to keep them under close review. We have also seen the implementation of the Covert Human Intelligence Sources (Criminal Conduct) Act 2021, which introduces a requirement on public authorities to notify a JC when a covert human intelligence source or undercover officer is authorised to carry out a criminal offence. Such conduct was already subject to oversight by IPCO but the notification process brings these matters to our attention in a more timely way and will allow us to focus

1 See: from paragraph 11.24.

more quickly on any potential areas of concern. We will provide more information on the first few months of operation in our 2021 Annual Report.

It is an important principle for me that my oversight responsibilities should clearly be defined and underpinned by statute. It is understandable that, exceptionally, interim positions do have to be found; current examples include oversight of the GCHQ Equities Process, which the previous IPC took on at the request of the Director, and the inclusion of the National Crime Agency and SO15 in my oversight of The Principles Relating to the Detention and Interviewing of Detainees Overseas. Discussions are underway with the Government on the most appropriate options for that essential clarity and I will provide more information on the IPCO website once agreed.

I end by emphasising what I have said above, that I am grateful to those who assist us with completing our work and am pleased with the overall levels of compliance that are highlighted in this report.

2. IPCO operations and the impact of Covid-19

Overview

- 2.1 In common with all public authorities, Covid-19 created unprecedented challenges for the Investigatory Powers Commissioner's Office (IPCO). In the weeks preceding the Prime Minister's first address to the nation on 16 March 2020, we began reviewing our business continuity plans for all eventualities as it was anticipated that the UK may follow other countries and implement a nationwide lockdown.
- 2.2 The outbreak of Covid-19 resulted in global debate about the balance between maintaining civil liberties and measures to protect public health, as governments around the world adopted various approaches in an effort to combat the spread of the virus. In a time of national crisis, it would be easy to dispense with the oversight of investigatory powers as a distraction to maintaining the core business of government. However, it is of course, during national crises that the risk of the misuse of investigatory powers is greatest and the oversight of civil liberties is arguably never more important. Our aim from the outset was clear: the oversight of investigatory powers must continue and we should find innovative ways to achieve this while protecting our staff. This would mean new legislation, new Judicial Commissioners (JCs) and the introduction of remote inspections.

Legislation

- 2.3 In early March 2020, we engaged in extensive dialogue with the Home Office with a view to identifying what legislative changes (if any) were required in order to ensure that IPCO was able to maintain business continuity as the pandemic started to grip the UK. It was identified that JCs might need longer to consider urgent warrants and that there might be a need to temporarily replace the JCs should they be unable to carry out their duties as a result of ill health or other reasons. The potential impacts on national security and law enforcement operations were clear if there was not a JC available to consider the necessary applications.
- 2.4 As an immediate contingency, the Investigatory Powers Commissioner (IPC) asked the Prime Minister to reappoint Sir Adrian Fulford as a JC. Sir Adrian had stood down as the IPC in October 2019 to take up the position of Vice-President of the Court of Appeal (Criminal Division). He was keen to assist as far as possible around his court commitments and the Prime Minister approved his appointment at the end of March.
- 2.5 On 19 March 2020, the Government introduced the Coronavirus Bill before Parliament. On 23 March 2020, the Prime Minister announced the UK's first national lockdown, telling the public to "stay home". On 25 March, the Coronavirus Act 2020 received Royal Assent and included enabling powers at sections 22 and 23 for the Secretary of State to make regulations for the appointment of JCs and for the extension of the time limits in respect of urgent warrants. These regulations could only be exercised if the IPC informed

the Secretary of State that they were necessary. The IPC did this on 26 March,² and the Security Minister made The Investigatory Powers (Temporary Judicial Commissioners and Modification of Time Limits) Regulations 2020 on the same day. The Regulations came into force on 27 March.³

Temporary Judicial Commissioners

- 2.6 The senior demographic of the JCs (all but one of whom was over the age of 70), presented IPCO with a unique business continuity challenge. The Government's guidance at the time stated the advice on social distancing would be "particularly important" for those over the age of 70 who were classified as "clinically vulnerable" due to the greater risk of death or serious illness from contracting the virus. It was uncertain whether this advice would change and further restrict the movements of the over 70s or how long the pandemic might persist. A decision was taken that the powers in the Coronavirus Act to appoint temporary JCs should be exercised on the basis that the JCs should not be placed at risk by, among other things, having to travel (often great distances) to attend the office to consider applications in a secure environment. The Investigatory Powers (Temporary Judicial Commissioners and Modification of Time Limits) Regulations 2020 made it possible to appoint temporary JCs provided they held or had held high judicial office. This resulted in the appointment of 10 temporary JCs, all of whom were under the age of 70 (and therefore not considered clinically vulnerable) and whom were all serving judges of the High Court or Court of Appeal of England and Wales.⁴
- 2.7 The temporary JCs were appointed for a period of six months. They were subject to a rapid, but comprehensive training programme and supported by members of IPCO's Legal Team and Inspectorate throughout their time in post. By August, lockdown restrictions had eased, infection rates had fallen, and IPCO had been able to implement measures to create a Covid-secure workplace. In the light of these developments, a decision was made to begin to roster the original JCs back for office duty. The temporary JC appointments were not renewed; instead they were held in reserve should there be further guidance impacting the clinically vulnerable (the law only permitted a maximum appointment for 12 months in total and it was unclear whether further lockdowns would necessitate their reappointment at a later date). At the time of writing, it has not been necessary to reappoint the temporary JCs.

Time limits for urgent warrants

- 2.8 Section 23 of the Coronavirus Act enabled the extension of the 'relevant period' for urgent warrants. While this was a useful flexibility to have in the early days of the pandemic, both for public authorities and for our JCs, in reality it did not prove necessary to exercise this power to the extent to which we had originally anticipated and the majority of warrants were authorised within the usual timeframes. For this reason, in February 2021, the IPC confirmed to the Home Secretary that he did not think it necessary to extend the regulations which brought this power into force.

2 See: <https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/26032020-Letter-to-Home-Secretary-requesting-emergency-powers-be-exercised.pdf>

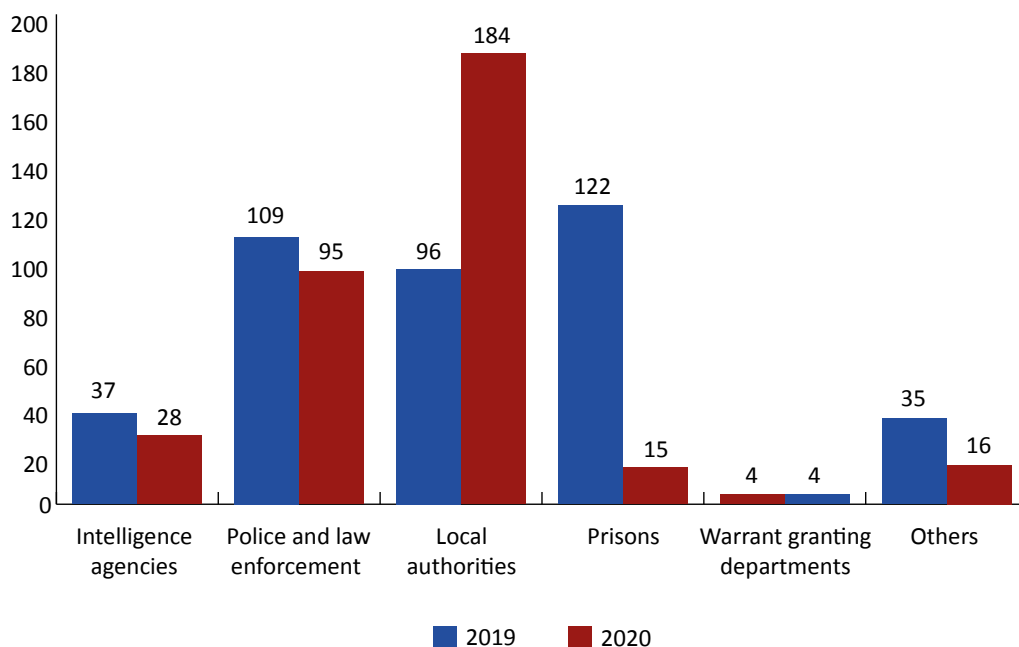
3 These Regulations ceased to have effect 12 months after they come into force.

4 See: <https://www.ipco.org.uk/news/temporary-judicial-commissioners-appointed/>

Inspections

- 2.9 On 16 March 2020, we took the decision to cancel all face-to-face inspections until the national position was clearer. We immediately began making arrangements for remote inspections instead and, with a few exceptions, this continued to be the model for the remainder of the year. While in some respects, remote inspections have proved challenging, we are satisfied that the key risk areas were prioritised and managed effectively and that our oversight has been no less rigorous than normal.
- 2.10 At the beginning of 2020, our Inspectorate teams had planned and scheduled 559 inspections, most of which would have been conducted in person. By the end of 2020, we had conducted 347 of the originally planned inspections. Figure 2.1 sets out the range of inspections completed during the year.

Figure 2.1 Number of IPCO inspections completed by organisation, 2019 to 2020



Notes:

- Figures for the intelligence agencies include data for the Ministry of Defence (MoD).
- All intercepting agencies (excluding UKIC and the MoD) are grouped with police and law enforcement.

- 2.11 We retained our in-person plans for a small number of UK intelligence community (UKIC) inspections where, because of the sensitivity and complexity of the material, we could not carry out a remote inspection in sufficient detail and where postponing oversight would not have been appropriate. However, the majority of law enforcement, public and local authority inspections could be conducted remotely. We have found in a number of cases that this reinforced our long-term ambitions to conduct challenging oversight using technology to make the most effective use of Inspectorate resources.
- 2.12 In 2018 and 2019, local authority inspections had been reduced due to resource constraints. We noted in our 2019 report our intention to complete all outstanding inspections by the end of 2020,⁵ an aim we were able to fulfil despite the pandemic.

⁵ Annual Report of the Investigatory Powers Commissioner 2019 (paragraph 14.2). See: Annual Report of the Investigatory Powers Commissioner 2019 (ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com)

Our ability to carry out these inspections was partly facilitated by the ease with which these could be done remotely. Conversely, with prisons in lockdown for the best part of 2020 and, in order to ensure the safety of our staff, these inspections were paused at the start of the pandemic. Once feasible to do so, arrangements for remote inspections were put in place and these inspections were prioritised from the start of 2021 to restore the inspection programme.

- 2.13 Remote inspections posed a series of new challenges, which we considered in the light of the risks and limitations that technical access and communication allowed. The inability to access systems directly, as we would during inspection visits at most locations, was a core consideration for our Inspectors in working to maintain robust and challenging oversight. Therefore, we considered alternative approaches. Several options, depending on the type of organisation being inspected, were implemented throughout 2020 and we have work underway to see what might be achievable in the future with further IT infrastructure or access permissions.
- 2.14 The innovative solutions borne out of the last year have demonstrated that our previous ways of working need no longer be the default option. We recognise there will always be certain aspects of oversight that can only be undertaken fully with a physical inspection, either due to the classification of the material to be seen, the location of material which is not suitable for management on an electronic system, and/or where there is real value of engaging directly with individuals or teams in their working environment. However, as a result of the lessons learnt in 2020, we are now operating a blended model of inspections, which we feel provides the most effective and efficient oversight while making the best use of our time and resources and of those we inspect.

Shift to other IT environments

- 2.15 As a consequence of the Covid-19 pandemic, all three UKIC agencies increased the extent to which their staff were working on different IT environments. In almost all cases, this has not involved any 'warranted data' subject to IPCO oversight (e.g., the product of warrants under the Investigatory Powers Act 2016) being moved onto such environments. However, there have been a small number of cases in which warranted data has been moved onto such systems. Where necessary, the handling arrangements approved by the Secretary of State as a prerequisite to issuing warrants have been updated to reflect this. We will keep the position under review during 2021.

Data assurance

- 2.16 In our 2019 report, we introduced the issue of data assurance and set out our intention to conduct a programme of work, led by specialist Inspectors, to investigate the adequacy of data holdings across the authorities we oversee. These plans were also affected by the pandemic, but the Inspectors have made substantial progress in working with all organisations to obtain relevant data to gain assurance in relation to the applicable safeguards.
- 2.17 Our objectives for this programme are:
- to inspect and investigate compliance with data safeguards to establish a high level of confidence that all data obtained under the powers overseen by IPCO is retained lawfully;
 - to embed and encourage best practice for compliance at each authority we oversee; and

- to assist the authorities we oversee to understand and investigate the compliance challenges arising from the use of bespoke, off-the-shelf and shared data handling programmes and technical storage environments.

- 2.18 Throughout 2020, the Inspectors benchmarked progress on compliance with safeguarding requirements across a selection of authorities. Our priority for this period has been working with law enforcement agencies given the volume of data that is obtained by those bodies, but we have also been in dialogue with public and local authorities on this issue. From 2021, we will be addressing data assurance at all IPCO inspections as a matter of routine.
- 2.19 Discussions with MI5, the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) about data assurance began in 2019 under the thematic umbrella of 'safeguarding'. Because of the nature of our oversight of UKIC, this work built on our understanding of how their systems, policies and procedures safeguard relevant material. We planned to conduct a specific safeguards inspection at each agency in 2020 but had to defer the SIS and GCHQ inspections until 2021. Our work in relation to safeguarding is described in the relevant chapters for MI5, SIS and GCHQ, and the errors which have been reported to us are set out in Chapter 19 (Errors).

3. Legal and policy

Overview

- 3.1 Legislative, policy and operational issues can have a substantial effect on all the aspects of the work of the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data (OCDA). The legal and policy teams across both organisations monitor any developments that may affect the Investigatory Power Commissioner's (IPC) oversight role, particularly given that the powers that IPCO oversees, and upon which OCDA takes decisions, can all be subject to direct and indirect challenge in the UK and the European Court of Human Rights. The IPC remains committed to providing such assistance as the courts or the Investigatory Powers Tribunal (IPT) may reasonably require of him.
- 3.2 This chapter gives an overview of:
- the key legal and policy developments that have had an impact on IPCO and OCDA in 2020; and
 - legal and policy approaches and decisions that we have taken on particular topics relevant to the IPC's functions.

Legal and policy developments relevant to our work

Bulk communications data and the scope of EU law

- 3.3 On 6 October 2020, the Court of Justice of the European Union (CJEU) gave a preliminary ruling under Article 267 Treaty on the Functioning of the European Union (TFEU) in relation to the acquisition of bulk communications data (BCD).⁶ A preliminary ruling under Article 267 TFEU is given following the referral of questions of EU law by a domestic court or tribunal. Once the CJEU answers the questions, the case returns to the domestic court or tribunal to decide how the ruling should be implemented.
- 3.4 In this case, Privacy International were challenging the acquisition of BCD by the UK intelligence services before the IPT. In summary, Privacy International argued that the acquisition of communications data (CD) by the UK intelligence community (UKIC) should be subject to similar safeguards as those governing the acquisition of such data by law enforcement agencies (LEAs) required by EU law (applications for targeted CD by LEAs are subject to external independent authorisation by OCDA).⁷ The Government argued that the safeguards should not apply in relation to UKIC as national security is outside the scope of EU law. The IPT referred the case to the CJEU.

6 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* (C-623/17)

7 See: Joined Cases *Tele2 Sverige AB v Post- och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v. Watson* (C-698/15), ECJ, Judgment, 21 December 2016 and the associated judgment of the Court of Appeal in *Secretary of State for the Home Department v Watson and others* [2018] EWCA Civ 70

- 3.5 The CJEU ruled that EU law does apply where UKIC compels a telecommunications operator to provide CD, notwithstanding it is for a national security purpose. The case will now return to the IPT which will determine what additional safeguards (if any) should apply to the BCD regime in the UK.

The UK-US Bilateral Data Access Agreement

- 3.6 In September 2020, Parliament enacted new regulations⁸ to require the IPC to oversee the UK's use of the UK-US Bilateral Data Access Agreement.⁹
- 3.7 The Agreement, signed by both governments in October 2019, facilitates public authorities' access to electronic data relating to the prevention, detection, investigation and prosecution of serious crime. Access to such data is subject to safeguards set out in both the Agreement and domestic legislation, and as agreed between the parties.
- 3.8 The regulations amended section 229 of the Investigatory Powers Act 2016 (IPA), requiring the IPC to oversee compliance with the Agreement (including all applicable safeguards) and ensure its proper use.
- 3.9 The regulations also amended section 229 IPA to include the oversight of functions exercised by public authorities under the Crime (Overseas Production Orders) Act 2019 within the scope of the IPC's functions. That Act grants LEAs and prosecuting authorities the power to apply for and obtain electronic data directly from service providers (those who create, process, communicate or store electronic data) for the purposes of criminal investigations and prosecutions. Overseas production orders may only be used when permitted under an international co-operation arrangement between the UK and the country where the subject of the order is located. Such an agreement has been reached with the USA and the regulations expressly require the IPC to keep under review the compliance by public authorities in the UK with the terms of the Agreement.
- 3.10 The Agreement will enter into force upon exchange of diplomatic notes by the parties.

Covert Human Intelligence Sources (Criminal Conduct) Act 2021

- 3.11 During 2020, the Covert Human Intelligence Sources (Criminal Conduct) Bill was introduced in Parliament and received Royal Assent on 1 March 2021. The Act provides express legal basis for intelligence agencies, LEAs and some other public bodies to continue to use authorised undercover officers and other covert human intelligence sources (CHIS) to participate in crime for the greater good, such as to disrupt and detect more serious crime or safeguard national security. The Act introduces a new requirement for all criminal conduct authorisations to be notified to the IPC within seven days. The IPC will also have oversight of the enhanced safeguards which the Act introduces for juvenile and vulnerable adult CHIS.

8 The Functions of the Investigatory Powers Commissioner (Oversight of the Data Access Agreement between the United Kingdom and the United States of America and of functions exercisable under the Crime (Overseas Production Orders) Act 2019) Regulations 2020. See: <https://www.legislation.gov.uk/uksi/2020/1009/contents/made>

9 The Agreement between the Government of the United Kingdom and the Government of the United States of America on access to electronic data for the purpose of countering serious crime dated 3rd October 2019 (CP 178). See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

3.12 We will report on these new oversight functions in our 2021 report.

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

3.13 Schedule 3 to the Counter-Terrorism and Border Security Act 2019 provides the IPC with functions in relation to “port stops” that are undertaken for the purpose of determining whether a person appears to be engaged in hostile activity. Schedule 3 came into force in June 2020.

3.14 In accordance with paragraph 62(1) of Schedule 3 to the Act, the IPC will keep under review the operation of the Schedule 3 powers and a separate report for 2020 will be made to the Secretary of State in due course.

Passive data collection techniques: when is a communications data authorisation required?

3.15 In the context of CD inspections in 2020, we reviewed a number of cases involving “passive” collection. We were asked whether the use of “passive techniques” would need a CD authorisation. “Passive” techniques use equipment which receives and records signals emitted by target equipment, without causing the target equipment to produce those signals. As a result, the collection of data was from, or about, equipment which would not, absent lawful authority, constitute an offence under the Computer Misuse Act 1990 (CMA) and therefore did not constitute equipment interference. For the CMA to be engaged, the technique must cause a computer to perform a function.

3.16 Where a “passive” technique involves the acquisition of CD directly from a telecommunication system, we concluded that the data obtained must meet the following criteria:

- it must include either entity and/or events data (section 261(5) IPA);
- it must not include the content of a communication or anything which, absent the provision in the IPA that systems data is not content, would be content of a communication (section 261(5)(c) IPA); and
- the entity and/or events data obtained must be comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system by means of which the communication is being or may be transmitted (section 261(5)(b) IPA). In this context, the “communications” in question may consist entirely of systems data such that they do not include any content.

3.17 Where a “passive” technique meets the above criteria, we have advised that it may be properly authorised under a CD authorisation.

Operational purposes

3.18 As we reported in our 2019 report, UKIC continues to rely on the full range of operational purposes in the vast majority of its bulk warrants issued under the IPA. Where these warrants were selected for review, we continued to be satisfied that this was appropriate and that the relevant statutory tests as to the necessity of including all of the operational purposes had been met.

- 3.19 Operational purposes are also audited during the inspection process, to test whether the examination of data is undertaken according to an operational purpose for which examination is or may be necessary, as specified in the warrant. During our UKIC inspections, we cross referenced the examination audit with a list of operational purposes to satisfy ourselves that each justification to examine bulk data was associated with a valid and recorded operational purpose.
- 3.20 The Prime Minister reviews the list of operational purposes annually, and last did so in September 2020. We received the latest list of operational purposes from the Government in February 2021.

Call recording software

- 3.21 Between 2016 and June 2020, both Surrey and Sussex Police permitted the installation of a call recording software application ('the app'). The app could be downloaded to a force-issued mobile telephone (or similar device) by any member of the force from a version of the Google Play Store. The app was one of several similar apps that can be freely downloaded from the ordinary versions of the Google Play Store or Apple's App Store by any member of the public.
- 3.22 The free version of the app used by Surrey and Sussex Police automatically recorded all telephone calls (inbound and outbound) made using the device's normal telephony service. The app recorded the calls by accessing the voice audio data feeds to/from the device's microphone and speaker (within the device). The app then recorded a copy of the voice data in a file which was stored on the device's local storage. It is important to note that the version of the app used by Surrey and Sussex did not permit the data automatically to be exported from the device, such as to the Cloud. Once stored on the device, the user could play back the recording from the device.
- 3.23 There would appear to have been 545 installations of the app by Sussex and 238 by Surrey. It is currently unclear as to how many calls may have been recorded during the period in which the app was available and how many of these were with external (i.e., non-police) parties. It is also not clear why the app was downloaded by so many officers. However, there is anecdotal evidence that the purpose was to enable officers to rely on a recording of a conversation with a member of the public in the event that a dispute as to what was discussed should arise.
- 3.24 We were notified of the use of the app by both forces as a potential relevant error of conduct that may have constituted the interception of communications and/or surveillance without the requisite warrant or lawful authority being in place.
- 3.25 After very careful consideration, the IPC concluded that, as the app was recording the communication while it was being transmitted, this constituted recording at a "relevant time" due to the definition at section 4(4)(a) IPA. However, the content of the communication was not made available to a third party while in the course of transmission; it was only available to the app user (i.e., the sender or recipient as the case may be) once the recording had been stored locally on the device. This meant that the conduct was not sufficient by itself to render the call recording "interception". Such a conclusion is of general interest as the alternative conclusion would mean that any similar call recording activity, including by a member of the public, would be a criminal offence.

- 3.26 In the view of the IPC, a further, separate, act from the use of the app would be required for the app user to make the contents of the call available to a third party (for example, the user would need to export the recording from the device in circumstances where the Cloud storage area is accessible by a third party). Accordingly, it is our view that the installation and use of the app is not interception. This is consistent with the Court of Appeal judgment in *R v Hardy* which reached the same conclusion in relation to a tape recorder (which might be considered a precursor to the call recording app).¹⁰
- 3.27 However, the IPC did conclude that the use of the app by the police constituted surveillance. In reaching this view, the IPC considered the IPT cases *Re A Complaint of Surveillance* and *AB v Hampshire Constabulary*.¹¹ In these cases, the IPT concluded that an audio recording of a voluntary interview was not surveillance, but that an audio and video recording of the inside of residential premises using body worn video was surveillance. The IPC considered that the IPT was not drawing a blunt distinction between audio and video recording. In reaching his conclusion, the IPC noted in particular that 'correspondence' (which covers telephone calls) was specifically protected by Article 8 European Convention on Human Rights (ECHR) in the same way that the IPT noted that 'the home' was specifically protected in *AB*. Further, the IPC noted that although it was conceivable that some recordings by Surrey and Sussex Police might have been similar voluntary interviews to those in *Re A Complaint of Surveillance*, the anecdotal evidence appeared to suggest that the purpose of the recording was very similar to the officer's reasons for using the body worn video camera in *AB*. That is, it was not a substitute for note taking as part of a voluntary declared interview, but to record by way of anticipation anything that might happen during a police officer's interaction with a member of the public. Accordingly, the use of a call recording app could be distinguished from *Re A Complaint of Surveillance*. In addition, the use of the app was not a one-off targeted activity. Its use was widespread, indiscriminate and arbitrary. It resulted in the systematic covert recording and indefinite retention of the voice of the other party and would therefore seem to clearly engage Article 8 ECHR.
- 3.28 For the above reasons, the IPC determined a relevant error in relation to surveillance had occurred and, given the widespread nature of the error, we consider it is important that special attention be drawn to it in this report. To their credit, both forces, upon discovery of the issue, promptly brought it to our attention and took immediate steps on their own volition to cease use of the app by removing it from devices.
- 3.29 We wrote to all LEAs to identify if the practice went beyond Sussex and Surrey and responses confirmed that it did not. The issue stemmed from Surrey and Sussex's decision not to restrict access to the Google Play Store on official devices to prevent the installation of the app. We are satisfied that both Surrey and Sussex have taken appropriate action to prevent the use of the app going forward and to review any recorded data with a view to its destruction, unless required evidentially.
- 3.30 It is important to emphasise that, in terms of the analysis regarding surveillance, the call recording app used by Surrey and Sussex Police was covert as it did not warn the other party that they were being recorded. Accordingly, it can be contrasted with apps which do inform other parties whenever a participant records the call; this includes, for example, Skype for Business, Microsoft Teams and Zoom, which all have a feature to record video calls but activating this function will automatically warn all other parties. The use by public

10 [2002] EWCA Crim 3012.

11 [2019] UKIPTrib IPT 191 C.

authorities of the overt recording functions in such software therefore does not, in our view, constitute directed surveillance.

Raising concerns with IPCO

- 3.31 In our 2019 report, we included the process for making a disclosure to IPCO as enabled by the information gateway set out in section 237 IPA. This statutory gateway enables both current and former staff of the public authorities which we oversee to raise with us any serious concerns they have. Where it is assessed that such concerns have merit, these will be investigated thoroughly, and appropriate action will be taken.
- 3.32 In 2020, we received one new disclosure which engaged our statutory responsibilities. However, investigation of the allegations raised has not concluded due to delays caused by the Covid-19 pandemic.
- 3.33 As we set out in last year's report, three disclosures were made in 2019, with one case still under investigation at the time our report was published. Following investigation, the allegations regarding the LEA in that case were substantiated and the applicant was duly informed. Additionally, one of the other disclosures made in 2019 concerning a police force was reopened following the receipt of additional information; this concluded in 2021 with the allegations not substantiated.

4. Protecting confidential or privileged information

Overview

- 4.1 The Investigatory Powers Act 2016 (IPA) provides enhanced protection for certain forms of confidential or legally privileged information and Judicial Commissioners (JCs) have a statutory role in authorising and overseeing the acquisition and retention of such material. The IPA and its Codes of Practice (CoP) introduced specific safeguards for confidential or legally privileged material. Similar safeguards are set out in the Regulation of Investigatory Powers Act 2000 (RIPA)¹² and its CoP to protect sensitive material acquired from the use of surveillance, covert human intelligence sources (CHIS) and property interference.

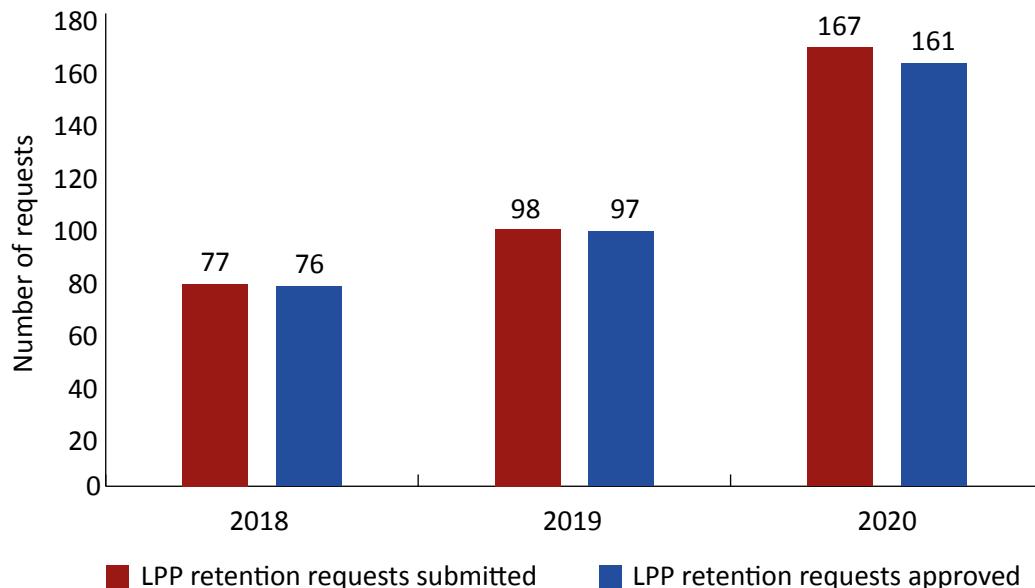
Legal professional privilege (LPP)

- 4.2 Legal professional privilege protects the right to seek legal advice and conduct litigation confidentially. Material subject to legal privilege, which would include most conversations and written advice between an individual or organisation and a professional legal adviser or representative, are protected by specific safeguards as set out above.
- 4.3 Authorities must inform the Investigatory Powers Commissioner's Office (IPCO) if they wish to retain LPP material for a purpose other than destruction. Any request to do so is considered and approved, if appropriate, by a JC. In these circumstances, the material and proposed use and handling arrangements are considered in order to determine whether the public interest in retaining it outweighs the public interest in the confidentiality of the item.
- 4.4 In 2020, we became concerned that law enforcement agencies (LEAs) were adopting an inconsistent approach to notifying IPCO of their desire to retain legally privileged material. For example, forces would write to IPCO with varying degrees of detail. In an effort to address this, we produced a new form for LEAs to use for applications to retain legally privileged material. This form also served a dual purpose of acting as a prompt for the applicant to ensure all aspects of the relevant legal test were considered. This may account in part for the marked rise in applications in 2020.
- 4.5 Another factor that may account for this rise is that during 2020, we proactively encouraged LEAs acquiring intercept product under either the Prison Rules 1999, Young Offender Institution Rules 2000 or Secure Training Centre Rules 1998, to follow an approach that is analogous to that for interception under the IPA. The Prison Rules and the relevant Prison Service Instruction (which is a policy document) currently make no provision for the independent external authorisation for the retention of legally privileged material. We have recommended to Her Majesty's Prison and Probation Service that this should be amended in the next update of the legislation or policy.

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

- 4.6 In 2020, a total of 167 applications were made to IPCO in relation to the retention of LPP material. Of those, 161 were approved.

Figure 4.1: Number of requests submitted and approved for LPP material, 2018 to 2020



Confidential journalistic material and sources of journalistic information

- 4.7 Confidential journalistic material and sources of journalistic information are subject to specific safeguards to respect the freedom of the press. All applications made under the IPA and RIPA set out 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. Journalistic freedom is protected under Article 10 (freedom of expression) of the European Convention on Human Rights and we would expect all relevant applications to consider the necessity and proportionality of any request in that context. Journalistic sources are protected in the IPA and RIPA and we expect these applications to be rare.
- 4.8 The acquisition of communications data (CD) relating to journalists and sources of journalistic information is covered in Chapter 14.
- 4.9 In relation to the use of other powers, our inspections have not identified any concerns in respect to the handling of any journalistic material. The number of applications to acquire journalistic material in other powers will always be substantially smaller than those seeking to acquire CD and all warrants will have been subject to the double lock approval by a JC. As with all authorisations, it must be necessary and proportionate to conduct the proposed interference or interception and so the test that must be satisfied is no different. However, we expect additional consideration to be given to the sensitive material that may be obtained and to the public interest in safeguarding freedom of the press in order to satisfy the threshold in this context. We would also expect applications to give some consideration to how confidential material will be handled and the extent to which this material is expected to be relevant to the investigation.

Example: confidential journalistic material

If a journalist was being investigated for their involvement in a serious crime, it may be necessary and proportionate to intercept the relevant communications but not necessary to review their professional communications other than to identify them and disregard them from the investigation. We would therefore expect the intercepting agency to make provisions to disregard or dispose of that material for the duration of the interception. However, this would not be the case if the journalist was using professional communications for the furtherance of serious crime.

- 4.10 Under the RIPA CoP, applications to conduct surveillance and use CHIS where there is a likelihood of obtaining journalistic material must be subject to an additional level of internal scrutiny. The enhanced procedures for obtaining confidential information include requiring the request to be authorised at a more senior level. We would expect any relevant applications to include details of how this sensitive material would be protected.
- 4.11 In 2020, 29 applications were made for warrants under the IPA where the purpose was to obtain material which the intercepting agency believed would relate to confidential journalistic *material*. Applications relating to journalistic *sources* might either be for warrants, which could be considered by a JC, or for CD under section 77 of the IPA, which will also be subject to judicial consideration. Under section 77, the JC must have consideration to the public interest in protecting a source of journalistic material. There were 25 warrant applications to identify a journalistic source and 18 other applications were considered under section 77 in 2020.

Additional safeguards for health records

- 4.12 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. However, we can confirm that we have not identified any issues of non-compliance or made any recommendations in relation to these safeguards.

5. Communications and engagement

Overview

- 5.1 Engagement and external communication remain central to the Investigatory Powers Commissioner's (IPC) delivery of effective and accountable oversight. We have worked hard to ensure that, despite the constraints of the pandemic, we have been able to maintain engagement through different means over the last year. We also used 2020 to develop our future communications strategy, through which we intend to communicate more regularly and responsively with both partners and the public.
- 5.2 Throughout 2020, we met with various organisations, including public authorities, non-governmental organisations (NGOs), international oversight bodies and other independent bodies. We will continue to build on this through 2021, with a focus on enhancing transparency and capitalising on the expert input of others in the sector.
- 5.3 The full schedule of the IPC's engagements in 2020 is found at Annex D.
- 5.4 We have revamped our website, and unveiled a new, user-friendly version in early 2021.¹³ It houses information about our work, including the two Annual Reports (2018 and 2019) which were published in 2020. Our website is our main method for communicating proactively with external audiences; we shared announcements on the Coronavirus Act 2020 and what this meant for the Investigatory Powers Commissioner's Office (IPCO), the appointment of temporary Judicial Commissioners (JCs) and our role in the oversight of the UK and US Bilateral Data Access Agreement.¹⁴
- 5.5 In addition, we provide regular updates to the organisations we oversee to ensure they are updated on matters of interest to IPCO, for example guidance, case studies and process updates.

UK engagement

Non-governmental organisations (NGOs)

- 5.6 Prior to the national lockdown, the IPC met Liberty and Reprieve, two NGOs who focus on areas covered by our work and are committed to challenging us to increase transparency around our work and that which we oversee. These meetings helped us to look again at our methodology and consider how we might be able to provide more information. Although there are limitations to what we can publish due to statutory restrictions, such as the need to safeguard national security, we welcome the challenge to provide as much meaningful information as we can. For example, in this year's report:

¹³ See: www.ipco.org.uk

¹⁴ See: <https://www.ipco.org.uk/news/>

- we have included statistics from the Office for Communications Data Authorisations on the reasons for rework/refusal (see Chapter 8);
 - we have provided a full report on the use of The Principles in the first year since implementation (see Chapter 13); and
 - we have provided additional information about the use of communications data where journalistic source material might be involved (see Chapter 14).
- 5.7 Reprieve presented at one of our regular JC Days in February 2020. These events are an opportunity for our Commissioners to work through key issues which might arise from our oversight for example, from new legislation or recent litigation. The session with Reprieve focussed on IPCO's oversight in relation to intelligence sharing under The Principles.¹⁵ Reprieve outlined its own understanding of the implementation and oversight of The Principles and set out some of its concerns about the potential application of the policy.
- 5.8 Privacy International wrote to IPCO in 2019 and 2020 on the use of social media monitoring by local authorities for investigative purposes. Our response set out our approach to oversight in this area, focusing on the development of local training and policies, and we intend to communicate this more widely to public authorities in 2021.
- 5.9 Following the publication of our 2018 report in March 2020, we had planned a roundtable with a group of NGOs to discuss the report. Due to the national lockdown, this roundtable was cancelled. Instead, it took place remotely in January 2021 which enabled the discussion to cover the 2019 report as well. The IPC outlined the findings of our reports, updated attendees on our ways of working in the light of the pandemic and stressed his ongoing commitment to enhance engagement with external parties. He then invited attendees to raise specific questions regarding our publications and work. Topics included statistics on the use of the Consolidated Guidance, oversight of the use of covert human intelligence sources (CHIS), applications from law enforcement agencies and use of other investigatory powers. Subsequently, the IPC met with the NGOs individually throughout 2021 to discuss some specific concerns more directly. We will provide more information on this in next year's report.

Independent bodies

- 5.10 In addition to the NGOs, the IPC had meetings with a number of other regulators, including: the Independent Reviewer of Terrorism Legislation; the Information Commissioner's Office (ICO); and the Surveillance Camera Commissioner and the Biometrics Commissioner.¹⁶ Discussion focused on areas of mutual interest and concern.

Public authorities

- 5.11 Throughout the year, the IPC has met with representatives from a variety of public authorities including: the Commissioner of the Metropolitan Police Service (MPS), Dame Cressida Dick; the Director of the Serious Fraud Office, Lisa Osofsky; and the Director General of the National Crime Agency, Dame Lynne Owens. In 2020, the IPC also met with two Chief Constables and ended the year meeting a group of Police and Crime Commissioners (PCCs), including Paddy Tipping, Chairman of the Association for Police and

15 The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees (The Principles).

16 The offices of the Surveillance Camera Commissioner and Biometrics Commissioner were merged in March 2021 and now operate as the "Biometrics and Surveillance Camera Commissioner".

Crime Commissioners, to discuss whether PCCs should have more direct engagement in IPCO's inspections.

- 5.12 In 2020, our Inspectors continued to engage with various UK independent bodies, such as the National Anti-Fraud Network, whose members include some of the public authorities we oversee. In addition, Inspectors have contributed to several national working groups which include: representatives from various organisations who meet to discuss specific issues relating to the use and oversight of investigatory powers. Examples of these working groups include: the Internet Intelligence and Investigations Group; the National Undercover Working Group; and the National Human Intelligence Unit.
- 5.13 Last year, our Inspectors also delivered training to public authority staff. This included presenting to the Crown Prosecution Service (CPS) to help aid understanding of investigatory powers and their use. On two occasions, team members delivered presentations as part of the CPS' lunch and learn programme, covering topics such as our inspection methodology, common areas of recommendations and the use of combined warrants for sensitive intelligence. One of our Inspectors also delivered a presentation as part of the MPS' training course for CHIS authorising officers. Another Inspector was scheduled to deliver a training session as part of a College of Policing course for Operational Security Advisors, but this was unfortunately postponed to 2021 due to the Covid-19 pandemic.
- 5.14 In November 2020, OCDA held a virtual law enforcement stakeholder event which included representatives from a wide range of police forces and public authorities. During the event, OCDA provided an update on its activity and performance, including the challenges faced during the Covid-19 pandemic and how critical functions were maintained. Participants at the event also considered the challenges for all those working within the communications data community and future plans for OCDA.

Others

- 5.15 In 2020, the IPC met ministers and Members of Parliament with a specific interest in our area of work. He also gave a masterclass to employees of the Foreign, Commonwealth and Development Office (FCDO) in the autumn of 2020, during which he outlined the work of IPCO and its JCs and explained how the organisation has maintained its work throughout the Covid-19 pandemic.
- 5.16 Throughout 2020, IPCO received correspondence from the News Media Association and Media Lawyers Association. Both organisations suggested it would be helpful to provide more information on the use of material involving journalistic sources. We discussed this further with them in a meeting in early 2021 and have sought to address some of their points in this report, while still safeguarding national security and individual privacy rights. We will continue to consider and review how we present this information in the future to ensure we are providing as much clarity as we can.

International engagement

Europe

- 5.17 In January 2020, we attended the Intelligence Oversight Working Group in Oslo with representatives from a number of European oversight bodies. The meeting discussed specifically how to make the most of the tools available to them, the use and retention of data and improving oversight methodology.

- 5.18 Following a meeting in Paris in September 2019, an exchange visit was scheduled with France's CNCTR (*Commission nationale de contrôle des techniques de renseignement*, or "The National Commission for the Control of Intelligence Techniques") to enable us to learn from external parties and develop our ways of working. The visit, which was due to take place in spring 2020 was postponed and it is hoped that this will go ahead in 2021 instead.
- 5.19 Throughout 2020, the European Intelligence Oversight Network, a gathering of organisations that together explore intelligence oversight and build good practice, was unable to meet due to the ongoing pandemic. It was agreed that it would be preferable to wait for an opportunity to meet in person rather than try to arrange a virtual conference. It is hoped that the next conference will take place towards the end of 2021.

Global

- 5.20 The annual meeting of the Five Eyes International Oversight Review Council (FIORC) was last hosted by IPCO in late 2019, with all five participating countries represented (Australia, Canada, New Zealand, the UK and the USA). The 2020 meeting, due to take place in New Zealand in October 2020, was replaced by virtual meetings throughout 2020 with a focus on progressing the joint work that was agreed at the 2019 conference.
- 5.21 In early 2020, one of our Inspectors and JCs presented to a delegation from Ghana. The delegation included representatives from the Ghanaian Ministry of Communications, Parliament and the Attorney General's Department. The focus of the visit was to inform the drafting of Ghana's Cybersecurity Bill. Our colleagues shared information on our oversight processes, safeguards and privacy issues.

6. Technology Advisory Panel

Overview

- 6.1 Section 246 of the Investigatory Powers Act 2016 (IPA) requires the Technology Advisory Panel (TAP) to submit a report to the Investigatory Powers Commissioner (IPC) about the carrying out of the functions of the Panel.¹⁷ The IPC has agreed that he will make this report publicly available through his Annual Report. The full text of the 2020 report is set out below.

Foreword

Despite the challenges of the Covid-19 pandemic, the TAP had an active year in 2020. In the early part of the year, it continued its pattern of briefings, which it receives in order to make sure it is well informed about the areas on which its advice may be required. These briefings had to be reduced to remote only because of the pandemic, thus restricting some of their scope, but nevertheless continued where possible. The briefings the TAP has had since its inception have been, for example, from the Secret Intelligence Service (SIS), the Government Communications Headquarters (GCHQ), the National Crime Agency (NCA) and Home Office agencies. The Panel have found such sessions extremely useful, and we would like to thank all those who have willingly shared their time and expertise with us.

As shown in the report, the pandemic has obviously had an impact on the TAP's activities, but alternative ways of working have allowed the Panel to continue to operate during this time. This has included the provision of technical advice, papers and education. It has had regular online meetings together with (in the periods of less severe lockdown) meetings between secure locations using appropriate remote conferencing technology which enabled topics of a higher classification to be discussed. I would like to record my thanks to those agencies and organisations which facilitated those meetings.

In addition to its work with the Investigatory Powers Commissioner's Office (IPCO), the TAP has had ongoing liaison with other jurisdictions and oversight bodies internationally, including the Five Eyes, where it has worked alongside IPCO on topics of mutual interest to the UK and other partners.

Overall, the TAP has continued to provide its very important function which is to ensure that the IPC has access to the best possible scientific and technological advice, and has done so on very limited resource, around one person-year in total.

17 A copy of the report is also sent to the Secretary of State and the Scottish Ministers.

I would like particularly to highlight my thanks to the IPC, Sir Brian Leveson, and all the Judicial Commissioners (JCs) and IPCO staff, for an extremely constructive relationship. This has, for example, been very fruitful in giving individual JCs the facility to ask questions on relevant topics, in giving TAP access to IPCO staff meetings to give plenary presentations on technological topics of general interest to them, and of course in helping the TAP develop its independent work programme, both on topics (the majority of its work) where it provides advice at the specific request of the Commissioner, and where it initiates advice independently of its own volition.



Sir Bernard Silverman FRS, Chair of the Technology Advisory Panel

Remit of the TAP

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

Membership of the TAP

- 6.3 The Chair of the TAP is Sir Bernard Silverman FRS, formerly Chief Scientific Adviser to the Home Office and Emeritus Professor of Statistics at Oxford University. TAP members during 2020 were: Professor Dame Muffy Calder, Vice-Principal and Head of the College of Science and Engineering at Glasgow University, and previously the Chief Scientific Adviser for Scotland; Professor Derek McAuley, Professor of Digital Economy in the School of Computer Science at the University of Nottingham; John Davies, who has an extensive technical background in both government and private industry roles; and Daryl Burns, who has worked in cryptography and cyber security for over 30 years and was Deputy Chief Scientific Advisor for National Security.
- 6.4 Professor Niall Adams was appointed to join the Panel in April 2020. He is Professor of Statistics, Imperial College London and his research interests are in computational statistics, machine learning and data science.
- 6.5 The initial three-year term of four of the members, including the Chair, ends in January 2021. All four have been offered formally extensions to their terms of office by the IPC and have accepted. Two further members have been recruited and are expected to join the Panel in the course of 2021. A formal appraisal process took place for all TAP members during the year.
- 6.6 TAP members are remunerated at an agreed daily rate. During 2020, members contributed an average of 20 days each to TAP duties. The TAP is supported by a Secretary who is a part-time (50%) civil servant.

Activities undertaken by the TAP and its members during 2020

Covid-19 and lockdown

- 6.7 Unsurprisingly, the global pandemic had an impact on the TAP's activities. A number of planned activities were postponed including TAP presence at IPCO inspections and proposed visits to the technical areas of GCHQ and MI5 as well as a range of technical briefings. TAP members were due to give a Masterclass to the Office for Communications Data Authorisations (OCDA) in March 2020 (covering the TAP's activities including two specific technical topics in detail) and this was also postponed. The TAP has continued to meet regularly though virtual means and to discuss topics over email. Some new topics for papers and other work during this time were pursued (see below). A proposal for upskilling the Inspectorate in technical subjects during the period of lockdown was agreed by the TAP Chair and the IPCO Chief Executive. Activities under this effort have been recorded.
- 6.8 Training provided for IPCO included:
- Location Services. Starting with basic spatial geolocation (on graph paper), working up to how GPS works, and how smartphones aggregate location information streams;
 - introduction to Coding and Cryptography. Using a free online coding platform, members of the Inspectorate were helped to learn basic Python coding and using the Caesar cipher as a first example, they were helped to write modular code to encrypt and decrypt messages;
 - understanding the differences between desktop programmes, local web-based apps, and more distributed 'Cloud' services;
 - technical training provided for the new data assurance Inspector; and
 - TAP members gave briefings to the Inspectorate teams on Internet Connection Records (ICR).

Meetings

- 6.9 A formal panel meeting took place in February 2020 and post lockdown, seven shorter meetings took place approximately monthly, mostly in virtual form. All meetings and actions were formally recorded. We would like to thank those external organisations who have allowed us to use their secure facilities on occasions to permit more sensitive discussions at times when travel has been limited.
- 6.10 Formal biannual meetings between the IPC and the Chair of the TAP took place in May 2020 and November 2020 (both virtually). IPCO's Chief Executive was also present. Both meetings were formally recorded.

Publications

- 6.11 In April 2020, the first formal report of the TAP covering 2019 was sent to the Home Secretary, the Cabinet Secretary for Justice (Scottish Government) and the IPC. An unclassified version of this was included in the IPCO 2019 report.
- 6.12 There were no other publications during the year.

Technical support and advice

6.13 Technical support was provided to inspections, either through TAP participation in inspection visits or in responding to requests for advice resulting from IPCO inspections. This has included responses on issues that cannot be described at this level of classification, and a number of ad hoc queries by Inspectors and JCs were also addressed informally. Though Covid-19 restrictions meant plans for TAP members to join further inspections had to be cancelled, several queries emanated from IPCO's inspections during lockdown and other restricted periods. Examples of the queries addressed to the TAP included:

- discussions on the technical aspects of whether a directed surveillance authorisation (DSA) or targeted equipment interference (TEI) authorisation was required in a specific law enforcement agency (LEA) context. Discussions widened to cover other uses of remote Wi-Fi including Wi-Fi surveys and penetration testing;
- discussions and a written briefing on the use of Near Field Communications (NFC) and the definition of what is a computer;
- discussions on the use of an App which is downloaded to police-issued devices. IPCO Inspectors needed to understand how the app worked in order to assess if it fell within the realms of interception or surveillance; and
- guidance on warrantry-related technical topics was given to the JCs. This involved providing technical support in relation to National Security Notices and Data Retention Notices.

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

- Covid-19: collecting data in a developing epidemic; a letter was also sent to the IPC with an update on the NHSx Covid-19 contact tracing app position;
- a briefing to the JCs on ICR;
- meetings with the IPCO Legal Team to give them a better understanding of ICR;
- internal guidance paper on ICR for IPCO staff;
- the TAP Chair briefed the new temporary JCs on the TAP in April 2020 and the TAP Secretary briefed the Inspectorate teams on the TAP's activities to date;
- a letter and commentary were sent to the IPC in August 2020 in response to a Royal United Services Institute (RUSI) occasional paper: "Artificial Intelligence and UK National Security"; and
- a paper on encryption technologies was written to provide guidance for IPCO.

Visits and liaison

6.15 During 2020, the following visits and engagements took place:

- the TAP visited Her Majesty's Government Communications Centre (HMGCC);
- the TAP Chair participated in a European Intelligence Oversight Network (EION) conference in Brussels in January 2020 and has also had separate discussions with Dr Thorsten Wetzling, Director of EION;
- a Panel member participated in the Scandinavian oversight group meeting in January 2020;

- TAP members took part in IPCO's inspection of GCHQ's Equities Process;
- TAP members have participated in several ongoing discussions on the topic of ICR; and
- a Panel member was an invited speaker at a RUSI-Wilton Park Workshop on *AI in the UK Public Sector*.

Ongoing discussions

- 6.16 The TAP worked with UK Research and Innovation and other government departments to create a successful bid to Her Majesty's Treasury for funding from the Strategic Priorities Fund for a programme of research into "Protecting Citizens Online".
- 6.17 A research grant proposal and associated budget for taking forward the Metrics of Privacy work through the RUSI has been finalised.

7. The Office for Communications Data Authorisations: operational developments

Overview

- 7.1 The Office for Communications Data Authorisations (OCDA) is a separate organisation from the Investigatory Powers Commissioner's Office (IPCO) with the Investigatory Powers Commissioner (IPC) having responsibility for the discharge of the functions of both offices. OCDA operates out of two locations, in Manchester and Birmingham, from 7:00am to 10:00pm, seven days a week, with a total complement of just over 100 staff.
- 7.2 Having completed the transition of over 600 authorities from the Regulation of Investigatory Powers Act 2000 (RIPA) to the Investigatory Powers Act 2016 (IPA) in November 2019, we became fully operational on 13 January 2020. As part of our planning for the 2020/21 year, we used available data to estimate that approximately 230,000 applications across all priority levels would be submitted for consideration during that year.
- 7.3 We were in a good position preparing ourselves for the first full year of live operations. However, the emergence of the pandemic forced us to react quickly to rebalance the requirement to discharge our critical functions alongside the safety and wellbeing of our staff.

Service

Operational response to the Covid-19 pandemic

- 7.4 In order to mitigate the impact of the pandemic on our working practices, we took a proactive approach and, through early engagement with Home Office Technology colleagues (who support our IT infrastructure), we were able to procure laptops for all members of staff, allowing them to work securely and safely from home. Furthermore, staff were able to continue to consider applications classified as Official Sensitive, a concept which had already been explored pre-pandemic. Security remained of critical importance, with clear guidance provided to staff to highlight the importance of continuing to manage information safely and responsibly when not in the office.
- 7.5 As part of our immediate response to the pandemic, and to safeguard our staff, we identified our potentially vulnerable staff and asked them to work from home in advance of the initial lockdown, ensuring they had priority access to laptops. We also ensured staff who remained in the office were able to do so in a safe environment by following the guidance set out by Public Health England and Home Office Health and Safety. As an organisation, delivering a regular stream of communications to both staff and stakeholders was critical to ensure all parties were well informed on how we would manage the impact of the pandemic, particularly during the early stages. This was achieved through regular written communications and all-staff conference calls with OCDA's CEO and members of the senior leadership team.

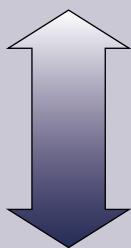
- 7.6 We also needed to ensure that critical functions were still being delivered, particularly those which required access to secure systems, that were unavailable to those working from home. We identified a small number of volunteers who would continue to attend the offices during lockdown to consider these more sensitive applications. In consultation with those authorities who required this service, and to protect the welfare of our staff, we agreed to reduce our operating hours on these services to between Monday and Friday (9:00am to 6:00pm). The combination of this work and staff working from home allowed us to transform completely our operations in a matter of weeks and continue to deliver our critical services without disruption.

Workflow

- 7.7 From an operational perspective, the Covid-19 pandemic was a significant factor in the volume of applications that we received. During the initial lockdown period in April, we encountered a 4% decrease in the number of applications received. This is most likely attributed to the period of adjustment in which most organisations found themselves going through. However, as authorities began adapting to new ways of working, we then began to see an increase in the number of applications being received. With lockdown restrictions in place and traditional surveillance options being limited, we started to pick up that communications data (CD) was becoming an even more important tactic that authorities were utilising as part of their ongoing investigations. This increased demand for CD on a national scale, and the efficiency with which we were returning decisions to authorities resulted in a steady increase in the number of applications received. This meant that volumes were beyond the anticipated numbers during May and was a trend which continued for the subsequent seven months.
- 7.8 The impact of the increased workflow was further exacerbated by the delay to our recruitment campaign, which had commenced in early March and subsequently postponed at the onset of the pandemic. Reduced resources contributed to the steady increase to the workflow queue, and ultimately caused us to breach our service level expectations (as set out below) for the first time on 6 June 2020. We considered a number of options and engaged with authorities to agree an approach that would ensure the best possible service during these difficult times. We placed a concerted effort in ensuring Priority 2 and Priority 3 applications were met, given their level of importance of risk management and protecting the public.

Communications data request prioritisation structure

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



Priority 1 (urgent) applications: dealt with by the authorities themselves

Priority 2 applications: dealt with within 6 working hours

Priority 3 applications: dealt with within 1 working day

Priority 4 applications: dealt with within 4 working days

- 7.9 We continued to explore ways of improving our workflow management and reducing the number of Priority 4 applications that were awaiting approval. These initiatives included offering additional hours to staff, utilising all non-operational staff who had been trained to consider applications as well as support from IPCO Inspectors. We initiated a pilot of using templates to help Authorising Individuals (AI) reduce the time taken to record their considerations for an application, while always ensuring, through our Quality Assurance framework, maintenance of the highest standard of consideration of every application. This work, alongside transitioning our entire induction training programme from classroom based to virtual sessions (and therefore facilitating the onboarding of the previously delayed new recruits), helped us clear our outstanding applications by 31 December 2020.
- 7.10 Table 7.1 sets out the details of volume of applications we received during 2019 and 2020. It should be noted that the figures are not wholly comparable given OCDA only became functional in March 2019.

Table 7.1: Applications submitted to OCDA, 2019 to 2020

			2019		2020	
Total applications			71,610		226,383	
Decisions made			71,208	99.4%	223,322	98.6%
Of which	Authorised		63,688	88.9%	199,482	88.1%
	Not authorised		7,520	10.5%	23,840	10.5%
	Of which	Returned			23,596	10.4%
		Rejected			244	0.1%
Withdrawn			385	0.5%	3,051	1.3%
Applications with no decision at year end (31 December)			17	0.0%	10	0.0%

8. The Office for Communications Data Authorisations: observations

Overview

- 8.1 The increasing numbers of applications received by the Office for Communications Data Authorisations (OCDA) highlight how communications data (CD) continues to provide an important contribution to a broad range of investigations. In particular, established crime priorities, such as county lines drugs offending, saw an increased demand for CD as an investigative tool, with examples of its effectiveness highlighted by media coverage.
- 8.2 The applications data we collect highlights clear trends for volumes and times at which applications are submitted and this is helping to support us becoming even more efficient in managing our workflow and provide value for money. The information available has also highlighted that the delay in implementing the recruitment plan (as a result of the pandemic) was a significant contributing factor in us failing to meet our service level expectations.

Returns for Rework (RfRs)

- 8.3 Where an Authorising Individual (AI) is not satisfied that the case for obtaining CD is fully and completely made out, we will return that application to the requesting authority for further work to be done on it before it can be reconsidered. The number of applications we returned for rework during 2020 is an illustration of the level of scrutiny that is applied to each and every application. Despite the pressures of the pandemic and the high volume of applications received, the data shown below provides assurance that our high quality of case consideration has remained consistent. Table 8.1 highlights that the primary reason for an application not being authorised and subsequently being returned to the submitting authority is that an AI does not believe the application meets the necessity or proportionality requirements. Some of the other reasons given are more technical in nature but all relate in some way to inadequacy or lack of clarity in the information given by requesting authorities. The information on RfRs is shared regularly with law enforcement and public authorities to help them get applications right first time.

Table 8.1: Returns for Rework (RfRs) reasons during 2020

Reason	Number of Returns for Rework	Proportion of Returns for Rework
Necessity	2,832	12%
Proportionality	2,832	12%
Dates/Times	2,596	11%
Consequential ticked/not ticked	1,888	8%
Accuracy	1,652	7%
Consequential Justification	1,652	7%
Attribution	1,416	6%
Collateral intrusion	1,180	5%
Forward facing	944	4%
Data Type	944	4%
Other reasons (19 categories)	5,663	24%

Lessons learnt

- 8.4 We have developed good practice among our AIs in respect of interpretation of relevant legislation and Codes of Practice. With the support of other partners, such as the Investigatory Powers Commissioner's Office (IPCO), and two years of operating experience, we are focussing considerable attention on the ongoing learning and development of our AIs. We are building on their knowledge of the changing CD landscape, liaising with law enforcement and Home Office policy stakeholders to ensure we are abreast of the latest developments.
- 8.5 In relation to maintaining business continuity, the changes made to operations in response to the Covid-19 pandemic by enabling AIs to consider Priority 4 applications has helped prove that the concept of working from home is feasible and beneficial to both the organisation and the welfare of our staff. Looking to the future, we intend to incorporate opportunities to work from home into our operating model.
- 8.6 We are continuing to make improvements to our systems which will streamline processes and improve the service provided. Our bespoke case management system will be subject to an upgrade in many of its features during 2021. We will also support our submitters, who do not have access to our automatic workflow system, by rolling out an application system which will provide a level of service in line with those who use our case management system.

9. MI5

Overview

- 9.1 Throughout 2020, we continued to conduct regular inspections at MI5. While the Covid-19 restrictions meant that many of these inspections were carried out remotely, in certain circumstances it was necessary to carry out inspections in person, which we did within the health guidelines.
- 9.2 A substantial proportion of MI5's use of investigatory powers is conducted using powers that are subject to the double lock. This gives us oversight of the range of live operations as well as post facto oversight through our inspections. During our inspections, we have interviewed operational staff, legal and policy representatives and senior management at MI5 to give us insight into its policies, practices and culture of compliance.

Findings

- 9.3 In general, we concluded that MI5's use of investigatory powers available under the Investigatory Powers Act 2016 (IPA), Intelligence Services Act 1994 (ISA) and the Regulation of Investigatory Powers Act 2000 (RIPA) was compliant with the statutory provisions, the Codes of Practice (CoP) and internal policies that we have seen.
- 9.4 However, MI5 has two programmes of work initiated in response to compliance concerns which were still in progress at the end of 2020. The first seeks to ensure that authorising officers complete reviews of directed surveillance authorisations (DSA) as required by RIPA. The second is the change programme launched following the Donnelly Review (see paragraph 9.37), which includes a comprehensive review of systems handling warranted data. We will be revisiting both of these issues in 2021.

Covert human intelligence sources (CHIS)

- 9.5 On our 2020 inspection, we noted further improvements in MI5's compliance in relation to covert human intelligence sources (CHIS). MI5 has robust processes in place for managing the highest-risk cases, especially those involving a significant element of criminal conduct. Rigorous independent risk assessment remains vital and MI5's operational security officers have an essential role to play in ensuring this standard is maintained.
- 9.6 In our 2019 report, we noted that MI5 had implemented changes to authorising online CHIS activity with a view to authorising each officer engaged in such activities separately under RIPA, rather than authorising one online persona which may be used by several individuals. This recommendation has now been fully discharged.
- 9.7 Separately, we were pleased to note that reviews were consistently being conducted, an improvement on our findings on previous inspections.

- 9.8 We continue to discuss with MI5 the most effective method of presenting all relevant documents on our CHIS inspections.

Directed surveillance

- 9.9 As we reported in 2019, we have been raising concerns with MI5 since 2018 about its process for DSAs. This continued to be an issue of concern in 2020, particularly the lack of detail in statements of necessity and proportionality by authorising officers (AOs), both when first granting an authorisation and with subsequent renewals. We also found that as with previous years, MI5 did not have an adequate review process in place for DSAs.
- 9.10 MI5 had previously launched a programme of work to address recommendations raised in the 2018 and 2019 inspections. This had not achieved the desired change and further effort was required to ensure authorisations, renewals and reviews are undertaken to the desired standard. We agreed with MI5 that we would conduct an interim review focused specifically on directed surveillance. This was conducted in early 2021 and will be covered in our 2021 report.

Property interference

- 9.11 MI5 frequently combines warrants authorising interference with property under section 5 of the ISA with warrants issued under the IPA. We reviewed a range of these 'combined' warrants in 2020 and were satisfied that the property interference component of each was necessary and proportionate (noting that Judicial Commissioners (JCs) do not have a role in approving the section 5 component of a 'combined' warrant).
- 9.12 In January 2021, judgment was handed down in *Privacy International v IPT & others*, a challenge to the Government Communications Headquarters' (GCHQ's) use of "thematic" section 5 authorisations to conduct what is now equipment interference. The judgment has wider relevance to what conduct can lawfully be authorised under any section 5 warrant issued to the UK intelligence community (UKIC). We have carefully considered the implications of the judgment with reference to MI5's existing section 5 warrants and will report our findings in our 2021 report.

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

- 9.13 MI5 continues to make extensive use of combined warrants under schedule 8 to the IPA. During 2020, we conducted a single combined inspection looking at TI and TEI authorised under the IPA. No bulk interception or bulk equipment interference warrants have been issued to MI5.
- 9.14 Overall, we were satisfied that MI5 had achieved a high level of compliance with the IPA.

Additional reviews imposed by the Secretary of State

- 9.15 Under the IPA, interception and equipment interference activity is authorised by the Secretary of State and approved by a JC through the double lock process. In some cases, for instance where there are concerns about the potential level of collateral intrusion, the Secretary of State may authorise a warrant but require an early review of necessity and proportionality by the requesting agency. Our previous inspection report noted that, where the Secretary of State requested that a warrant be reviewed, a letter of clarification

providing such a review was provided to the Home Office by the agreed deadline in the vast majority of cases. This inspection confirmed that this continued to be the case, and we saw well drafted review notes in all relevant cases. We examined a number of reviews, both internal and external, and found them to be clear and concise.

Thematic warrants

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

Modifications

- 9.17 One objective of our inspection was to examine whether modifications to thematic warrants were being used appropriately by MI5. In particular, we sought to inspect whether the same threshold was being applied for providing details within applications for minor and major modifications that were authorised within MI5 as would be included in applications that are approved by the Secretary of State and a JC. Those cases examined were thorough and provided an appropriate necessity and proportionality case for the modification. We were satisfied that modification provisions were being used appropriately, and provided the necessary operational flexibility foreseen by the Act. In our view, the modifications scrutinised fell within the foreseeable scope of the application, and renewal documentation set out the scale and scope of operations clearly. We also saw good early use of modifications to remove factors that were no longer deemed necessary.

Use of TEI in lead/low priority investigations

- 9.18 MI5 informed us in 2020 that it planned to lower its threshold for the use of TEI in certain operational scenarios. The use of TEI in this particular operational context enabled MI5 to establish the validity and seriousness of the intelligence and determine the most appropriate resolution (including no further action). In some cases, this resulted in a faster resolution of the investigation, and less intrusion into privacy overall. Our inspection provided assurance that the techniques being used were necessary and proportionate to the activities and intelligence being investigated. We will continue to monitor this in 2021 to ensure compliance.

Communications data

Bulk communications data (BCD)

- 9.19 MI5 holds a bulk acquisition warrant relating to several UK telecommunication operators. In 2020, our BCD inspection was conducted remotely.

- 9.20 In accordance with the requirements in the IPA and the accompanying CoP, MI5 investigators or analysts are required to create a justification record prior to selecting data for examination. There are several elements that make up the record created for audit purposes: (i) why the examination is necessary for one of the statutory purposes (for example, in the interests of national security); (ii) the selection of one of the operational purposes specified on the warrant; and (iii) the necessity and proportionality justification for selecting the data for examination. These records will also include details of any sensitive information, such as that relating to sensitive professions, which might be examined. This allows for subsequent audit of the activities of specific members of staff who are authorised to undertake the examination of BCD.
- 9.21 During our on-site inspections, we are normally given access to the system used by MI5's investigators and analysts to record why the examination of specific data is both necessary and proportionate. This ensures we can examine the activities of specific members of staff who are authorised to undertake the examination of BCD. During an inspection, we would normally undertake random sampling and run query-based searches on the system. For our remote inspection, we set out specific requirements to enable data to be extracted from the systems used by MI5's investigators and shared with the Inspectors electronically through secure channels.
- 9.22 We were still able to scrutinise the majority of records that indicate the communications data (CD) sought related to a person who may work in an occupation regarded as a sensitive profession. For example, we searched for records which included the words 'medical practitioner' or 'journalist'. We examined the analysts' and investigators' necessity and proportionality considerations, examined particular operations and identified requests for more intrusive datasets including multiple communication addresses or those requiring data over longer time periods. We also interviewed members of staff (via video link) to probe their considerations around these complex operations or sensitive requests.
- 9.23 Overall, we concluded that MI5's recorded justifications to undertake the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality. The operational teams were interviewed and demonstrated the value of BCD to recent operations.

Targeted communications data (TCD)

- 9.24 MI5 makes use of TCD alongside its queries of communications already lawfully in its possession within the BCD holdings. The use of TCD includes the acquisition of data to contribute to the examination and further analysis of BCD. On our TCD inspection, which was combined with our inspection of BCD and bulk personal datasets (BPD), we concluded that MI5 was achieving a high standard of compliance with the requirements of the IPA.
- 9.25 The system used to manage applications for TCD identifies the grade of Designated Senior Officer (DSO) required; when an applicant selects a service, the system prevents progress to an approver below the statutory grade. The independence of DSOs is again managed by a system which ensures the DSO is independent from an operation or investigation. The process requires a DSO to be selected from outside the applicant's management chain, which in turn ensures they are not involved in an operation or investigation.
- 9.26 Similar to our inspections of BCD, we scrutinise the majority of TCD applications authorised by the DSO that indicated the CD sought related to a person who may work in an occupation regarded as a sensitive profession. We identified no such applications which raised any concerns.

Bulk personal datasets (BPD)

- 9.27 During 2020, with restricted staffing levels, the overall management of BPDs was maintained primarily via MI5's Bulk Oversight Panel (BOP). This panel, which normally sits monthly, was able to maintain its gatekeeper and safeguarding functions by replacing face-to-face meetings with email communications. On behalf of MI5, this collective of staff with skill sets across bulk data systems considered all operational and legal justifications to retain, examine and delete datasets. Additionally, and in support of the BOP, MI5 maintained its internal audit capability with continuous examination of justifications used by staff, to examine BPDs.
- 9.28 MI5 responded positively to previous recommendations; the remote inspection held in 2020 confirmed and approved changes made to its internal oversight in the light of these recommendations. We made a number of observations during this inspection, but no formal recommendations.

Safeguards

- 9.29 Following our investigation into compliance problems in a technology environment used at MI5 (reported on in our 2018 and 2019 reports),¹⁸ we conducted a standalone inspection at MI5 focusing on the safeguards in place relating to "warranted data" (that is, data obtained under a warrant or authorisation subject to IPCO oversight). This included briefings on the programme initiated at MI5 to improve its compliance posture as a result of the independent review conducted by Sir Martin Donnelly in 2019. The inspection identified a number of issues requiring action, as set out in detail below.

Legally privileged material

- 9.30 Where a public authority obtains material subject to legal privilege via one of the powers overseen by IPCO and wishes to retain that material for one of the authorised purposes, prior approval from a JC is required. The test that applies is whether the public interest in retaining the material outweighs the public interest in the confidentiality of items subject to legal privilege.
- 9.31 Previously, MI5's internal policy required staff to apply a different – and higher – test: whether there were "exceptional and compelling" grounds for retaining the material. This test applies when a public authority is deliberately seeking to acquire legally privileged material, but does not apply (as a matter of law) when a public authority is seeking approval to retain such material. With the Investigatory Powers Commissioner's (IPC's) approval, MI5 has now amended its policy so that staff apply the statutory test when seeking approval to retain legally privileged material.
- 9.32 Separately, MI5 briefed us on its process for "flagging" items subject to legal privilege; this system operates on some, but not all, relevant MI5 systems. We recommended that MI5 consider what statistics might be extractable from the system, to assist with future inspections on the adequacy of safeguards for legally privileged material.

18 Annual Report of the Investigatory Powers Commissioner 2018 (paragraph 6.44); and Annual Report of the Investigatory Powers Commissioner 2019 (paragraph 8.44). See: Annual Report of the Investigatory Powers Commissioner 2018 ([ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com](https://www.ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com)); and Annual Report of the Investigatory Powers Commissioner 2019 ([ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com](https://www.ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com))

- 9.33 Finally, we noted that when an MI5 lawyer needs to review a piece of material to determine whether it is subject to legal privilege, the lawyer receives a copy of the item through MI5's internal email. This results in additional copies of the material being created. We therefore recommended MI5 confirm that deletion of all copies of the material can be actioned if necessary, e.g., if the JC refuses to approve retention of the item in question.

Retention, review and deletion of warranted material

- 9.34 The retention, review and deletion (RRD) of warranted material was one of the central issues in our investigation into the technology environment at MI5 in 2019. We therefore revisited the topic on our safeguards inspection in 2020.
- 9.35 While MI5 has a clear and detailed RRD policy in place for its warranted material, we were concerned to note that MI5 did not have a comprehensive central understanding of data flow in its systems which would enable it to have confidence that safeguards were being applied adequately. Addressing this is a priority objective for the programme initiated at MI5 to respond to the Donnelly Review.
- 9.36 We asked MI5 to provide us with a full list of systems used to handle material obtained under the covert powers we oversee, setting out how the RRD policy applies to each system. This is a substantial and complex task and we intend to review the results on our safeguards inspection in 2021.

The Donnelly Review¹⁹

- 9.37 One of the recommendations made in Sir Martin Donnelly's report was that there should be an urgent programme to provide MI5 staff, including contractors, with tailored best practice training on MI5's statutory obligations in respect of handling warranted data, with input from IPCO.
- 9.38 We have reviewed the training packages developed by MI5 in response to this recommendation and attended a sample session for the training. We were satisfied that the approach and content of the training was appropriate.

Handling arrangements

- 9.39 The programme initiated at MI5 in response to the Donnelly Review includes an initial review of the handling arrangements covering warranted data which the Home Secretary is required to approve under the IPA as a precondition of issuing warrants. These handling arrangements are due to be reviewed in more detail following the conclusion of the Donnelly Review and we will examine them thereafter.

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

- 9.40 Separately, in December 2020 MI5 informed us that it had identified an issue with the way in which a specific – and small – category of warranted data was being handled within a particular set of MI5 systems. Sometime earlier, MI5 had updated the documentation it provides to the Home Secretary and the JCs as part of its handling arrangements to reflect its awareness of how this category of data was being processed by MI5 systems, and also amended the form of words used in its warrant applications to make clear how the data was being handled. While we were satisfied that the language used in warrant applications and supporting documentation was accurate, we would have expected MI5 proactively to draw this change to the attention of JCs at the time it was made, and to explain the context. Having reviewed the position in the light of MI5 updates, the IPC was satisfied that the handling of this category of data was compliant with the IPA.

10. Secret Intelligence Service

Overview

- 10.1 We continued to conduct regular inspections of the Secret Intelligence Service (SIS) in 2020 with most of our investigations relating to SIS's work overseas. However, we were unable to conduct any physical inspections at overseas stations due to the Covid-19 restrictions. Where possible, we spoke to officers based overseas during our London inspections, as well as to legal and operational staff working in the UK. As a result, we have maintained a holistic view of the working culture at SIS and the level of understanding of the legislative framework, both for officers working overseas and in the UK.
- 10.2 In our 2019 report, we reported that the Investigatory Powers Commissioner (IPC) had written to the Prime Minister about oversight of SIS's agent running activities overseas. This activity has a statutory basis under section 1 of the Intelligence Services Act 1994 (ISA). We oversee SIS's agent running overseas only insofar as it involves approvals under section 7 of the ISA. All other overseas agent running is not, and has never been, subject to oversight by the Investigatory Powers Commissioner's Office (IPCO) or its predecessors. The IPC recommended that the Government carefully consider whether this was still the right policy position.
- 10.3 In October 2020, the Foreign Secretary replied to the IPC's letter on behalf of the Prime Minister. He informed the IPC that he continued to be satisfied that oversight arrangements for SIS's overseas agent running operations under section 1 were appropriate and proportionate, taking into account the established Foreign, Commonwealth and Development Office (FCDO)/SIS mechanisms of oversight which had further been strengthened since the IPC had written his letter.

Findings

- 10.4 Overall, we found a good level of compliance across all powers from the inspections we were able to conduct. We note the work undertaken to respond to our 2019 recommendations and recognise that, while there have been some improvements, progress has been affected by the pandemic. One area where we hope to see improvement in our next inspection is in the written consideration of authorisations for covert human intelligence sources (CHIS). We note that new mandatory training will be implemented shortly and we hope that this will provide greater consistency in the written evidence of oversight and governance of CHIS activity.
- 10.5 Although our inspections of targeted interception (TI) and targeted equipment interference (TEI) were focused on a smaller number of warrants, we noted that the use of broad thematic warrants was increasing. We found the internal approvals to be of a good standard but noted some small areas for improvement.

Covert human intelligence sources (CHIS)

- 10.6 On our 2020 CHIS inspection, we continued to observe that SIS was taking a great deal of care in the management of its agent operations and that all the CHIS conduct authorised under the Regulation of Investigatory Powers Act 2000 (RIPA) which we scrutinised was both necessary and proportionate. However, we also continued to observe many of the same issues with RIPA authorisations that we have commented on at previous inspections. This included: insufficient written consideration by the authorising officer (AO); lack of regular reviews for CHIS cases; a lack of timely cancellations; and the inconsistent application of the correct authorisation periods both initially and at renewal.
- 10.7 We were pleased to see that the SIS compliance team has made significant progress towards addressing our recommendations in many areas, not least the appointment of a Senior Responsible Officer (SRO). This is reflected in a reduction in the number of errors this year. However, we also noted that by and large, this work is yet to result in changed behaviours by the operational staff completing and authorising the RIPA paperwork. We accept that progress against our recommendations has been slowed by the Covid-19 pandemic and the SIS compliance team is to be commended for its efforts in these difficult times. This team is now in the final stages of trialling a mandatory, online, pass/fail RIPA training package. We hope that once this package is made available to case officers, we shall start to see a significant improvement in the quality of consideration recorded in RIPA documentation.

Directed surveillance

- 10.8 On our 2020 inspection, we reviewed three directed surveillance authorisations, all relating to online surveillance. These were broad authorisations covering activity at the lower end of intrusiveness. It was not possible for us to examine in detail the tasks being carried out under the authorisations due to Covid-19 restrictions. While we have examined this activity previously, we are conscious that capability in this area is advancing at pace and we will want to examine this activity in greater depth on future inspections to understand how it is evolving.

Property interference

- 10.9 A very small number of property warrants were issued to SIS in 2020. We reviewed one property warrant in the course of an inspection in 2020 and were satisfied that it was necessary and proportionate, noting that it involved no intrusion into privacy.
- 10.10 In January 2021, judgment was handed down in *Privacy International v IPT & others*, a challenge to the Government Communications Headquarters' (GCHQ's) use of "thematic" section 5 authorisations to conduct what is now equipment interference. The judgment has wider relevance to what conduct can lawfully be authorised under any section 5 warrant issued to the UK intelligence community (UKIC). We have carefully considered the implications of the judgment with reference to SIS's existing section 5 warrants and will report our findings in our 2021 report.

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

- 10.11 Our TI and TEI inspection of SIS in 2020 found that it was demonstrating a good degree of compliance with the Investigatory Powers Act 2016 (IPA). SIS had also responded positively

to a recommendation made in 2019 that processes to keep warrants under close review ought to be strengthened.

- 10.12 Due to physical access restrictions arising from Covid-19, we inspected a reduced sample of warrants this year. However, we were still able to review a substantial number of records provided by SIS and are confident that our conclusions on this sample are representative of the whole.
- 10.13 We noted that SIS is now making some use of broad thematic warrants, a number of which we selected for inspection. These thematic warrants are all underpinned by internal approval documents supporting operational activity conducted under a “general descriptor” of the subject matter of the warrant, such that there is no need to modify the warrant to conduct new activity as long as it falls within the descriptor. We selected and read a number of these internal approvals and found them to be of a good standard. We are satisfied that SIS’s use of thematic warrants is appropriate, and that the internal approval process provides an additional safeguard to ensure that all actions are documented as necessary and proportionate.
- 10.14 We identified a small number of areas for improvement. During inspection it became clear that SIS had committed a relevant error in relation to modifications made to a warrant where legal professional privilege (LPP) material could have been anticipated. These modifications ought to have been authorised by a Judicial Commissioner (JC) but were externally approved by a senior official in the FCDO because of human error. Once discovered, proper authorisation was sought and granted and the error was reported to IPCO for investigation.

Communications data

Targeted communications data (TCD)

- 10.15 SIS makes limited use of TCD. On our TCD inspection, we concluded that SIS was achieving a high standard of compliance with the requirements of the IPA.

Bulk communications data (BCD)

- 10.16 Consistent with its activity in 2018 and 2019, SIS did not undertake bulk acquisition of communications data (CD) in 2020. SIS continues to have access to certain BCD acquired by GCHQ and MI5 where it is operationally necessary. We inspect how that data is used by SIS at the other agencies and confirm that it is lawfully obtained and that disclosure between the agencies is appropriate. Our inspections at SIS have also provided a good level of assurance in relation to internal safeguards applied to all data, and so we are confident that any BCD material accessed and stored by SIS is being handled appropriately.

Bulk personal datasets

- 10.17 Our BPD inspection at SIS was conducted remotely in 2020. The focus of the inspection continued to be testing whether systems used to retain and examine BPD were compliant, all processes and procedures were carried out lawfully and each internal examination of datasets was justified.

Legacy data

- 10.18 During the implementation of the IPA, SIS focused on reassessing and obtaining warrants to authorise the retention and examination of known BPDs, as well as ensuring BPDs were handled in compliance with the safeguards set out in the Act. SIS identified a potential risk in the existence of old archived data in its systems that would, since the introduction of the IPA, now constitute BPD. In 2020, an internal project team completed a review of archived data, identifying 60 files it believed required further examination. Of those 60 files, the relevant compliance panel at SIS concluded that three should have been deleted and were retained in error; a matter that was subsequently reported to IPCO.
- 10.19 As a consequence of our internal examination of data in 2020, we were satisfied that SIS remained compliant in its current handling and administration of BPDs. However, Covid-19 restrictions precluded a detailed examination of legacy systems and these will be a focus of our 2021 inspection programme.

Other findings

- 10.20 The Covid-19 pandemic had an impact on the BPD compliance network, but by prioritising workloads SIS was able to focus on authorising retained datasets, reviews, renewals, and urgent deletions; and ingesting business critical data.
- 10.21 SIS's compliance staff were able, during the year, to work in tandem with policy and legal teams in order to provide operational guidance on the use of material. In addition, SIS processed a number of new datasets. It also reviewed class warrants resulting in recommended deletions and warrant cancellations.
- 10.22 We mentioned in our 2019 report that the internal audit process at SIS would be inspected in detail in 2020. The pandemic prevented that inspection taking place, but we hope to physically inspect SIS's internal audit function in 2021.

Section 7 of the Intelligence Services Act 1994 (ISA)

- 10.23 We usually examine SIS's compliance with section 7 through inspections in London and at overseas locations. Overseas inspections were not possible this year due to Covid-related travel restrictions.
- 10.24 On our London-based inspection, we found that SIS had achieved high levels of compliance with the requirements of the Act and had taken our feedback on previous submissions into account.
- 10.25 In some cases, SIS operates a 'framework' section 7 authorised by the Foreign Secretary, where SIS officers then operate an internal approval regime authorising individual instances of reliance on the submission. These 'framework' submissions clearly set out the parameters of what conduct was and was not authorised; and they were supported by detailed and appropriate internal policies. The internal records of reliance we reviewed were produced to a high standard.
- 10.26 We also reviewed one submission relating to a specific operation which raised some complex legal issues, including an issue relating to conduct which might take place both in the UK and overseas. To the extent that UK-based conduct was occurring in the context of the authorised operation, this was not capable of authorisation under section 7. However, we concluded that, insofar as SIS would engage in conduct in the UK in the course of the

operation, the Secretary of State was entitled to conclude that this would not breach UK law. We recommended that, in future submissions where conduct may need to take place in the UK and overseas, SIS sets out more clearly the limits to what is and is not authorised under section 7 and the legal basis for activity conducted in the UK. We intend to revisit this issue, with reference to further section 7 authorisations, in 2021.

- 10.27 Separately, we reviewed a number of section 7 authorisations relating to a separate class of operations. These involved complex legal issues. The submissions we reviewed set out the analysis on these issues for the Secretary of State with great care and in extensive detail. We concluded that the Secretary of State was entitled to accept SIS's analysis that the conduct authorised was lawful. We identified one submission in which SIS's internal records did not record the necessity case in as much detail as we would have expected, in line with best practice.

Safeguards

- 10.28 As foreshadowed in our 2019 report, we planned a standalone inspection at SIS in 2020 focusing on the handling of warranted data in SIS systems. The inspection had to be postponed due to Covid-19 restrictions and will now take place in spring 2021.
- 10.29 One of the safeguards in place in relation to SIS's access to bulk datasets is internal review by the audit team. SIS's compliance auditing team examines a certain proportion of the justifications used by staff to examine bulk datasets on a regular basis. However, in response to the pandemic guidelines, SIS suspended its contemporaneous compliance audit of those justifications between 19 March and 25 August 2020. This change was not communicated outside of SIS or to the central compliance staff during this time. SIS compliance staff informed IPCO of the suspension a day after it was made aware. At the same time of disclosure to IPCO, a retrospective audit was commenced, and the Foreign Secretary and the IPC were notified in writing. That retrospective audit was completed by the end of 2020 and shared with the Foreign Secretary and the IPC.

11. Government Communications Headquarters

Overview

- 11.1 As with the other agencies, we continued to conduct regular inspections at the Government Communications Headquarters (GCHQ) during 2020. The majority were carried out remotely but, where necessary and in line with the health guidelines in place at the time, we conducted inspections in person. We are grateful for the support we received to make this possible.

Findings

- 11.2 GCHQ's use of bulk powers under the Investigatory Powers Act 2016 (IPA) continues to evolve as technology and capabilities change. We see this area as a vital element of oversight which can only be successful through regular discussions on policy and technology with GCHQ. We have been pleased by GCHQ's open and informative approach, as well as its response to our recommendations in this evolving area. We noted in our 2019 report that our approach to the inspections of bulk interception would change from 2020 onwards, following both the *Big Brother Watch v UK* judgment and our internal review.
- 11.3 We conducted the first new format inspections in January 2020. We focussed on the 'discovery' aspects of bulk interception (see paragraph 11.24 for further details.) We identified a number of areas for improvement in relation to the rules guiding GCHQ's "discovery" work in relation to bulk interception material but, given this was the first time many of these rules had been reviewed by an external oversight body, this was not unexpected. We made a number of recommendations, which we expect GCHQ will be able to address by expanding the policies and procedures already in place for "selection" to apply to "discovery rules", rather than making any more fundamental changes.
- 11.4 Unfortunately, as a result of the pandemic, we had to postpone our review of GCHQ's safeguards arrangements to 2021. However, we were made aware that temporary changes to the audit processes for the handling of warranted data had not been properly communicated to us. We note that all outstanding audit activity has now completed and that we will be informed of any future changes.

Covert human intelligence sources (CHIS)

- 11.5 In our 2019 report, we noted that several recommendations made on previous inspections were still in the process of being implemented. On our 2020 inspection, we were pleased to note the progress that had been made in relation to these previous recommendations. Only two remained not fully discharged.

- 11.6 First, we had previously recommended that CHIS risk assessments should be more specific and should relate to individual CHIS. We were informed that this had been addressed but we were unable on our 2020 inspection to review examples. We intend to do so in 2021.
- 11.7 Secondly, we made recommendations regarding access to records required in relation to CHIS cases. A new IT solution was being implemented at the time of our inspection which will help to address this.
- 11.8 Overall, we noted that the newly-designed Regulation of Investigatory Powers Act 2000 (RIPA) forms in use at GCHQ had been instrumental in making real improvements in compliance.

Directed surveillance

- 11.9 We made two recommendations in relation to directed surveillance in 2020. First, we noted that some directed surveillance authorisations (DSAs) were too broadly drawn, and did not relate to a single investigation or operation. Secondly, we identified that GCHQ did not have a process in place for authorising DSAs in urgent cases. We recommended that GCHQ should ensure that an urgency process is mapped out and tested, to ensure it has an effective procedure in place to allow urgent directed surveillance to be made and authorised in line with the procedures set out in the Code of Practice (CoP).

Property interference

- 11.10 GCHQ has a small number of warrants issued under section 5 of the Intelligence Services Act 1994 (ISA) authorising interference with property. Where GCHQ is conducting equipment interference to obtain communications, equipment data or any other information, this is now authorised under the IPA.
- 11.11 In January 2021, judgment was handed down in *Privacy International v IPT & others*, a challenge to GCHQ's use of "thematic" section 5 authorisations to conduct what is now equipment interference (EI). The judgment has wider relevance to what conduct can lawfully be authorised under any section 5 warrant issued to the UK intelligence community (UKIC). We have carefully considered the implications of the judgment with reference to GCHQ's existing section 5 warrants and will report our findings in our 2021 report.

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

- 11.12 On our 2020 inspection, we reviewed a range of TI and TEI warrants and were satisfied that GCHQ was achieving a high level of compliance with the requirements of the IPA. We made a number of recommendations in relation to particular warrants. These were aimed at further improving GCHQ's internal records of conduct undertaken in reliance on certain warrants and ensuring the renewal of warrants presented as clear and comprehensible picture as possible as to what conduct was being undertaken.

GCHQ policy on equipment interference targeting individuals travelling between the UK and overseas

- 11.13 On our TEI inspection at GCHQ in 2020, we discussed GCHQ's policy on when, for the purposes of the EI regime under the IPA, a targeted examination warrant is required to authorise the selection for examination (S4E) of data acquired under a bulk EI warrant.

Definition: Selection for examination (S4E) of protected material

Section 193(4) of the IPA requires that S4E of protected material (content) acquired under a bulk EI warrant must be authorised by a targeted examination warrant, or a temporary authorisation issued under section 193(5), if, at the time S4E takes place, the criteria used for that selection is referable to an individual known to be in the British Islands at that time.

- 11.14 In the context of the bulk EI warrants we reviewed at GCHQ, S4E occurs at the point GCHQ acquires data from the targeted device. As such, if a person normally resident in the UK travels abroad for a short period (e.g., on holiday), the Act does not strictly require GCHQ to apply for a targeted examination warrant or temporary authorisation to obtain that individual's stored communications, most or all of which will be communications which occurred while that person was in the UK. This is because S4E only takes place at the point the data is acquired, when the individual happens to be overseas.
- 11.15 GCHQ's internal policy includes a clear commitment that analysts will not seek to exploit a target's temporary absence from the UK solely in order to retrieve stored messages that were sent or received while the target was in the British Islands, as this could be perceived to amount to an avoidance of the protections afforded to persons in the British Islands.
- 11.16 While we were content that this policy commitment will ensure GCHQ complies fully with the spirit of the IPA, we were concerned that it also highlights a possible gap in the legislation. We have highlighted this potential legislative gap to the Home Office and we will update on this matter in our 2021 report.

Extent of Ministerial oversight of particularly sensitive operations conducted under bulk warrants

- 11.17 GCHQ will seek a thematic targeted EI warrant for operations that are capable of being authorised with an existing bulk EI warrant but where there are sensitivities that GCHQ wishes to bring to the attention of the Secretary of State. Seeking a thematic targeted EI warrant ensures that the Foreign Secretary is consulted in greater detail about the necessity and proportionality of these particular operations.
- 11.18 By contrast, GCHQ does not generally seek separate thematic warrants for operations against similarly sensitive target sets conducted under bulk interception warrants.
- 11.19 We challenged GCHQ on this apparent disparity. It was explained that there is a risk that GCHQ's EI operations may be detected by targets, increasing associated risks whereas, for interception, the risk of detection is much lower. We were content with this explanation; it is for GCHQ to determine when it ought to seek separate approval from the Foreign, Commonwealth and Development Office (FCDO) to target individuals posing particular sensitivities.

Assessing risks to the integrity of telecommunications systems

- 11.20 When applying for warrants under the IPA, GCHQ has a duty under section 2(2)(c) to have regard to the public interest in the integrity of telecommunications systems. We tested GCHQ's compliance with this duty by reference to a specific operational example. Overall, we were satisfied that GCHQ has a robust set of measures in place to ensure any risks to the integrity of telecommunications systems are minimised as far as possible.

Use of “descriptive” factors

- 11.21 Where a targeted warrant authorises or requires the interception of communications, or authorises the selection for examination of the content of communications acquired through bulk interception, the IPA requires that the warrant must specify the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications (section 31(8)). The IPA also provides that “specify” in this context means “specify or describe” (section 263(1)).
- 11.22 In reliance on these provisions, GCHQ frequently includes a general description of the factors which will be used to conduct interception against the subjects of a targeted interception warrant or targeted examination warrant. Having reviewed a number of examples, we were satisfied that this approach was consistent with the IPA, although the Interception CoP should be amended for clarity in this regard. While GCHQ has a range of safeguards in place to guard against abuse, this approach still enables factors to be subject to interception without any need for further approval (either internally within GCHQ or externally) as the factors to be intercepted are already covered by the general description.
- 11.23 For this reason, our intention is that interception inspections in 2021 will operate an enhanced oversight regime for GCHQ interception warrants containing “descriptive” factors.

Bulk interception

- 11.24 In our 2019 report, we reported that we would be reviewing our approach to inspecting GCHQ's use of bulk interception in the light of the judgment of the European Court of Human Rights in *Big Brother Watch v UK*. In January 2020, we conducted our first inspection of bulk interception under a new format.

Background

Definition: Bulk interception process

Bulk interception is authorised by warrant pursuant to section 136 IPA. Given its potentially broad scope, the process of bulk interception generally involves a number of stages:

- a) choosing the most suitable location from which to intercept wanted communications;
- b) choosing which streams of data are most likely to contain communications of the highest intelligence value;
- c) refining the intercepted communications to discard unwanted data;
- d) selecting which communications initially to retain from those streams for possible examination; and
- e) deciding which of the retained communications should be read, analysed or examined, and should continue to be retained for further analysis.

- 11.25 In the light of the *Big Brother Watch* ruling and following discussion with GCHQ, we reviewed our approach to these inspections. Regarding stages a) and b) above, the Court held that, “by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications and, as such, does not consider the [lack of external oversight] alone to be fatal to the Article 8 compliance” of the old RIPA regime under consideration by the court. As a result of that judgment, our inspection focused on

stages c) to e) above, though we did review the processes in place for making and justifying decisions as to what data is to be intercepted and why under stages a) and b).

- 11.26 Furthermore, our inspection methodology distinguished between “selection” and “discovery” in the context of bulk interception. Both “selection” and “discovery” involve moving bulk interception into longer-term storage such that it is available for examination by analysts, but for different reasons:
- “selection” involves identifying and storing data on the basis that it is likely to meet a set of criteria defined in advance by GCHQ and is therefore likely to be of intelligence interest;
 - “discovery” involves moving larger volumes of data into storage on the basis that, by querying these tranches of data using carefully designed queries, GCHQ will “discover” previously unknown targets of intelligence interest; and
 - the length of time for which a particular type of data is held (which may be very brief) depends on a number of factors, including its intrusiveness and the extent of collateral intrusion likely to be involved.
- 11.27 The focus of our January 2020 inspection was “discovery” in its various forms. “Selection” was not in scope on this occasion. Our inspection was the first time the rules governing “discovery” had been subject to detailed *ex post facto* review.

Key findings: discovery

- 11.28 We concluded that GCHQ needed to improve the standard of its necessity and proportionality justification for rules in the “discovery” category, including by developing a clear set of minimum standards for drafting justifications. We also recommended that GCHQ implement a clear and consistently enforced policy, including when and how this category of rules should be subject to review.
- 11.29 We noted that GCHQ was developing a new policy governing a particular type of discovery activity at the time of our inspection. The implementation of this policy has since been delayed by the Covid-19 pandemic. We concluded that this policy would play an important role in ensuring the necessity and proportionality of this category of discovery operations was considered in sufficient detail and we recommended that all future operations in this category should be subject to the new policy.
- 11.30 Finally, we concluded that GCHQ needed to articulate in greater detail the necessity and proportionality case for storing metadata in bulk for the purposes of discovery, both internally and in warrant applications.

Key findings: choice of what data to intercept and why

- 11.31 Decisions as to where to conduct bulk interception, and which streams of data are most likely to be of intelligence interest, are primarily operational decisions which are subject to GCHQ’s discretion. However, it is crucial that the reasons as to why GCHQ decided to conduct bulk interception at a particular location, or to prioritise particular streams of data, are justified and recorded properly.
- 11.32 We identified in this context that, for a particular set of decisions falling into this category, GCHQ was not producing any centrally retrievable justification setting out the reasons for its decisions. We acknowledge that, at the point a decision is made to conduct bulk interception in a particular location, or against a particular data stream, it may be difficult

to articulate the necessity and proportionality case in detail. However, we recommended that GCHQ develops a clear policy on what the minimum standard of justifications should be in this area and seek to agree it with IPCO.

Conclusion

- 11.33 As noted above, many of the types of rule inspected in 2020 had never previously been reviewed by an external oversight body. It was therefore unsurprising that we identified areas requiring improvement on this first inspection of its kind. However, GCHQ already has good systems in place to record and justify the rules it has in place governing “selection”. We expect GCHQ will be able to address our recommendations for “discovery” rules by expanding its existing policies and procedures, rather than making any more fundamental changes.
- 11.34 Prior to the Grand Chamber handing down its judgment in *Big Brother Watch v UK*, we had agreed with GCHQ that we would inspect bulk interception in an “end-to-end” manner in future, examining both “selection” and “discovery” rules, along with the justifications as to what data is to be intercepted in the first place and why. We will review the implications of the Grand Chamber’s judgment on this approach and will report further in our 2021 report.

Bulk equipment interference (BEI)

- 11.35 In our 2019 report, we reported our plans to discuss how best to conduct *ex post facto* oversight of GCHQ’s growing number of BEI warrants. In 2020, we continued with the enhanced oversight regime which was already in place in respect of GCHQ’s more well-established BEI warrants. In addition, we began to develop an oversight regime for the new BEI warrants approved over the course of the year.
- 11.36 For those BEI warrants which have been in force for some time at GCHQ, we found that internal records of reliance were being produced to a high standard. This is in part due to action GCHQ has previously taken in response to our recommendations about improving standards in this area. Due to physical access restrictions arising from the Covid-19 pandemic, it was not possible to conduct our usual enhanced oversight regime of these warrants, which involves access to the relevant systems at GCHQ. However, we were still able to review a substantial number of records provided by GCHQ in electronic form and are confident that our conclusions on this sample were representative of the whole.
- 11.37 We also reviewed a new BEI warrant for the first time on our 2020 inspection. We identified a need to improve the way in which GCHQ recorded the necessity, proportionality and risk of operations conducted under this warrant. In particular, we recommended to GCHQ that, where relevant information is stored in various locations across the corporate record, all of this information is easily retrievable using the record of reliance under the warrant as a reference point.
- 11.38 Separately, GCHQ informed us that, where EI is being conducted entirely overseas such that there is no “British Islands connection” within the meaning of section 13 IPA,²⁰ the policy is that it would still seek a Part 5 warrant even though this is not strictly required by the Act. In the context of GCHQ operations, we were satisfied that this was the appropriate policy position. We were briefed on one case in which, due to human error, GCHQ did not seek a

20 Section 13(2), Investigatory Powers Act 2016. See: <https://www.legislation.gov.uk/ukpga/2016/25/section/13/enacted>

'non-mandatory' EI warrant when it ought to have done so under its policy. A BEI warrant has since been issued.

- 11.39 GCHQ's use of BEI continues to evolve and we continue to closely scrutinise decisions taken by GCHQ as to how its suite of capabilities in this area ought to be authorised under the BEI regime.

Communications data

Bulk communications data (BCD)

- 11.40 GCHQ holds bulk acquisition warrants relating to several telecommunication operators.
- 11.41 Similar to MI5 (see paragraph 9.21), GCHQ has a system used by its analysts to outline why the examination of specific data is both necessary and proportionate. As a result of the Covid-19 restrictions, we had to delay our full inspection of GCHQ's acquisition and use of BCD until early 2021. However, we were able to incorporate an audit of BCD into our inspection of bulk personal datasets (BPD). We concluded that GCHQ's recorded justifications to undertake the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality. We were satisfied that no unnecessary examination of sensitive material was being made.
- 11.42 As we explained in our 2018 report, 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. This was achieved by including: desk-side prompts; explanatory guidance within relevant systems; and encouraging analysts to use simple text setting out what operational benefit is sought when undertaking the queries. We are satisfied that training, and awareness of the requirements set out in the CoP, had matured and that the justifications being recorded by the analysts were sufficiently detailed.

Targeted communications data (TCD)

- 11.43 Similar to MI5, GCHQ makes limited use of TCD as it has the ability to undertake queries of communications data (CD) already lawfully in its possession within the BCD holdings. The use of TCD includes acquisition of data to enrich CD obtained under a BCD warrant, helping to enhance or develop the available intelligence. On our TCD inspection, we concluded that GCHQ was achieving a high standard of compliance with the requirements of the IPA.
- 11.44 The system used to manage applications for TCD identifies the grade of a Designated Senior Officer (DSO) required; when an applicant selects a service, the system prevents progress to an approver below the statutory grade. The process requires a DSO to be selected from outside the applicant's management chain, which in turn ensures they are not involved in an operation or investigation. The independence of DSOs is managed by the Single Point of Contact.
- 11.45 Similar to our inspections of BCD, we scrutinise the majority of TCD applications authorised by the DSO that indicated the CD sought related to a person who may work in an occupation regarded as a sensitive profession. We identified no applications which raised any concerns.

Bulk personal datasets (BPD)

- 11.46 Our remote BPD inspection of GCHQ concluded that all processes and procedures inspected were carried out lawfully and in accordance with the IPA. We requested information and briefings on topics relating to the handling and management of BPDs in advance. The inspection confirmed that three recommendations made in 2019 relating to internal audit, sharing and operational purposes were all resolved.

Audit arrangements

- 11.47 Section 221 of the IPA provides that the examination of bulk datasets held under a warrant may only be selected for examination in accordance with the operational purposes specified in the warrant, and only when that selection is necessary and proportionate. Arrangements must include provisions relating to the creation and retention (for the purposes of subsequent examination or audit) of documentation outlining why access to the data by authorised persons is necessary and proportionate, as well as the applicable operational purposes.
- 11.48 There should be periodic audits carried out to ensure that the requirements set out in section 221 IPA are being met. These audits must include checks to ensure that the documentation justifying the selection for examination has been correctly compiled and, specifically, that selection for examination of data was for an operational purpose that the Secretary of State considered necessary for examination. Any mistakes or procedural deficiencies are managed internally and any breaches of safeguards are reported to the Investigatory Powers Commissioner (IPC).
- 11.49 We expect to see compliant working practices to reduce the level of interference with privacy arising from the retention and examination of a BPD. The measures can include:
- minimising the number of results presented to analysts;
 - training;
 - requiring staff with access to frame queries in a proportionate way; and
 - confining staff access to specific datasets.
- 11.50 GCHQ's Internal Compliance Team carries out retrospective audit of justifications outlined by staff for the selection and examination of BPD. When the team identify that the case for necessity or proportionality is below minimum requirements, a Policy and Compliance Lead is responsible for ensuring that the member of staff is made aware and that support and guidance is provided.
- 11.51 The Policy and Compliance Network is a network of staff distributed throughout GCHQ who are responsible for compliance in their areas. This includes working with colleagues to ensure their justifications are up to standard and providing additional training. Importantly, GCHQ was able to demonstrate how this network works throughout key business areas.
- 11.52 We were belatedly informed that GCHQ's internal audit had been paused due to staffing restrictions during the pandemic. As a consequence, we subsequently conducted a deeper audit of the justifications made by staff to examine all forms of bulk data. Before our inspection, we worked with GCHQ to select several hundred records from the system which we then examined to review the cases of necessity and proportionality from several sources including BPD and BCD. Our requests set out specific detail to enable data to be extracted from the systems and shared electronically through secure channels. During

the inspection, we spoke to the Internal Compliance Team to discuss the findings and outcomes. We concluded that overall, the justifications used to examine bulk data had correctly outlined why it was necessary and proportionate to examine the datasets.

- 11.53 Our review concluded that improvements in the standard of justifications used to examine BPDs had been made. We did recommend that the comprehensibility of some justifications required improvement. We identified a number of complex engineering terms within justifications that did not enhance the case of necessity or proportionality. We also requested that, on future inspections, the sample of justification records provided for review by Inspectors should not include records made by machine-to-machine transactions where no human interaction was undertaken and where no selection for examination by an analyst has taken place. This will ensure that the sample includes only justifications recorded by staff, enabling us to focus inspection resource in this area.

Governance

- 11.54 GCHQ's internal governance process for BPD is overseen by a Bulk Personal Data Panel. The panel meets on a regular basis to consider the necessity and proportionality of the retention and examination of all BPDs. With strong terms of reference, the panel focuses on novel and contentious, complex and/or finely balanced cases. During our inspection, we examined the minutes of the panel's meetings and noted the skill sets of attendees and the attendance of colleagues from MI5 and SIS's bulk data teams. The minutes evidenced the panel's positive impact as guardian and gatekeeper in relation to the management of BPDs (for example, reviewing proposals to renew, operational developments impacting on retention and examination and considering issues relating to proportionality). We concluded that the panel was an essential function in the lawful retention and examination of BPDs.
- 11.55 The panel maintained its governance role throughout 2020. This was evidenced in the requests made to the panel to share datasets (which we examined at inspection) and acknowledged the role of the panel and its decision-making process.

The Equities Process

- 11.56 In our 2019 report, we noted that IPCO had agreed with GCHQ to oversee the Equities Process.

Definition: The Equities Process

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

- 11.57 Our oversight of the Equities Process continues to take place on a non-statutory basis, pending a Government decision as to the future of our oversight in this area.

- 11.58 Overall, we were satisfied that the Equities Process is functioning effectively and that GCHQ is making rational, evidence-based decisions about whether to retain or release vulnerabilities. It was clear from the briefings we received on this inspection about the work of the National Cyber Security Centre (part of GCHQ) that GCHQ has a wealth of information and assessment about cyber security risks in the UK. We recommended that GCHQ ought to make more explicit reference to this in individual equities decisions where appropriate.
- 11.59 While we were content with the substance of the equities decisions we reviewed, we recommended that GCHQ should improve the way in which these decisions were recorded. Currently, the written record is not sufficiently clear to give an external reviewer a coherent picture of how a particular decision was arrived at. We have since been briefed on improvements to the systems in place at GCHQ which should address this recommendation.
- 11.60 Finally, as foreshadowed in our 2019 report, we observed an Equities Board meeting in 2020. We were impressed by the openness to challenge and debate within this senior group, as well as the emphasis placed on taking account of developments both in technology and in the national security threat picture.

Section 7 of the Intelligence Services Act 1994 (ISA)

- 11.61 We reviewed a number of operations conducted by GCHQ which were conducted in reliance on a section 7 authorisation. Section 7(9) provides as follows:
- (9) For the purposes of this section the reference in subsection (1) to an act done outside the British Islands includes a reference to any act which:
- a) is done in the British Islands; but
 - b) is or is intended to be done in relation to apparatus this is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus;
- and in this subsection “apparatus” has the same meaning as in the Regulation of Investigatory Powers Act 2000 (c 23).
- 11.62 In the light of the growing complexity of internet infrastructure, it can be increasingly difficult to determine whether a particular online operation conducted from the UK could be said to be done “in relation to apparatus” overseas. We will continue carefully to scrutinise online operations conducted in reliance on section 7 authorisations.

Safeguards

- 11.63 As set out in our 2019 report, we planned a standalone inspection at GCHQ in 2020 focusing on the handling of warranted data in GCHQ systems. The inspection had to be postponed and will now take place in spring 2021.
- 11.64 In April 2020, GCHQ took the decision temporarily to suspend or adjust a number of compliance processes or assurance controls, in the light of the pressures on staffing arising from the Covid-19 pandemic. These changes were inconsistently and incompletely communicated to the IPC and the Foreign Secretary at the time. We first learned the full extent of the suspensions and adjustments during a briefing given to the IPC in July 2020. One of the measures which had been temporarily suspended concerned the internal audit

of necessity and proportionality justifications written by analysts to justify their selection for examination of bulk data. While GCHQ always intended to conduct the necessary audits outside of the previously agreed monthly tempo (and in fact completed all audit activity by October 2020), this nevertheless represented a change and deviated from our expectations. The IPC and the Foreign Secretary made clear to GCHQ that, in future, they expect GCHQ to inform them of any changes relevant to the handling of warranted data.

12. The Ministry of Defence

Overview

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

Findings

- 12.2 In line with previous years, the MoD continues to make limited use of investigatory powers in the UK. While our proposed inspection plan for 2020 was restricted, we remain 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 (CoP) for activities both within the UK and overseas

Covert human intelligence sources and directed surveillance

Statutory inspection of CHIS and directed surveillance in the UK

- 12.3 Our inspection of the MoD's CHIS and directed surveillance activities in the UK in 2020 was delayed due to the Covid-19 pandemic and was rearranged for early 2021.
- 12.4 The MoD continues to demonstrate a high standard of professionalism and takes great care to ensure that covert activity in the UK is properly authorised under RIPA. We found the applicants, legal and policy advisors, and authorising officers to be knowledgeable and well versed in the issues and the level of consideration around necessity and proportionality is commendable. All recommendations made in our previous report have been addressed and no further recommendations were necessary following our most recent inspection. No errors were reported during the period under review.

Non-statutory inspection of overseas CHIS and directed surveillance

- 12.5 In February 2020, we carried out the deferred 2019 inspection of the MoD's CHIS and directed surveillance activities conducted overseas. This activity rarely requires authorisation under RIPA (due to the European Convention of Human Rights not being engaged) but the MoD uses processes analogous to those required by this legislation and this inspection is carried out on a non-statutory basis at the request of the MoD.
- 12.6 The overall standard of consideration by the MoD of CHIS and surveillance activity conducted overseas was very high and we made no recommendations.

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

- 12.7 We were satisfied that the MoD is complying with the IPA and the relevant CoP. The MoD has a very thorough and detailed process for internally authorising and tracking warranted activity. The MoD's authorisations were completed to a high standard and all the personnel we spoke to from various branches of the Armed Forces were well versed in the relevant legislation and had a good grasp of necessity, proportionality and collateral intrusion.
- 12.8 The MoD's internal documentation regarding the retention and deletion of warranted material is comprehensive. Last year, we recommended that the MoD draws up a formal stand-alone safeguards document for material obtained under warrant and that this should be approved by the Secretary of State. This has been done.

13. The Principles

Overview

- 13.1 On 1 January 2020, 'The Principles relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence relating to Detainees' (The Principles) came into force and replaced the Consolidated Guidance.²¹ The most important changes included:
- the inclusion of SO15 (the counter-terrorism command of the Metropolitan Police) and the National Crime Agency (NCA) alongside the UK intelligence community (UKIC) and the Armed Forces;
 - the expansion of the types of harm explicitly covered to include unlawful killing, rendition and extraordinary rendition, as well as the existing harms (torture; cruel, inhuman or degrading treatment (CIDT); and unacceptable standards of arrest and detention);
 - a change in the language used to describe the test to apply when deciding whether to refer a case to Ministers for a decision, replacing the term "serious risk" with the term "real risk". The Divisional Court when considering the Consolidated Guidance stated that there was no material distinction between these two terms, but the term "real risk" is consistent with the language used in equivalent contexts by the European Court of Human Rights;
 - explicit statements that UK personnel must adhere to The Principles insofar as possible when working with non-state actors, and that they apply to units of a foreign authority working directly with and in support of the work of UK personnel where its activities engage The Principles; and
 - a formal "errors" process for reporting to the Investigatory Powers Commissioner (IPC) instances of non-compliance with The Principles (see paragraph 13.45 below).

Findings

- 13.2 We identified a number of issues concerning the implementation of The Principles during the 12 months following them coming into force, summarised in the section below on implementation. The most significant of these is the policy on cases in which there is no causal link between the actions of UK personnel and any risk of mistreatment.
- 13.3 Generally, we observed a good level of compliance with The Principles in most of the organisations inspected, although we identified some areas requiring particular improvement on our inspections at the NCA and the MoD.

21 See: <https://www.ipco.org.uk/news/oversight-of-the-principles/>

Implementation

Cases in which there is no causal link between the actions of UK personnel and the risk of mistreatment

- 13.4 The six organisations subject to The Principles (as set out above) are known as the “Principles partners”. Collectively, they have developed a policy which applies where there is no causal link between the actions of UK personnel and the risks of mistreatment as set out at paragraph 6a and 6b of The Principles (known as “relevant conduct”). This policy was discussed in detail with the IPC, was agreed by him, and is being published here in the interests of transparency.

Agreed policy for when no causal link between the actions of UK personnel and the risks of mistreatment

In all cases where UK personnel are engaged in the activities listed at paragraph 6a-6d of The Principles,²² the Principles partners have agreed that they will proceed as follows in cases where there is no causal link between the actions of UK personnel and any risk of relevant conduct:

- Personnel must not proceed, and must notify Ministers, if they know or believe unlawful killing, torture or extraordinary rendition has occurred, is occurring or will occur.
- Personnel must submit to Ministers for approval before proceeding if there is a real risk unlawful killing, torture or extraordinary rendition has occurred, is occurring or will occur.

Where there is a real risk that any other form of relevant conduct has occurred, is occurring or will occur, personnel need not refer to Ministers unless they identify a real risk their actions will breach the UK's stated policy position (as set out in paragraphs 1-4 of The Principles), and/or there is a serious reputational or political risk to the UK Government.

Special rules apply to the receipt of unsolicited intelligence that has been obtained from a detainee in the custody of a foreign authority. By definition, UK personnel will not have had any involvement in the case prior to the unsolicited intelligence being received.

Where unsolicited intelligence is received in circumstances where there is not a real risk that relevant conduct will result from the actions of UK personnel:

- Ministers must be notified where: a) personnel know or believe the information originates from a detainee, *and* b) there is a real risk the detainee has been or will be subject to relevant conduct, *and* c) senior personnel agree there is a real risk.
- Relevant authorities²³ will consider whether there is a real risk that relevant conduct will result from the receipt of the intelligence, including the UK's response to that intelligence.

They will also consider what (if any) action is necessary to avoid the foreign authority believing that HMG's receipt of the intelligence is an encouragement of the means used to obtain it or adversely affects the conditions under which the detainee is held. The notification to Ministers must include the result of these considerations.

22 Interviewing a detainee/soliciting intelligence from a detainee via a foreign authority; passing intelligence about a detainee; passing intelligence where a detention is sought or where personnel know/believe detention will occur, including in cases where there is a real risk the subject will be unlawfully killed rather than detained.

23 This refers to relevant personnel in UKIC, the MoD, UK Armed Forces, the NCA or SO15, as applicable. The same text in the Consolidated Guidance referred to these considerations being made by “Agencies, the MoD or UK Armed Forces”.

Finally, UK personnel may receive intelligence that originates from a detainee in the custody of a foreign authority without that foreign authority's knowledge, in circumstances where there is a real risk that the detainee has been or will be subject to relevant conduct. Ministers will be notified of this fact.

Where receipt of detainee intelligence in these circumstances is ongoing, and it is not reasonably practicable for Ministers to be informed of individual instances of intelligence being received, UK personnel may provide Ministers with a general notification setting out the facts. Ministers will then consider whether the receipt of the intelligence in question is consistent with the UK's stated policy position as set out in paragraphs 1-4 of The Principles.

The "last pair of hands" policy

- 13.5 The Principles partners now have in place an agreed policy that, where intelligence is being exchanged with a foreign authority in circumstances engaging The Principles, the organisation which is directly in contact with the foreign authority will be responsible for assessing the risks involved. This policy, known as the "last pair of hands", generally ensures that The Principles partner with the most detailed knowledge of the foreign authority in question, completes the assessment.
- 13.6 We are content that this is an appropriate way to proceed where more than one Principles partner is involved in an operation. On inspection, we frequently seek to test the consistency of judgements made under The Principles across the relevant organisations.

Urgent cases

- 13.7 The Principles contain the same provision for urgent cases as was included in the Consolidated Guidance:
- "Where UK Armed Forces or other personnel are operating in a coalition with others and are under time-sensitive operational conditions...all personnel should continue to observe this guidance insofar as is practicable and report all the circumstances to senior personnel at the earliest opportunity."*
- 13.8 In discussions with the NCA and SO15 over the course of 2020, it became clear that both organisations may, from time-to-time, identify an urgent need to pass intelligence in circumstances where it is impossible to obtain Ministerial approval in time, e.g., because the intelligence is received out-of-hours and concerns an imminent threat to life. Pending any change to the urgency provisions in The Principles in the future, we have advised the NCA and SO15 that The Principles do not have any legal force in their own right, but merely set out actions personnel should take to ensure compliance with the law. As such, in a genuinely urgent case, senior personnel might decide to authorise a course of action themselves if they are satisfied, on the basis of legal advice, that it is lawful to proceed. We would expect such cases to be extremely rare and would expect Ministers to be provided with full details as soon as possible.
- 13.9 The NCA and SO15 are preparing a policy setting out how they, and the other Principles partners, would proceed in urgent cases. Once agreed, we will include details of this policy in our next annual report. We will also include statistics on the number of cases which engaged the urgency provision in future reports. We intend to examine all urgent cases on inspection.

Multi-agency assessment team

- 13.10 We have previously reported that a multi-agency team, hosted by UKIC with representation from the other Principles partners, has been established to conduct assessments of the human rights risks in countries where operations engaging The Principles are taking place. This team's work ensures that Principles decisions are made on the best available evidence base. We were concerned that this team was under-resourced at the time of our inspection. The IPC wrote to UKIC suggesting that the resourcing of the team ought to be looked at carefully to ensure it remained capable of delivering against its objectives.

Internal policies

- 13.11 Each of the Principles partners has internal guidance setting out how its staff should comply with The Principles. We have reviewed these and are content that they accurately represent the requirements of The Principles. The IPC has previously recommended to the Cabinet Office, and to the Principles partners, that these policies should be published, if possible, noting that in some cases full publication may not be possible for national security reasons.

Assessing risks of mistreatment following conviction and imprisonment

- 13.12 On inspections in 2019, we identified a number of Ministerial submissions which implied that the Consolidated Guidance did not apply after the point a detainee was convicted of a criminal offence and sentenced to a term of imprisonment. We wrote to the Government requesting clarification as to the policy position in relation to the Consolidated Guidance and The Principles.
- 13.13 In November 2020, the Government wrote to the IPC confirming that there is not a blanket policy that The Principles cease to apply once a detainee is convicted. Each case is assessed on its own facts. In many cases, the conviction will be sufficiently remote from the actions of UK personnel in exchanging intelligence that there is no longer any causal link between the UK's actions and any mistreatment in post-conviction detention. However, the Government has confirmed that it does not rely on a criminal trial to exclude entirely the possibility that post-conviction monitoring of the risk of mistreatment may be required.
- 13.14 In all cases, the variables to which UK personnel have regard include:
- their level of involvement in the case;
 - the extent to which that involvement will materially contribute to a detention by any particular foreign authority (including the likelihood of a conviction flowing directly from that involvement);
 - the conditions in detention (including in relation to due process); and
 - assuming that their involvement is assessed to contribute materially to a detention by one or more foreign authorities, whether any conditions that fall below the requisite standard can be mitigated or assured against.
- 13.15 We were content with this explanation of the Government's policy position and will evaluate relevant cases on future Principles inspections against it.

MI5

- 13.16 We inspected MI5's compliance with The Principles by reviewing a sample of cases in which MI5 was sharing intelligence directly with a foreign authority. Overall, we were satisfied that MI5 was maintaining a high level of compliance. However, we once again observed several instances where caveats attached to intelligence passed to a foreign authority were not being applied appropriately, either because they omitted relevant requirements or were out of date. MI5 has an action plan in place to improve standards in this area and we expect to see improvements in 2021.
- 13.17 We also reviewed a number of cases at the Secret Intelligence Service (SIS) which involved sharing intelligence with a foreign authority in support of an MI5 intelligence requirement. SIS had already produced an assessment of the risks, but MI5 also produced its own internal documentation considering those same risks. Given that the risks had already been assessed in detail by SIS, we concluded that MI5's internal records were unnecessarily detailed and might risk causing confusion by duplicating or contradicting judgements made by those with more detailed knowledge of the foreign authority in question.

Secret Intelligence Service (SIS)

- 13.18 Our first Principles inspection at SIS took place in March 2020 and was disrupted by the national lockdown. We read papers covering a range of cases and asked SIS questions about them by correspondence, but it was not possible to hold any in-person discussions either remotely or face-to-face. We identified an issue concerning the potential mistreatment of detainees in a facility overseas by a foreign authority. We followed this up on a separate investigation (see paragraph 13.37 for further details). Our other substantive recommendations focused on the implementation of The Principles (see above).
- 13.19 In December 2020, we reviewed a broad range of cases engaging The Principles. In many cases, the underpinning authorisation was owned by SIS but MI5 and/or the Government Communications Headquarters (GCHQ) also relied on it for their own purposes (e.g., to authorise the passing of intelligence to a foreign authority via SIS).
- 13.20 Despite the challenging operational context to many of the cases we reviewed, we observed a high level of compliance with the requirements of The Principles. Risk-based decisions continued to be made on the basis of detailed and careful legal advice combined with a solid body of evidence as to the human rights risks involved. This was the case even in very difficult or urgent decisions.
- 13.21 The Principles make clear that there is a 'presumption not to proceed' in cases where there is a real risk of torture which cannot be mitigated. We reviewed one example in which this presumption was engaged and which SIS submitted to the Foreign Secretary for approval. We reviewed SIS's submission and the accompanying legal advice in some detail. We were satisfied that the Foreign Secretary was entitled to conclude that, despite the risks, it was nevertheless lawful to proceed. We were also satisfied that both SIS and the Foreign Secretary had paid proper regard to the requirements of both domestic and international law and to the UK's stated policy that it does not encourage, solicit or condone torture.
- 13.22 Separately, we reviewed a number of cases in which there was an identified risk that detainees might be subject to methods of obscuring vision. We carefully considered these cases in the light of both Annex B of The Principles and the Divisional Court's decision in *Al Bazzouni and others v Prime Minister* and concluded that the Secretary of State was entitled to approve the various submissions involved. We noted in particular the

analysis that methods of obscuring vision do not *automatically* constitute CIDT and that the question of whether a particular technique, considered in context, is unlawful and/or contrary to UK policy is a question of fact.

- 13.23 We also reviewed a number of cases in which allegations of mistreatment arose in the context of detention operations. The evidence we reviewed suggests that these were followed up thoroughly and, where necessary, robust action was taken to ensure no further intelligence work was done with the offending party.

Government Communications Headquarters (GCHQ)

Intelligence support to debriefings conducted by third countries

- 13.24 Our Principles inspection at GCHQ in 2020 identified that, on occasion, GCHQ grants permission for its intelligence to be used by third countries to inform the debriefing of a detainee in the custody of a foreign authority overseas. In these cases, GCHQ assessed that there was no causal link between the use of GCHQ intelligence in the debriefing and the subsequent treatment of the detainee.
- 13.25 The Principles require Ministers to be consulted in all cases involving the passing of intelligence about detainees where there is a real risk that relevant conduct “will result from...interviewing detainees” (paragraph 6b of The Principles); for these purposes, it is immaterial whether the interview is being conducted by the UK or by a third party. We recommended to GCHQ that its contribution to detainee interviews in such cases ought to be brought to Ministers’ attention, enabling them to consider the causality of UK involvement and the associated legal and policy risks in line with paragraph 14 of The Principles. This recommendation has since been discharged.

Assessment of international law risks

- 13.26 We were pleased to note that, when considering cases that engaged The Principles, GCHQ was also carefully assessing the wider international law risks associated with passing intelligence, where necessary. We reviewed a number of cases in which GCHQ assessed whether there was a risk that passing the intelligence in question might lead to an internationally unlawful act; where any such risk was identified, GCHQ rejected the request.

Use of a list for low risk countries

- 13.27 GCHQ maintains a list of countries it judges to pose low risks under The Principles. GCHQ adds a country to the list if it judges there to be a lower than real risk of relevant conduct when sharing intelligence with that country. Unless there are particular concerns raised in relation to an individual case, GCHQ does not complete individual assessments against The Principles for cases in countries on the list. We noted that the list was underpinned by a detailed evidence base compiled by a specialist, multi-agency team, and was subject to regular review. We were therefore satisfied that this was an appropriate approach to countries posing low levels of compliance risk.

The Ministry of Defence (MoD)

- 13.28 During our inspection in March 2020, we identified serious gaps in the MoD’s assessment of the risks under The Principles in a particular operational context. Some of the risks arising from the MoD’s operational activity had not been assessed adequately, or at all. We

recommended that the MoD conduct a comprehensive refresh of its risk assessment in this area by overhauling its internal assessments and its Ministerial submissions. Shortly after the inspection, in response to this recommendation, the Minister of State for the Armed Forces initiated a programme of work to revise and refresh the MoD's approach. While we will report our findings on the results of this programme of work in full in 2021, our initial review of the MoD's updated submissions and other documents in 2020 suggested that the risks are now being more clearly and comprehensively assessed.

- 13.29 Separately, we noted that in a number of internal assessments, MoD personnel framed their decision under The Principles as a simple balancing exercise between the rights of the detainee on the one hand and the necessity case on the other. These comments mirror a statement (since corrected) in the MoD's internal policy on the Consolidated Guidance that Ministers might authorise action if they "agree that the potential benefits justify accepting the risk and the legal consequences that may follow." The MoD has acknowledged that it is never sufficient, where a real risk of mistreatment exists, simply to assert that this risk is outweighed by the importance of the objective sought. We are satisfied that the MoD has corrected its policy in this area and expect to see no similar comments in future given the communications that have now gone out to MoD personnel on the matter.

The National Crime Agency (NCA)

- 13.30 We conducted our first Principles inspection at the NCA in June 2020. We noted that the NCA had an internal policy of only assessing the risks of relevant conduct up to the point a detainee was charged with an offence, which in some cases might occur soon after the initial detention. Having regard to the requirements of The Principles and the approach taken by other Principles partners, we concluded that this was not appropriate. We recommended that the NCA should assess each case on its own facts, taking into account the extent to which the NCA may be making a material contribution to any relevant conduct arising from the detention, charge and/or conviction and imprisonment of the detainee. The NCA has since made clear to its officers they must approach risk assessments under The Principles on this basis.
- 13.31 We reviewed a range of country assessment documents produced by the NCA as an overview of the relevant risks in a given country to support decision making under The Principles. We concluded that these documents were insufficiently focused on the particular risks covered by The Principles, and that their ongoing use risked confusing officers by introducing new and potentially contradictory or extraneous information. The NCA has introduced more focused assessments and officers no longer use the Country Assessment when completing assessments in respect of The Principles.
- 13.32 We identified that the quality of risk assessment conducted under The Principles was variable. In some cases, judgements about risk presented across multiple documents could not easily be reconciled. Overall, officers appeared to be assessing all possible risks on a "worst case scenario" basis, rather than examining in the light of the specific risks arising from the activity the NCA was seeking to conduct and the available mitigations.
- 13.33 Following the inspection, the NCA has kept us updated on the actions it has taken in response and we have already observed an improvement in the quality and structure of the NCA's internal documentation. We expect to see further improvements in 2021.

SO15

- 13.34 We conducted our first Principles inspection at SO15 in June 2020. Having regard to the fact that SO15 had only been subject to The Principles for six months at the point our inspection took place, we were impressed by the standards of training, internal processes and paperwork we reviewed.
- 13.35 We identified a need to improve SO15's assessment of Principles risks in one particular country where one of its liaison officers was operating, but otherwise the standard of decisions we reviewed was high.
- 13.36 The other issue identified on this inspection concerned cases where SO15 needed to make judgements about risk under The Principles which rely on an assessment which has previously been made by another Principles partner. In the example we reviewed, SO15 did not ask to see that assessment; we concluded that it ought to have done so and ought to do so in all such cases.

Investigation into potential mistreatment of detainees

- 13.37 In the course of an inspection at SIS in 2020, we became aware of allegations of unacceptable treatment in a detention facility overseas by a foreign service, in which individuals were detained as a result of UK operations.
- 13.38 The facility was subject to compliance monitoring by Foreign, Commonwealth and Development Office (FCDO) staff overseas, who reported to a joint oversight team. We therefore launched a standalone investigation into the allegations, reviewing relevant material at both SIS and the FCDO and discussing the matter with members of the oversight group.
- 13.39 An individual employed by the FCDO was the first member of UK personnel to learn that detainees in the facility were being subject to treatment that was highly likely to constitute unacceptable treatment under The Principles. This individual heard about the treatment second-hand and did not directly witness the practice. They did not report the allegations to the oversight group until around a year later, when a detainee made a specific allegation that he had been subject to unacceptable treatment.
- 13.40 When the oversight group became aware of the treatment, the group did not identify the practice as unacceptable when it ought to have done. This error has since been corrected and the FCDO has now obtained credible assurances that the practice will not be used in future.
- 13.41 The FCDO has also taken steps to ensure that its response to allegations about potential mistreatment are handled appropriately in future. This includes the inclusion in the oversight group of an FCDO legal adviser.

Errors

Background

- 13.42 The Consolidated Guidance did not include a formal process for reporting incidents of non-compliance to the Investigatory Powers Commissioner's Office (IPCO). This has now been addressed in The Principles, which include a process for reporting non-compliance

to the IPC. For simplicity, we have referred here to reports of non-compliance with The Principles as “errors”.

- 13.43 All of the organisations subject to The Principles must report any error of which they are aware as soon as reasonably practicable after the event has been identified by internal governance procedures. The organisation must also make the details of both error and investigation available on inspection. When an error is reported, the IPC will determine whether non-compliance has indeed occurred. If non-compliance has occurred, the IPC will assess the level of seriousness and will determine the appropriate response. For serious errors, this may involve raising the matter with the principal of the relevant agency, department or authority and the matter may be reported to the Prime Minister, either in our annual report or immediately by separate letter. If the IPC has concerns that criminal conduct may have taken place, he will raise the matter with the relevant agency, department or authority and, if he has continuing concerns, may refer the matter to the relevant UK authorities.

Errors reported in 2020

- 13.44 Four errors were reported to IPCO in 2020: three from the NCA, and one from SO15. All three of the NCA's errors involved the passing of intelligence to a foreign authority without fully applying The Principles. SO15's error involved soliciting intelligence from a detainee without assessing the risk of relevant conduct. In all cases, we concluded that these errors were not sufficiently serious to require any further action and that appropriate steps had been taken to prevent recurrence. It is not surprising that SO15 and the NCA reported errors during the first 12 months of being subject to The Principles, during which time changes to their working arrangements were taking effect.
- 13.45 Separately, The Principles require the IPC to be notified as soon as reasonably practicable if a relevant public authority becomes aware that any conduct to which The Principles relates has or may have led to: an unlawful killing; torture; CIDT; extraordinary rendition or rendition; or unacceptable standards of arrest and detention. There were no such incidents reported in 2020.

14. Law Enforcement Agencies and Police

Overview

- 14.1 Throughout 2020, we conducted oversight of law enforcement agencies (LEAs) across England and Wales despite the inevitable disruption caused by the Covid-19 pandemic. As set out in Chapter 2, alternative ways to conduct inspections needed to be found to mitigate the impact of Covid-19 on our work. While meetings could be conducted helpfully by video, the most challenging aspect was to find a means to examine remotely authorisations for covert activity, either by accessing an IT database or electronic versions of the relevant documents. We were very conscious of the sensitivity and confidentiality involved in trying to do things differently and we are very grateful for the co-operation and willingness of forces and agencies who enabled remote inspections to be conducted. As a result, we carried out 95 inspections in 2020 across territorial forces, Regional Organised Crime Units (ROCs), the armed service's police forces (Royal Naval Police, the Royal Air Force Police and Royal Military Police), the National Crime Agency (NCA) and Her Majesty's Revenue and Customs (HMRC).
- 14.2 Some inspections were necessarily abbreviated, with less emphasis on interactive meetings with practitioners and a greater emphasis on the examination of authorisations. We asked some forces and agencies to facilitate Covid-compliant inspections where we believed it was essential. This assessment was based on the nature and scale of the organisation, their usage of covert activity (both in terms of volume and scope) and compliance findings in previous inspections.
- 14.3 Counter Terrorism Policing Units are an example where this has proved particularly challenging in this regard given the sensitivity of their investigations and operations. As a result, no units of this category were inspected after the first quarter of 2020. They will be a priority for 2021.
- 14.4 The Investigatory Powers Commissioner's Office's (IPCO's) role in the renewal of long-term covert human intelligence source (CHIS) authorisations of relevant sources moved online at the outset of the pandemic. Renewals of authorisations for use and conduct of relevant sources that extend past 12 months require a comprehensive review by an Inspector of the management and governance of undercover operatives to be reported to the Judicial Commissioner (JC), who will consider whether to approve the renewed authorisation. These reviews were conducted via telephone or video conference calls, which allowed the Inspectors to speak directly to staff managing the operations.
- 14.5 We also managed our data assurance inspections of police and LEAs remotely in 2020. For the majority of forces, we interviewed relevant personnel, such as heads of units and strategic leads responsible for storing, using and safeguarding data obtained by the authority. Where possible, we were able remotely to access police systems to check policies, training, and any scheduling of review or deletion requirements. Based on our findings, we wrote to each Chief Constable outlining both specific observations identified

during our inspection and general guidance based on the information we have obtained about data safeguarding across the country. We also worked with the National Police Chief's Council (NPCC) to design and issue general information to further understanding of safeguarding principles across the country. We have stressed that it is now incumbent upon each force to demonstrate progress against these observations and guidelines and to minimise any period of non-compliance with a safeguarding action plan.

- 14.6 From April 2021, forces which are non-compliant with safeguarding requirements²⁴ and assessed as not making progress towards compliance²⁵ will receive data assurance recommendations as part of their routine inspection reports. In the future, we will test safeguarding measures against IT systems and physical storage. This means that, in most cases, we will wrap our data assurance into routine inspections; the exceptions will be some of the larger forces, such as the Metropolitan Police Service (MPS) and Police Service Northern Ireland (PSNI), where these important safeguards will continue to be monitored by a standalone data assurance inspection.

Findings

- 14.7 Our inspections of CHIS and surveillance found that LEAs recognise the human rights needs and evidential benefits of compliance with the legal provisions of the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA). However, while investment in processes, structures and governance to ensure compliance has been considerable, mistakes continue to be made. These are identified through the double lock procedure of JC oversight, the inspection regime, or the self-reporting of errors (which in itself is a positive indication).
- 14.8 The 2019 IPCO Inspection report for Greater Manchester Police (GMP) highlighted several compliance issues for the force in respect to CHIS and surveillance. Many of the issues raised had been highlighted in previous reports and, despite the efforts of some, had not properly been addressed. The Investigatory Powers Commissioner (IPC) personally visited GMP headquarters in January 2020 and discussed the lack of progress directly with the Chief Constable. The compliance issues discussed included outdated methods, inconsistent training for authorising officers (AOs) and limited oversight and management arrangements. The organisation's Senior Responsible Officer (SRO) and his management team responded positively and implemented changes in an effort to improve compliance. Experienced staff were employed in key roles, funding was secured to facilitate the purchase of commercial software and a cadre of accredited AOs was formed. An inspection of the organisation in October 2020 confirmed the measures taken have dramatically improved compliance levels. This is an excellent example of how IPCO inspection teams work with SROs to improve compliance with the legislation.
- 14.9 Our work on data assurance identified weaknesses in the safeguarding of data obtained under all covert powers used by law enforcement. We have seen a tremendous effort by the Police to review and revise policies, to address weaknesses in automatic and manual processes and to demonstrate adherence to compliance principles at the core of their business. Our inspections in 2020 sought to fact-find on this topic but we have signalled a requirement for substantial improvement to be demonstrated to our teams throughout 2021. We asked each force to identify and review the data pathways for relevant material

24 Requirements are set out in IPA 2016, RIPA 2000 and in the safeguarding chapters of Code of Practice for each covert tactic.

25 'Progress towards compliance' is defined as the force meeting the minimum expectations set out under the final sub-heading within this letter.

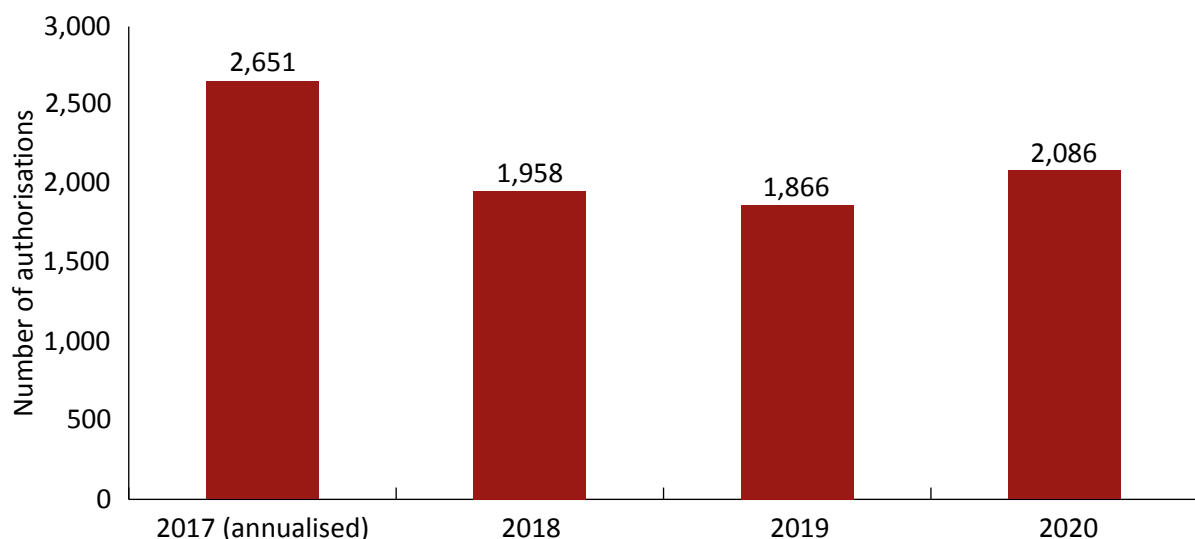
across all teams and systems from acquisition to deletion. This will enable meaningful action on core safeguards such as reduction of duplication and will inform policy reviews. So far, good progress has been made, but most forces have not yet completed this work.

- 14.10 All forces have legacy material stored on IT systems, hard-drives and physically in local and central storage. Forces also note that there will be some material stored in ungoverned spaces, such as team/individual email accounts and shared/personal folders, that residual material may also be held on encrypted USBs or that communications data (CD), in particular, may be held within analytical software. We requested that forces prioritised the review of their live material (i.e., that which has been obtained under an authorisation and which is still active) and material obtained from 2018 onwards (i.e. from the implementation of the IPA). Where resources were available and systems and processes allowed, we have also encouraged a review of product obtained before 2018. This included material obtained under now closed authorisations, that held on systems which were no longer in use and that retained on a long-term basis, for example in relation to historic investigations, sometimes referred to as 'legacy material'. Some forces are starting to index and organise legacy material ready to implement refreshed retention, review and deletion (RRD) policies. We believe that this will give a comprehensive picture of what material is being held and ensure that all material held in physical or technical storage will be compliant in the future.

Covert human intelligence sources (CHIS)

- 14.11 The acquisition of intelligence using CHIS remains a core function of the LEAs. This specialised covert tactic is increasingly necessary as criminal groups become more sophisticated in avoiding detection by LEAs utilising other surveillance and investigative techniques, and as these groups become more knowledgeable of covert tactics deployed. The term CHIS encompasses both members of the public who provide intelligence to the LEA and relevant sources, which is the statutory term used to describe staff from a designated LEA that are trained to act as undercover operatives and are subject to an enhanced authorisation and oversight regime.
- 14.12 Figure 14.1 shows the number of CHIS authorisations (excluding relevant sources) from LEAs since 2017.

Figure 14.1 Number of CHIS authorisations, 2017 to 2020



- 14.13 Risks presented through using a CHIS may include matters relating to the wellbeing and mental health of the individual, including the additional pressures the role may bring or other social or medical issues the CHIS may display. Increasingly, there has been a focus on these specific risks by LEAs and we have seen highlighted in individual cases the measures that have been considered or put in place to mitigate these. The National Source Working Group (NSWG) has begun a consultation process on how best to assist CHIS management teams in identifying such risks and then putting steps in place to mitigate them. Our Inspectors have offered to assist in this consultation using the evidence we gather during our inspections. This work is at a very early stage but should greatly benefit the management of risks presented by CHIS when completed.
- 14.14 Throughout the year, we have been impressed by how CHIS management teams have adapted to the pandemic restrictions. They have developed safe and novel ways to continue to manage and gather intelligence from CHIS. The specialised training undertaken by Dedicated Source Units has proved to be of significant benefit to the dynamic way in which staff have adapted to the conditions, while continuing to provide the compliant level of care and governance needed in the management of CHIS.
- 14.15 Managing these cases is necessarily one of the most bureaucratic forms of covert activity, requiring a comprehensive record of the relationship between the CHIS and the LEA. However, we continue to find that there is some unnecessary repetition of details within authorisations, in particular in circumstances where the AO is less experienced. This approach creates a risk that important matters may not be addressed within the authorisation, or that specific instructions or parameters set by the AO for the management of the CHIS may not be easily picked up by the reader (controller and handler).
- 14.16 We often find a lack of bespoke consideration given to potential collateral intrusion. We identified several examples where the same stock phrasing was used, although the CHIS clearly had gathered intelligence in different ways.

Example 1: Collateral intrusion scenarios

CHIS (A) is a member of an OCG (Organised Crime Group) and occasionally meets with other members' friends and family at social events. In this setting, issues other than the OCG's criminal enterprises will naturally be discussed.

CHIS (B) gathers intelligence on various criminal matters, such as illegal drugs supply, by associating with street dealers. These conversations can be expected to be solely, or mainly, about criminal matters of interest to the LEA.

- 14.17 Although a stock phrase may appear adequate when viewed as part of the consideration to approve a single authorisation, when viewed in succession, as is the case in an inspection, the use of similar phrasing can give the impression that little or no consideration is being given to the gathering of unrelated private information. We made observations to the relevant LEAs when cases such as these were identified. In a few cases, we made a recommendation because the evidence we saw suggested inadequate consideration, which in turn suggested a systematic failing.

- 14.18 Examples of scenarios in which CHIS have been used to glean valuable intelligence are noted below.

Example 2: Use of CHIS intelligence

A CHIS was used to create some 'theatre' in support of a Force's counter corruption investigation. The CHIS was reporting on an organised crime group, and was used to relay fictitious information to invite contact between a member of the OCG and an as yet unknown (corrupt) police officer in an attempt to identify them.

Example 3: Use of CHIS intelligence

CHIS intelligence identified an illegal drugs supply chain, commonly known as 'county lines'. Through the development of unique CHIS intelligence, the LEA was able to identify persons involved in the higher level distribution of the drugs and the use of children as 'drugs mules'. The CHIS intelligence led to the conviction of those involved in the illegal drugs supply and the safeguarding of several vulnerable children.

Juvenile CHIS

- 14.19 This category of CHIS authorisations continues to be rarely used: only three juvenile CHIS authorisations were granted in 2020. Each case is subject to close examination during our inspections. We focus on the risks to the juvenile, how their welfare is being managed and on ensuring that their use as a CHIS is not endangering them or extending or increasing their involvement with criminals.
- 14.20 There was a good deal of parliamentary debate about juvenile CHIS during the passage of the Covert Human Intelligence Sources (Criminal Conduct) Act 2021, which received Royal Assent in March 2021. An authorisation for a juvenile to engage in criminal conduct would be exceedingly rare, but the Bill reignited debate around some of the more generic concerns regarding the use of juveniles as CHIS.
- 14.21 In the light of the commentary during the passage of the Bill, as well as earlier interest of the Joint Committee on Human Rights in the use of juveniles as CHIS, the IPC has asked us to introduce more contemporaneous oversight of authorisations involving juveniles or vulnerable individuals, rather than considering these cases at scheduled inspections. This will commence in 2021, once the new legislation comes into effect.
- 14.22 Our Inspectors are members of the Home Office CHIS Working Group and have been major contributors to the drafting of enhanced guidance in the CHIS Code of Practice (CoP) relating to the safeguarding and welfare considerations of juvenile CHIS.

Participation in Criminality

- 14.23 Among LEAs, authorisations to participate in crime are still relatively infrequent. A high proportion of those that are granted relate to an authorised CHIS being a member or showing support for an organisation that is proscribed,²⁶ in order to be able to report on the machinations of those organisations that are a threat to national security. Other authorisations relate to an authorised CHIS carrying out criminal activity to prevent a greater crime, or to prevent harm to others. In many cases, the activity relates to a crime that is already being planned or carried out. The AO will consider the planned action, including the likely consequences of not supporting the CHIS to conduct a potentially criminal act, and how allowing that action will allow the authority to progress their investigation.

Example 4: CHIS Participation in Criminality

CHIS are, on occasions, offered illicit goods to buy such as a firearm. The purchase of the firearm prevents it being sold to another person, enables the weapon to forensically be examined and stimulates a closer investigation of the seller based on the 'actionable intelligence' of their illegal activities.

Relevant sources

- 14.24 The enhanced authorisation and oversight regime in relation to relevant sources came about as a result of concern regarding how this form of covert activity was being managed. This followed several revelations regarding historic cases and a number of police internal investigations. A public inquiry was established by the then Home Secretary in 2015.²⁷

Table 14.1 Relevant sources authorisations and applications, 2020¹

Total Applications (incl. renewals) ²	Total Authorisations (incl. renewals)	Urgent	Renewals (long term authorisations)	JC refusals ³
301	293	2	75	0

Notes:

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

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

3 Refusals relate to applications to renew only.

- 14.25 The Covid-19 restrictions in 2020 had a substantial impact on operations involving the physical deployment, as opposed to online deployment, of operatives. The lockdown restrictions and subsequent social distancing measures resulted in some operations being cancelled or reduced due to the dangers of meetings in person. Units responsible for the

26 Under the Terrorism Act 2000, the Home Secretary may proscribe an organisation if they believe it is concerned in terrorism, and it is proportionate to do. For the purposes of the Act, this means that the organisation: commits or participates in acts of terrorism; prepares for terrorism; promotes or encourages terrorism (including the unlawful glorification of terrorism); is otherwise concerned in terrorism.

27 The Undercover Policing Inquiry. See: <https://www.ucpi.org.uk/>

management of undercover operatives invariably carried out a generic risk assessment in the light of the pandemic and overlaid this with case specific considerations. Decisions to delay contact, revert to telephone contact, or give permission for contact were taken on a case-by-case basis.

- 14.26 Online deployments, which have been the growth area, were less affected by the pandemic but the restrictions nevertheless needed to be factored into the deployment of operatives and their working conditions.
- 14.27 In our 2019 report, we noted that we were working with the Home Office to discuss changes to the CoP which would help practitioners by clarifying grey areas in the current guidelines. In particular, we are proposing changes to the CoP in relation to the guidance and considerations when deciding if a relevant source is authorised as part of the same investigation or operation, which would require a renewal to be issued by means of the enhanced authorisation and oversight process required for long-term authorisations. This would help to deal with instances where authorisations are cancelled at a point just short of the 12 months and new authorisations are granted purporting to be for a new operation, even though the nature of the deployment and purpose of the operation is the same. The deployment and operation are not considered to be the same because there is not likely to be interaction with subjects previously encountered.
- 14.28 We have seen this practice particularly for online investigations, where operatives are frequenting websites and social media sites where illicit activity is being conducted or enabled. The interaction with subjects on those sites is often fleeting. Operatives are, in effect, covertly patrolling this virtual world and interacting with persons suspected to be committing crime. The need for this enforcement activity can go on for prolonged periods. We are concerned that some forces may be cancelling, rather than renewing, authorisations around the 12-month point, which avoids the higher level of authorisation, including scrutiny by the Chief Constable (or equivalent) and prior approval by a JC. We have found a lack of consistency in this area both within, as well as among, LEAs. We have continued to suggest that applying to renew the application, with the higher level of scrutiny, should be considered as best practice if the applicant is unsure of the right approach. Cancellations just prior to the 12-month point will be closely scrutinised to ensure the enhanced authorisation regime is not being circumvented. Although no relevant source applications have been refused by a JC in 2020, this is not surprising given the involvement of our Inspectors in the nine-month review process.

Data assurance in relation to CHIS material

- 14.29 Access to CHIS material is typically restricted to the small number of defined roles set out in the CHIS CoP and is well managed. However, our inspections identified problems in relation to indefinite retention of CHIS material. Guidance from the NSWG has been retention for the lifetime of the CHIS plus 100 years, with 10-year review points which should establish the continuing need to retain or destroy the material. This policy is often cited by forces. There are varying levels of interpretation of this policy in terms of the intended duration of retention, but in practice there is no process to implement reviews. We have found that forces, with some limited exceptions, are not comfortable destroying any CHIS material. In some instances, the UPCI was cited as a barrier to reviewing or deleting any CHIS material. Although any material relevant to the UPCI must be retained, we discussed the issue of data retention with the relevant units and have suggested that they should consider what RRD policies should look like in this space once the inquiry has been concluded. We observed that the purpose and intended duration of all retention should be clear and each force should ensure that they are appropriately applying RRD principles to CHIS material,

as well as the strict access controls which we have seen. We were pleased to note that some forces are indexing, or have indexed, CHIS material in anticipation of implementing a refreshed CHIS retention policy. Most forces still have work to do to organise physical and electronic material.

- 14.30 Another issue we identified was the absence of an electronic workflow system in some smaller forces. Typically, the process for acquiring and retaining CHIS material is that all hand-written notes from CHIS/handler meetings are transferred onto a contact log within the case management system. The hand-written notes are also retained in physical storage. Multiple forces are considering scanning the original hand-written notes and attaching these to the contact log held on the electronic case management system, negating the need to retain the original hand-written notes. This is something the NSWG have sought legal advice on in the past.
- 14.31 Some forces are currently recording telephone conversations with CHIS either via the use of a third-party company software (Invisilink for example) or by using their business mobile phone when physically meeting the CHIS. In most cases, these calls are then deleted once the contact log is typed onto the case management system. Some forces retain both with the SD card or Invisilink call being added to the Charter record.²⁸
- 14.32 Very few forces were able to state with confidence they had a clear schedule of all legacy CHIS, whether the record was held on a current case management system, a hard-drive de-commissioned system or in physical storage. We observed that forces should have a central record of where all such material is stored, as well as a record of the purpose and intended duration of retention.

Surveillance and property interference

- 14.33 Despite Covid-19, law enforcement has continued to make effective use of covert powers, mindful of the risk factors linked to Covid-19 to ensure the safety of staff members and the public. We found good evidence of this for surveillance deployments.

28 Charter is a commercially supplied covert tactics records management system, used by many LEAs.

Figure 14.2 Number of intrusive surveillance authorisations and number of directed surveillance authorisations, 2017 to 2020

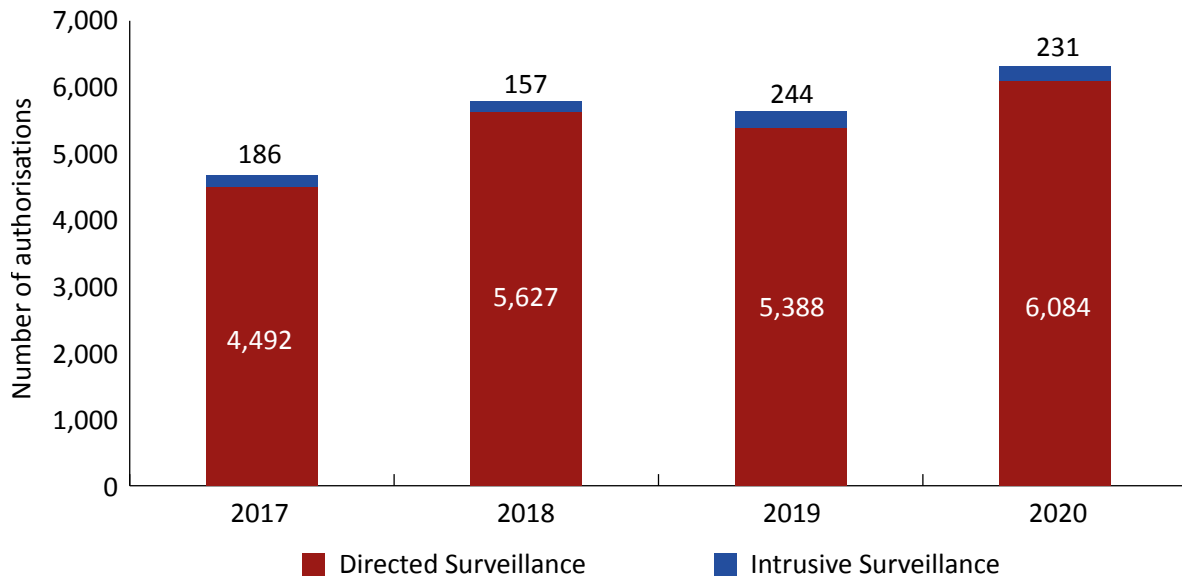
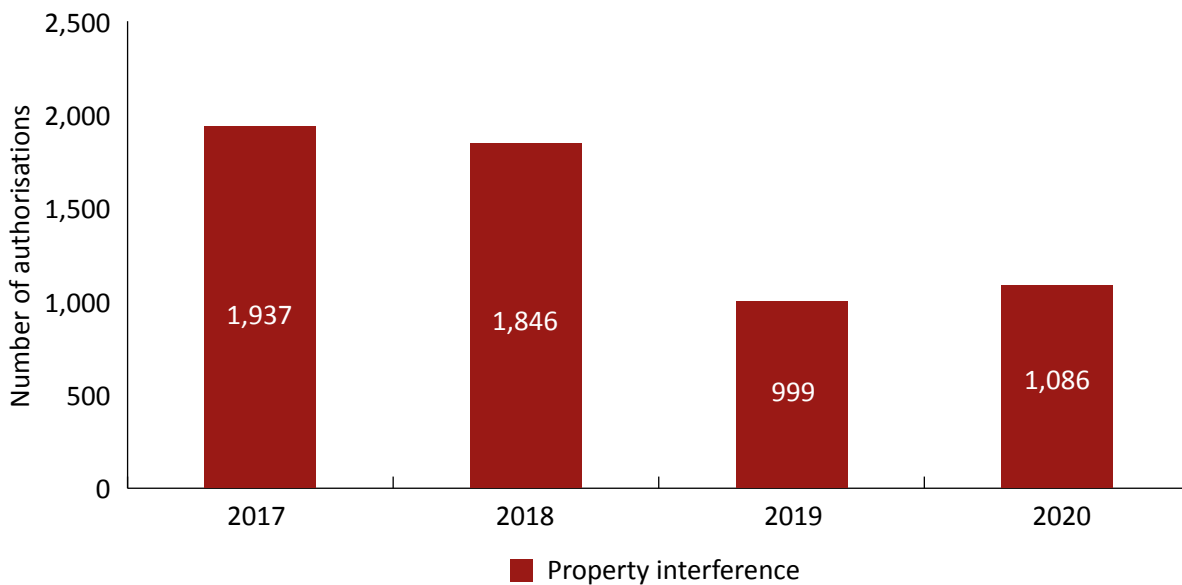


Figure 14.3 Number of property interference authorisations, 2017 to 2020



14.34 While the quality of applications and authorisations of covert surveillance and property interference does vary slightly throughout the law enforcement community, we have found that there is generally a very good standard being applied and that those involved in the process are committed to ensuring compliance is always achieved.

14.35 Those forces with the highest standards of compliance are those where the Covert Authorities Bureau (CAB) structure within the organisation has strong engagement and communication lines with force and senior authorising officers as well as operational teams. Most CAB managers adopt robust and challenging attitudes to ensure compliance with the legislation. In those organisations where standards of compliance are strongest, the CAB and CAB managers are also extremely visible.

- 14.36 This year, we have seen good evidence that the various Covert Operations Management Systems in place within organisations are better used and the functions available are fully being capitalised. This has enabled Inspectors to have a more holistic view of the administration of the records linked to operations and to have sight of the rationale and legal basis behind key decisions. We have encouraged the use of these systems, which support an open and transparent view of operational decision making. We have found that in many forces the administration of records attached to the authorisation of covert tactics has been very good and there has been a significant increase in the maintenance of policy and decision logs to demonstrate evidence which would justify when key changes affect authorisations.
- 14.37 We have found that applicants for covert surveillance and property interference can provide overly lengthy intelligence cases to an AO. The best intelligence cases we examined focused on the key elements which justify necessity and proportionality and therefore enable AOs to provide bespoke and specific considerations. In some cases, the length of intelligence cases can overload AOs with unnecessary information, making it more difficult for them to discern what is relevant. We also see overly lengthy commentaries by AOs, which again makes it more difficult for senior AOs to draw on the key information relevant to their decision making. We have made observations to a number of forces to ensure that the intelligence cases and supporting comments focus the information and intelligence on the key aspects of investigations. This will help illustrate to AOs where investigative hurdles exist and why it is necessary to deploy covert surveillance and property interference, as well as demonstrate why the activity sought is the least intrusive method to reach the operational objective.
- 14.38 We have seen examples where applicants fail to explain why each surveillance tactic required is necessary. These more generic approaches are more prevalent in applications relating to surveillance using ANPR, CCTV, social media monitoring and the use of recording equipment. We have made observations reminding applicants to provide adequate justification for each tactic and, additionally, not simply to seek a suite of covert tactics just in case they may be required.
- 14.39 We have similarly observed that it is essential to record bespoke considerations of proportionality. Some applicants rely on templated and formulaic descriptions of the key elements required. While we accept that proportionality arguments relating to a class of covert tactics may be similar, the best applications contain specific considerations based on unique features of the investigation, the individuals being targeted and the tactics being sought.
- 14.40 These observations apply equally to considerations attached to collateral intrusion. Some applications lack the specificity to enable a full assessment of the risk and the most effective identification of the control measures necessary to reduce the risk to those who are not the targets of the covert activity. Some applications cover disclosure provisions under the Criminal Procedure and Investigations Act 1996 (CPIA) as opposed to the considerations required by RIPA and the CoP.²⁹ Again, we have found very good evidence in some forces, where applicants showed excellent appreciation of the risk and are developing comprehensive management plans to reduce the impact on individuals not subject to the activity. This thereby ensures that Article 8 rights are protected and that any material gathered is appropriately handled in line with the CoP.³⁰

29 Home Office Code of Practice on Covert Surveillance and Property Interference, August 2018; and Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017.

30 Ibid.

- 14.41 Authorisations provided by AOs are generally of a very good standard, with the vast majority providing bespoke considerations for the necessity and proportionality of the tactics being sought. There is some evidence that AOs still rely on a templated form of words but, as we set out above, the best examples were found in cases where the application itself contained a focused intelligence case and specific arguments around necessity and proportionality to enable better considerations to be made by AOs.
- 14.42 We have made observations in relation to the submission of reviews and the context being provided on the progress of investigations that would enable AOs to be fully aware of the regularity of the tactics being deployed, what those tactics are achieving and how they may be benefiting an investigation. In many cases, reviews concentrate on certain tactics, mainly the physical deployment of surveillance assets, while ignoring or showing minimal focus on the frequency of use of the other authorised tactics and what benefit is being brought by them. We have advised that it is only when applicants provide a full picture that AOs appropriately can consider whether the authorised activity continues to be necessary and proportionate. We continue to see an increase in verbal cancellations; these are being used to good effect and being appropriately followed up by formal written cancellations.
- 14.43 We have found very good processes in many organisations in relation to the obligations laid down by *R v Sutherland*, where records are maintained to show that operatives are fully aware of the activity being authorised and of any parameters being set by AOs. We have noted robust processes which minimise relevant errors, which often occur when operatives are not fully aware of the extent of an authorisation and therefore conduct activity beyond what is authorised. Many of the CABs we inspected participate in the National Covert Authorities Bureau (NCAB) Group, which works to embed high standards nationwide.
- 14.44 As we reported in 2019, the processes many forces had in place for the administration of urgent oral applications and authorisations fell below the standard expected. The reasons for this ranged from the lack of contemporaneous note taking from applicants and AOs, to recording and administration processes in place not being fully auditable. While this is a general finding there have been instances where forces have been found to have well developed processes and high standards of administration on management systems. This is an area of compliance that we will scrutinise in more detail in the future.

Data assurance in relation to surveillance, property interference and intrusive material

- 14.45 In accordance with the CoP, internal safeguards for this material must be kept under periodic review to ensure that they remain up-to-date and effective. We were briefed about good practice, particularly in specialist teams, but this was not reflected in policy documentation. The lack of written procedures means that teams will struggle to demonstrate that safeguards are applied and are effective. We have advised that applications should more clearly and consistently address safeguarding issues and set out how material to be obtained will be handled. This detail was lacking in many applications we examined.
- 14.46 We noted that the absence of formal processes creates a risk when different units within a force require access to surveillance material. For example, some forces share material between: a surveillance deployment team; a serious and organised crime unit, a major crime unit; other proactive policing teams; an imagery processing team; a digital forensics team; and a disclosure team. In this scenario, it is important for forces to review pathways for surveillance material and to develop processes and procedures that set out the responsibilities for each unit and individual handling the product.

- 14.47 Surveillance teams will often undertake taskings on behalf of other forces or partners. When this situation occurs, it should be agreed who has responsibility for the material and, if copies are made, who will ensure all product is handled consistently in line with agreed RRD.

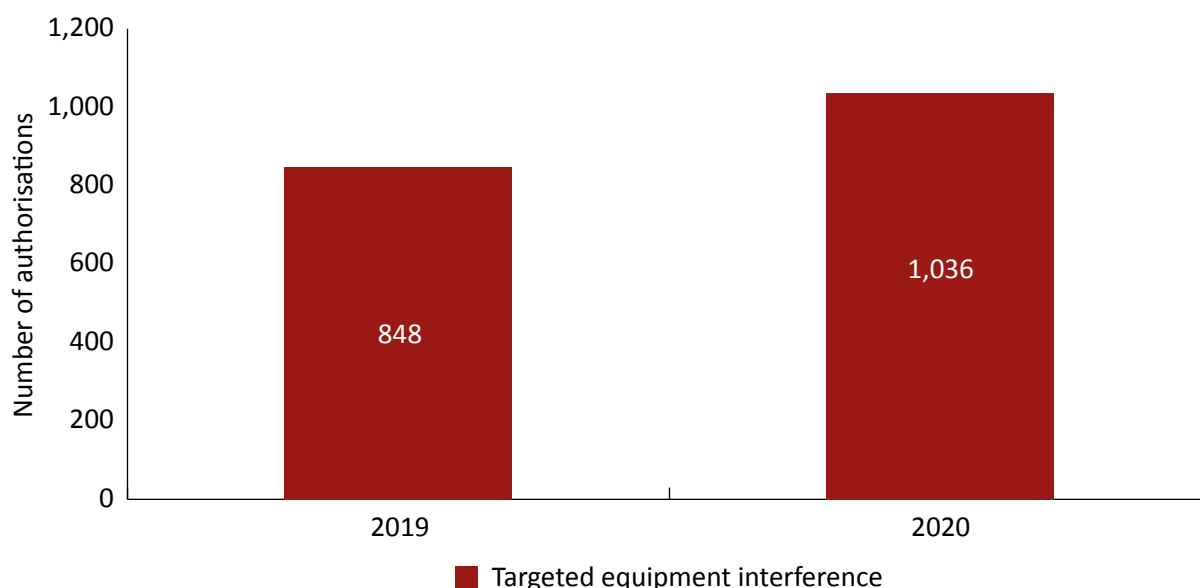
Legal professional privilege (LPP) material

- 14.48 During our inspections, we identified several cases where the likelihood that LPP material may be obtained was not well addressed on the application. Although we have a high level of confidence that any sensitive material obtained was handled appropriately, this issue has been a focus for Inspectors with several recommendations and observations being made during the year. We have found that some AOs do not fully acknowledge the potential, or likelihood, of acquiring material subject to legal privilege. Applications show an over-reliance on the generality that LPP material is usually unlikely to be obtained. In most cases where Inspectors have required remedial steps to be taken, AOs had failed to acknowledge and then document the required specific considerations. This often related to when covert surveillance was undertaken after a subject has been released from custody pending further investigation, having already received legal representation. This will continue to be a focus for both Inspectors and JCs.

Targeted equipment interference (TEI)

- 14.49 Part 5 of the IPA makes provision for LEAs to obtain warrants for TEI which are used to obtain communications, equipment data or other information where to do so would otherwise constitute an offence under the Computer Misuse Act 1990 (CMA). TEI covers interference with any equipment producing electromagnetic, acoustic or other emissions; in more simple terms, this means desktop computers, laptops, tablets, smart phones, other internet-enabled or networked devices and any other devices capable of being used in connection with such equipment. As shown in figure 14.4, there were 1,036 TEI authorisations in 2020. Of these, 344 were urgent authorisations.

Figure 14.4 Number of targeted equipment interference authorisations, 2019 to 2020



- 14.50 TEI applications have the potential to be complex, describing technically complicated and potentially novel actions. This poses a challenge to the authorities applying for warrants because they are required accurately, yet succinctly, to describe the planned operation, as well as providing an appropriate assessment as to the extent of risk for any collateral intrusion.
- 14.51 It is also challenging at times to define the boundaries between TEI, targeted interception (TI) of live-time communications and the field of digital forensics. This can arise, for example, where LEAs seek to retrieve evidence from cloud-based storage, following an arrest and the seizure of a telephone or computer during reactive investigations. Because of a lack of clarity and guidance on how existing statutory powers can be exercised to obtain this material, we have seen an increase in applications for TEI to conduct forensic examinations of communication devices to retrieve data held remotely on the internet, such as email or social media accounts. In some cases, this has involved direct access to this data where usernames and passwords have been lawfully acquired but it has not been possible, or feasible, to access the accounts using the seized device as a conduit.
- 14.52 Recognising the challenge of these boundaries, we are developing a revised inspection model to combine the oversight of TEI alongside the LEA use of TI, and the acquisition of communications data (CD) related to the use of these powers. This will be introduced in 2021 and further detail will be provided in our 2021 report.
- 14.53 As a result of the pandemic, the majority of oversight inspections completed between April and December 2020 were conducted with remote access to records, supplemented by interviews with key individuals involved in the application and management process. During 2020, we have seen a variety of methods being used to acquire information through the use of TEI and, where this involves new or emerging techniques, we have sought the support of the Technology Advisory Panel (TAP) in clarifying the nature of the activity to ensure that it falls within the TEI definition. Representatives from IPCO sit on a national TEI working group, to help shape guidance and assist in the development of appropriate safeguards and training material for the use of this power.
- 14.54 Our oversight has demonstrated that the use of TEI has been based on comprehensive intelligence cases and, where problems have been identified, these were associated more with the administration of the process rather than issues of legal compliance or the necessity and proportionality of the activity. Such issues have included confusion as to when a thematic warrant should be used in preference to a non-thematic warrant, uncertainty across LEAs as to the modification process, and when it is appropriate to rely on the use of a general descriptor or classification of persons included within the scope of a warrant, rather than being individually named.

Data assurance in relation to targeted equipment interference (TEI) material

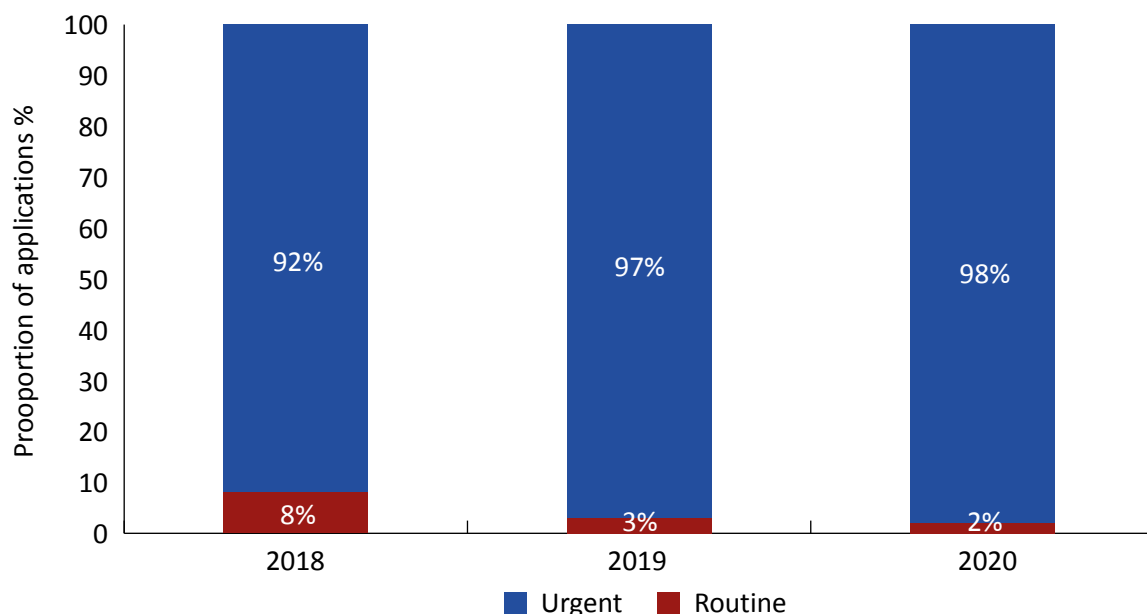
- 14.55 Some form of TEI is conducted across most forces, or within the ROCUs. TEI material is typically handled on specialist systems and equipment. In some cases, data has not been deleted since these systems were implemented. In others, although a policy of review and deletion was in place, when we tested the details we found that no review or deletion had taken place. We have reminded each force of their responsibility to ensure that these systems and equipment are handling TEI data in line with the CoP and force policies on data safeguarding. Each force is responsible for ensuring that specialist units performing acquisition or processing of TEI have the capability to securely store any material acquired. In addition, forensic, digital and analytical staff should receive training and guidance to ensure they understand the safeguarding requirements.

- 14.56 All TEI material is obtained under a warrant in which the adequacy and function of safeguards must be described. We advised that any force handling TEI material should review the safeguarding and intrusion statements in the authorisation requests in view of its understanding of the adequacy of its handling to ensure they are accurate. Forces must ensure that they comply with the safeguarding statements in the application and be aware that the reviewing JC will assess the adequacy of arrangements when considering whether or not to grant a prior approval.
- 14.57 We have seen some progress that reflects the intention to make greater use of TEI in future. Regional TEI managers are now embedded within forces and the ROCUs. There are also plans for additional training and quality assurance of TEI applications. At present, most forces are still completing TEI applications on paper rather than on a workflow or case management system. Some forces intend to upgrade their systems and processes to reduce the use of hard-drives and are considering whether cloud-based solutions may be appropriate. We have advised that an understanding of data pathways and the relevant safeguards should be central to this planning.

Targeted interception (TI)

- 14.58 There are five LEAs that are permitted to carry out interception of communications under the IPA for serious crime: the NCA, HMRC, the MPS, Police Scotland and PSNI. We inspect each of these on an annual basis. In 2020, we enhanced our inspections to take a more in-depth look at the handling arrangements in place for TI material and testing the LEAs' compliance with them. This aligns with the work described elsewhere in this chapter in relation to data assurance. Other than where errors have been reported, (see Chapter 19, Errors) we are satisfied that the procedures and systems used to handle TI material are compliant. We will continue to prioritise discussions on the application of safeguards with these authorities throughout 2021.

Figure 14.5 Percentage of urgent and routine applications by LEAs for targeted interception, 2018 to 2020



National Crime Agency (NCA)

- 14.59 The inspection of the NCA is one of our largest for TI. The NCA often has to deal with developments at pace and out-of-hours. There is good evidence to show that thematic warrants continued to be used lawfully and in line with the CoP, even in cases where the warrants were large with a high volume of modifications during the period inspected. The inspection team were satisfied that interception is being undertaken lawfully and concluded that the NCA has a good level of compliance with the IPA and its associated CoP.
- 14.60 The NCA reported an error to us in 2020 which related to an IPA safeguards compliance issue. The NCA is the intercepting agency that provides TI material to the police forces in England and Wales. The material is passed back to the forces on a secure network to trained individuals attached to the ROCUs. During late summer, the NCA became aware that one of these ROCUs was not managing the TI data in accordance with the safeguards specified in the IPA and Codes of Practice. This individual matter has been resolved but it has led to a wider review of the practices within the ROCUs for handling IPA TI material. We are continuing an investigation of this along with the NCA and expect to report the findings in our 2021 report.
- 14.61 The NCA commenced a project in 2020 assessing the value and use of extracts of TI voice samples to provide a voice attribution service. We were briefed on this as a limited scope project which will be assessed to determine further expansion and use. We will continue to monitor this and liaise with the NCA as it assesses the future for this project.

HM Revenue and Customs (HMRC)

- 14.62 HMRC demonstrated a high degree of compliance with the IPA and the CoP. HMRC carries out a wide range of investigations, some of which can be very protracted and complex, and it has invested heavily in managing safeguards relating to TI material. It has demonstrated good practice in handling potential legally privileged or other confidential material. We found HMRC has a very robust process for handling and retention of material with all applications, renewals and modifications being completed to a high standard.

Metropolitan Police Service (MPS)

- 14.63 Our inspection at the MPS showed that there was a high degree of compliance with the IPA and the CoP. Our focus was on modifications and safeguards. Authorising comments on minor modifications, which are internally approved, were detailed and very clear. The MPS wrote and implemented a Covid-19 policy at the start of the pandemic detailing how it would handle warranted data in the light of pressures on staffing arising from the pandemic. This was shared with IPCO, which we saw as good practice. The MPS has a strong compliance regime in relation to TI safeguards. It also has good policies in relation to retention and disposal of TI material. However, in common with the NCA, in certain circumstances the MPS provides TI material to other police forces in England & Wales. As discussed in paragraph 14.60 above, we are investigating the processes that the ROCUs have in place for handling IPA TI material. We expect to complete this investigation during 2021 and will provide details of our findings in our next Annual Report.

Police Scotland

- 14.64 Police Scotland demonstrated a high degree of compliance with the IPA and the CoP. Our focus was on modifications and safeguards. We found the modifications examined to be to

an acceptable standard and clearly set out necessity and proportionality. The potential for collateral intrusion in applications was well articulated and mitigations explained. Police Scotland demonstrated good compliance with safeguards for TI material and had clear policies for retention and disposal.

Police Service of Northern Ireland (PSNI)

- 14.65 In general, PSNI demonstrated a good level of compliance with the IPA and its associated Code of Practice. Necessity and proportionality cases were well made and clearly set out. We saw good use of thematic warrants and timely modifications as required. However, PSNI has an IPA compliance risk in relation to the safeguards governing how IPA and RIPA material should be handled. Two areas of risk were identified by PSNI and reported to us, in relation to warranted data from two different sources: both relate to the retention of IPA and RIPA material beyond the time that is necessary for the authorised purpose (in fact PSNI was retaining the material indefinitely).
- 14.66 These areas are now subject to mitigation and extra oversight. In 2020, we wrote to PSNI advising it should introduce a RRD process for TI product at the earliest opportunity. PSNI has been working to address these issues and has indicated that new processes are in place in relation to retention and deletion; these will satisfy the requirements of the IPA safeguards for both these sets of data. We are returning for an IPA safeguards inspection in early 2021 to check compliance.

Communications data (CD)

- 14.67 In 2020, we inspected the process in place to acquire CD within 41 police forces and two LEAs (the NCA and HMRC). While the restrictions imposed by the Covid-19 pandemic caused disruption to the CD inspection schedule, the planned cycle of 2020 inspections was completed using remote access to records and systems, supplemented by video interviews of key individuals involved in the authorisation and management of the acquisition process.
- 14.68 2020 saw the consolidation of the independent authorisation of routine applications to acquire CD by the Office for Communications Data Authorisations (OCDA: see Chapter 7). Only cases that meet strict urgency criteria, or relating to national security investigations, can now be authorised internally within LEAs. Throughout 2020, our inspections continued to focus on the articulation of necessity, proportionality and collateral intrusion issues.
- 14.69 Overall, the general standard of compliance across LEAs throughout 2020 has remained high. The safeguard of independent authorisation by OCDA is working well and the pre-submission scrutiny of applications by those LEA staff members who act as a Single Point of Contact (SPoC) provides an additional layer of protection to ensure legislative compliance and reduce the risk of errors. We have seen that authorising officers at OCDA have rejected or returned applications for additional work if the required threshold has not been reached. Across the SPoC community, we continue to see a good level of knowledge of the technology and tactics available, which allows them to advise and challenge investigators on the most appropriate method of applying CD tactics. On a few occasions, we identified authorisations that were granted by OCDA that, in our view, would have benefitted from additional detail, clarity and explanation. We have discussed these findings with OCDA and have worked with senior managers to review processes and deliver additional training to the authorising officers.

- 14.70 It remains the case that the vast majority of applications to acquire CD relate to the prevention and detection of crime, and most commonly offences concerning the unlawful supply of controlled drugs and offences concerning the sexual exploitation of children. A significant proportion of applications are also made in connection with the need to prevent death or injury, with cases involving high risk missing persons or dangerous offenders unlawfully at large usually granted using the urgency provisions.
- 14.71 In 2019, we saw a decrease in the number of reportable errors. We believe this was a result of a number of factors, including the additional scrutiny of OCDA, the professionalisation of the SPoC role, the wider use of auto-acquisition (which means data does not have to be manually transposed between systems following authorisation) and adherence by LEAs to the principles of the National Error Reduction Strategy. That situation has remained for 2020; the number of reportable errors has remained relatively static, although we have seen a slight increase in errors made by telecommunications operators (See Chapter 19 for errors).
- 14.72 Our 2019 report highlighted the difficulties (reprinted below) for both LEAs and OCDA when determining whether the acquisition of CD should be pursued under the provisions of the IPA or through a disclosure request in accordance with the Data Protection Act 2018 (DPA).

Data protection Act 2018 (DPA) vs Investigatory Powers Act 2016 (IPA)

Before the IPA, LEAs could seek certain information from online retailers under the DPA, for example if they needed data about a stolen credit card used to buy goods online, or to identify the address of a person selling stolen property on a web-based market place. The retailer could release that data under an exemption in the 1998 Act for use in preventing or detecting crime. Often, the data released included elements of CD that were inextricably linked to other account details, even though this data was not necessarily asked for or required.

The Data Retention and Investigatory Powers Act 2014 expanded the definition of 'telecommunications operator' to include companies who provide internet-based services, such as webmail and online retail.

When the IPA came in, a further major change was the creation of an offence in section 11 for knowingly or recklessly acquiring CD without lawful authority. Although it provides an important safeguard, this offence, when combined with the ambiguity and complexity of the definition of CD, poses significant challenges for public authorities.

For example, most online retailers do not understand themselves to be offering a telecommunications service and do not therefore recognise the requirement to respond to a CD notice under the IPA – instead, they often insist upon the use of the DPA. The outcome is that for what, in most cases, are relatively straightforward LEA requests for basic user information to assist in the detection of a crime, an authorisation for the CD element is required under the IPA and a request under the DPA for other personal data. It also means that a CD authorisation or notice may be sought out of an (understandable) abundance of caution (given the potential for criminal liability), even when the data is unlikely to constitute CD.

While this complies with the guidance in the CoP and Home Office advice, it creates what we believe is often an unnecessary process for the applicant, OCDA and the retailer, and appears to have created additional bureaucracy above and beyond what would have been envisaged by the safeguards introduced under the IPA.

- 14.73 These difficulties have continued and questions on what has become colloquially known as the "IPA versus DPA" issue are frequently received by both IPCO and OCDA. The most common problem arises where a telecommunication operator determines material is CD and insists on an authorisation under the IPA to disclose that information to the LEA. The LEA submits an application to OCDA to acquire the data, but OCDA refuses the application because it does not consider the material being sought falls under the IPA definition of CD. The IPC has now undertaken an in-depth review of the definition of CD and associated issues and has raised concerns with the Home Office that the definition needs to be examined as a priority during the IPA review. The IPC is concerned that the complexity and ambiguity of the definition continues to pose very real difficulties for public authorities and telecommunications operators. IPCO is working with OCDA and the Home Office to produce interim guidance for public authorities pending an update to the CD Code of Practice. However, notwithstanding any interim guidance, the IPC considers that there is a strong case for legislative change.

Internal investigations and professional standards

- 14.74 In 2019, we reported our concerns with a proportion of applications for CD by Professional Standards Units. We advised that applicants should be conversant with the Crown Prosecution Service's (CPS) advice in relation to Misconduct in a Public Office when

considering making such applications. During our 2020 inspections, we have seen little improvement. Much of the casework we have inspected has fallen short of providing a clear statement setting out the nature of the misconduct and has not made reference to those CPS guidelines in respect of clarifying the severity of the offence or included relevant material to address the points to prove. The bar for that criminal threshold is high. The fact that a public officer has acted in a way that is in breach of his or her duties, or which might expose the officer to disciplinary proceedings, is not in itself enough to constitute the offence.

- 14.75 In particular, we have seen a significant rise in the number of applications relating to what is referred to in policing as “Abuse of Position for a Sexual Purpose”. This ambiguous term does not necessarily describe a criminal offence and may be applied to a wide range of conduct which, more often than not, is likely to constitute a disciplinary matter rather than a breach of the criminal law.
- 14.76 The acquisition of CD in such circumstances can be justified if the criminal threshold is met; for example, in the case of persistent predatory sexual behaviour towards vulnerable victims of crime. We have found, however, that the severity of the misconduct typically was low and should have been assessed as not meeting the threshold. Where there was no likelihood of the officer's behaviour resulting in a criminal prosecution, CD should not have been requested.
- 14.77 The fact that an officer misconducts themselves and is a person who holds a public office does not, of itself, make out the case for a misconduct in a public office offence. The applicant must demonstrate that the alleged misconduct occurred while the officer was performing the duties of a public office holder, the misconduct related to those duties and that the misconduct was such as to seriously damage the public's trust in that office.
- 14.78 We plan to take a number of steps during 2021 to address these concerns:
- the IPC will meet with the Director of Public Prosecutions to ensure there is a common understanding of the criminal threshold of Misconduct in a Public Office;
 - IPCO will set out to the NPCC and the Independent Office of Police Conduct the minimum expectations of detail required within an application seeking to acquire CD in such cases;
 - IPCO will work with OCDA to develop relevant training to ensure its authorising officers are fully conversant with the extent of criminal threshold required in this type of investigation; and
 - IPCO will be recommending that applications to acquire CD in cases of Misconduct in a Public Office will have been reviewed by the SRO and, if necessary, a legal advisor to the public authority.

Sensitive professions

- 14.79 All CD inspections examine cases where applications have been made that are in some way connected to a sensitive profession. We continue to encourage applicants and SPoCs to think more widely as to what constitutes a sensitive profession and avoid relying on those examples listed within the CoP (lawyer, journalist, medical doctor etc) as an exhaustive list. It remains the case that most applications that are flagged as a potentially sensitive profession relate to the holder of that profession being a victim of a crime, who is often aware that CD is being acquired to corroborate their witness account. For example, where a journalist has reported being the subject of harassment, and the police will make a request to capture their CD records as evidence. Where the holder of the sensitive profession is

a suspect, in general, it is commonly found that the crime is unrelated to the conduct of the sensitive profession. For example, CD in respect of a telephone used by a solicitor may be required to corroborate relevant evidence of an alleged sexual assault or harassment offences against them.

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

- 14.80 Journalistic freedom is protected under Article 10 (freedom of expression) of the European Convention on Human Rights (ECHR) and we would expect all relevant applications to consider the necessity and proportionality of any request in that context.
- 14.81 Most applications relating to journalists fall into the sensitive profession category (as above) where a journalist has been a victim of crime. During our oversight inspections we scrutinise all applications and authorisations relating to journalists for compliance with the requirements set out in paragraphs 8.12 to 8.44 of the CoP. Under section 77 IPA, authorisations for CD seeking to identify a journalistic source require the prior approval of a JC. The JC must have consideration to the public interest in protecting a source of journalistic information.
- 14.82 The annual returns provided by public authorities indicated that LEAs had made six such applications in 2020. All of these were investigated further as part of IPCOs *ex post facto* oversight procedures and details are set out below.
- 14.83 The first case where two authorisations were granted, involved a call made to a newspaper by someone claiming to be the person responsible for making threats to kill and discharging a firearm. There is some ambiguity as to whether such a person is a source of journalistic information if they are providing information for the furtherance of a criminal purpose. While such conduct is clearly carved out from the definition of journalistic material in section 264(5) IPA, no express equivalent carve-out appears in the definition of a source of journalistic information in section 263(1) IPA. However, it is our view that a statute should not be interpreted as giving any protection to the furtherance of crime in the absence of express words to that effect and that Parliament must have intended to provide a consistent and coherent regime for the protection of journalistic freedoms. Accordingly, we consider that a similar carve-out for the furtherance of a criminal purpose should be read into the definition of a source of journalistic information in section 263(1) IPA. Accordingly, this application for CD was not to identify a journalistic source as the person's contact with the newspaper was in the furtherance of crime (i.e. to make threats to kill).
- 14.84 The second case involved a local news website. Data had been copied from the website and then used on Twitter to post malicious and grossly offensive messages. The application sought to identify the IP addresses of persons logged onto the website over a 15-minute period in order to provide a line of enquiry to identify the offender. This was another case we considered to be a cautious approach. The applicant was concerned that the information being acquired could potentially identify any journalists or sources who had been legitimately using the website at the same time. Although correct, this risk does not render the purpose of the application to identify a journalistic source and therefore did not engage the safeguard in section 77 IPA requiring JC approval. The purpose was to identify the offender publishing the malicious communication on Twitter. It should be noted in this case that the company concerned refused to disclose the data requested, claiming (erroneously in our view) that it did not meet the definition of a telecommunications operator, and so was not covered by the IPA. While this refusal could have been challenged

by the public authority, this was not pursued as a parallel line of enquiry identified that the offender was believed to be outside UK jurisdiction.

14.85 The third case related to two authorisations granted to an LEA as part of the same investigation. It concerned a public official, arrested in connection with offences under the Official Secrets Act 1989 and Misconduct in a Public Office as a result of the unlawful disclosure of protectively marked documents.

14.86 The final case concerned an application seeking to acquire CD relating to a person who claimed to be a freelance reporter who had been employed by a protest group to film/report on a demonstration during which criminal damage in excess of £10,000 had occurred. There was no suggestion that the person had been directly responsible for the criminal damage. This case was refused by the JC who believed the application failed to meet the test in section 77(6) of the IPA that requires the IPC to have regard to:

- the public interest in protecting a source of journalistic information; and
- the need for there to be another overriding public interest before a relevant public authority seeks to identify or confirm a source of journalistic information.

Data assurance in relation to communications data (CD)

14.87 A high volume of CD is used and stored by forces, relative to other powers, and yet we found that the handling of CD has the highest level of non-compliance with the statutory data handling safeguards. There are three core issues:

- systems and processes driving uncontrolled duplication and copying of CD results. Processes are often not using the potential of existing workflow and case management systems to direct applicants and analysts to one centralised, controlled environment for using and retaining CD results. Numerous users can make copies without having to record a reason and with very little oversight;
- system deficiencies preventing review and destruction. Workflow systems like Charter, CycComms and Optica are not capable of automated flagging of reviews. Some versions of CycComms and Charter now have a manual deletion capability, but this has not been rolled out and actively used in many forces; and
- unknown pathways or non-compliant handling of CD results outside the CAB/SPoC environment. Once the data has left the CAB/SPoC environment, onward pathways were not well understood. Applicants, investigators and specialist intelligence, digital media analysts across forces are not adequately supported with clear procedures that provide guidance on how to discharge this responsibility at unit or individual level.

14.88 Some SPoC units are considering their own independent RRD schedule. While this could be considered a sensible approach, it comes with considerable risk if overall the force has not yet understood the CD pathway when it leaves the SPoC environment or put adequate controls in place to ensure compliance. RRD of CD should be reviewed at a strategic level rather than an end user level, therefore ensuring that compliance is achieved overall. Resolving RRD within the SPoC/CAB environment simply creates a wider force risk of CD material being held/duplicated and moved within ungoverned spaces.

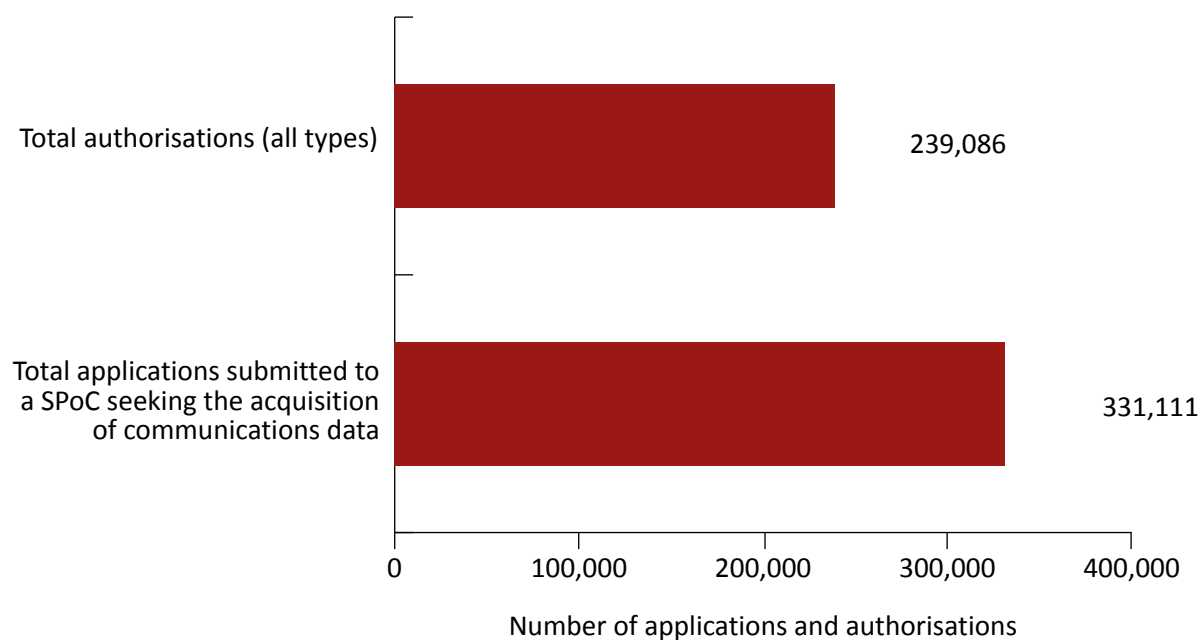
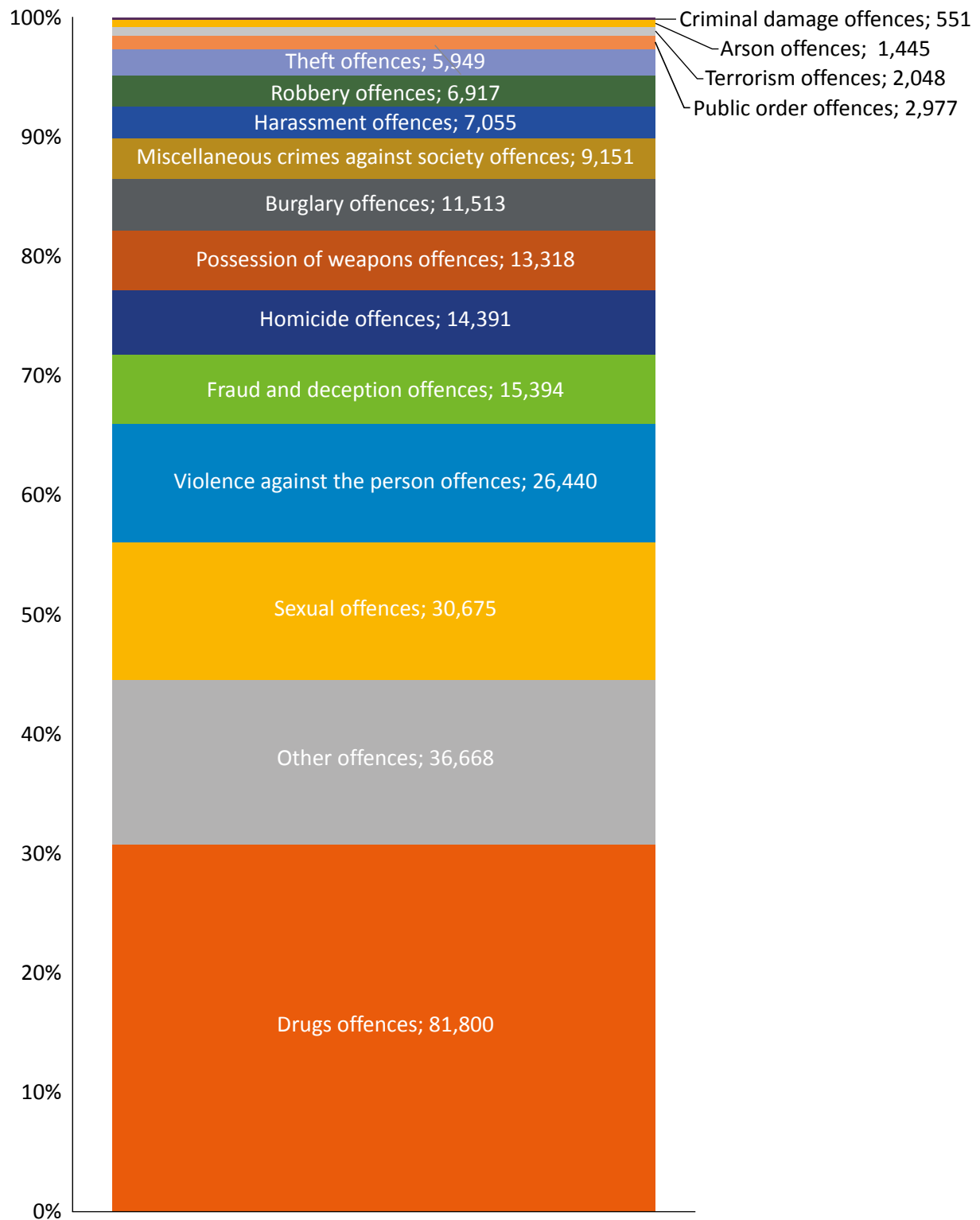
Figure 14.6 Communications data applications and authorisations, 2020

Figure 14.7 Communications data authorisations by offence, 2020

Note: The total number of authorisations shown here exceeds the figure shown in 14.6 as an authorisation may relate to more than one offence.

Overarching data assurance

14.89 This section addresses the principles and findings in relation to data assurance from a force-wide perspective. This should be read in conjunction with the notes on individual tactics set out above. We expect to see substantial progress in each area highlighted throughout 2021. Our work focuses on benchmarking compliance across all systems and processes used in relation to covert powers and once this had been completed, we set out minimum standards we would expect to see in the future:

- completed reviews of pathways resulting in clarity on pathways for all forms of covert material;
- clarity on accountability at each stage of the pathway;
- refreshed, force-wide, safeguarding policies and RRD processes;
- evidence of implementation of the refreshed process on covert material acquired since 2018 (for example, review dates set on case management systems or manual schedules implemented);
- action underway to index and schedule legacy material;
- appropriate guidance and/or training in place for all staff who have cause to handle covert material;
- safeguarding requirements factored into IT procurement, both ongoing upgrades and new procurements; and
- SROs aware of, and able to brief IPCO on, all compliance risks, having set up structures necessary to develop and implement a safeguarding plan that provides assurance about when full compliance will be achieved.

14.90 It is worth noting that some changes, such as upgrading case management systems used to house covert material, require significant financial investment in IT infrastructure and rely on action by commercial providers. This will delay implementation of automated processes, but we would expect forces to adopt manual processes and policies until technical safeguards can be implemented. Resource limitations, operational pressures and the impact of the pandemic will inevitably delay full resolution of the issues raised by the data assurance programme, but we expect to achieve a good level of confidence that data is being obtained and handled appropriately by each authority. They should demonstrate this both through the documentation of clear policies and processes and by providing on-system demonstration of compliant holdings in the future.

Findings

Accountability

14.91 We found a lack of understanding about who has overall accountability for covert material. Each CoP requires a nominated SRO, of senior rank, to be responsible for the integrity of the processes in place to acquire data/material and overall compliance. Historically, this has been a superintendent for CD, and a chief officer (Assistant Chief Constable or above) for surveillance, CHIS and property interference. This leads to confusion if they work independently, especially if data acquired through covert powers enters the wider intelligence network or becomes evidential material in criminal proceedings. Appointing an overall SRO for the management of covert material would simplify this. Collaboration *within* forces will bridge the specific legal requirements for safeguarding covert material with force-wide information management. Some forces have convened cross-force working groups to undertake safeguarding reviews and develop a safeguarding action plan; when

this approach is taken, all teams and units that handle or process covert material should be represented, alongside corporate functions responsible for wider information management and data protection.

- 14.92 Clear accountability for covert material is vital when material is moved between forces, external suppliers or regional units. There must be clarity about accountability and, for regional units, there must be agreement on which force policy should be used. We have suggested formalising accountability via a Memorandum of Understanding to ensure that everyone handling covert material, whether from the home force or regional unit, are clear on their responsibilities. Where the covert material constitutes personal data, such accountability arrangements should, of course, already be in place by virtue of the requirements of data protection legislation.

Policies and processes

- 14.93 Policy and practice vary between forces and regions; collaboration is essential for improvement in safeguarding and to ensure consistency across policing. Collaboration to assess regional challenges and scope shared solutions will help shape requirements at a national level and will inform the NPCC's role leading RRD policies from a national perspective.
- 14.94 Force policies did not generally reflect the data handling practices which were known to staff. For example, many teams we interviewed explained how material or equipment used to hold material was moved in and out of the unit, how that movement was recorded and how equipment was cleansed afterwards. But this was not documented anywhere, leaving a gap in practical guidance under force information management policies.
- 14.95 We found instances of duplicated material being held indefinitely where teams acquire covert material on behalf of others; limited reviews have meant that all duplicate copies are not accounted for. In a few forces, surveillance teams do not retain product once it has been passed on, eliminating duplication, and the Senior Investigating Officer (SIO) becomes responsible for the received product. However, some surveillance units retain all master copies of covert product acquired. They disseminate relevant copies for investigation and provide evidential and disclosure packages for court. The surveillance unit retains responsibility for the material, but adequate safeguarding relies on: (i) communication between the SIO and surveillance unit on the investigation and any judicial process; and (ii) consistent application of retention and destruction decisions across teams and systems. We did not find evidence of this best practice being applied within the forces we inspected in 2020.

Indefinite retention

- 14.96 Nearly all forces are retaining covert material without setting or tracking an appropriate retention period. Contributory factors include:
- confusion about the range of guidance and legislation, and an absence of explicit guidance on retention periods. Force policies refer to: Management of Police Information (MOPI); Applied Professional Practice (APP); the Criminal Procedure and Investigation Act (CPIA); and METSEC as well as their own Records Management or Management of Information policies but are often not clear about what should be applied in individual circumstances;
 - fragmented systems preventing the tracking and management between units;
 - lack of communication between units; and

- caution about destroying material based on previous experience and public inquiry directions. While an ongoing statutory inquiry may require retention of relevant material, it cannot be the basis for retaining all information indefinitely, without any process for review. We have advised forces to seek advice from inquiry leads when the requirement to retain data is unclear and have emphasised the need for a relevancy test to inform decisions to retain material.

Fragmented and limited systems

- 14.97 We found that a fragmented approach to technology procurement has resulted in covert material being processed and stored on a variety of systems with inconsistent or inadequate safeguarding, monitoring and review capabilities. Safeguarding and the ability to conduct effective RRD must be factored into technology upgrades and new system procurement.
- 14.98 Within each force, different systems and databases handle and store different types of data. Access is often limited to specific teams and cannot be controlled centrally. CD, surveillance, property interference material may be transferred, often manually, between multiple workflow and case management systems, as well as hard-drives and network folders. We have suggested that forces should be able to track the pathway of data through these systems to ensure that compliance is upheld at all stages, but this current fragmentation inhibits effective reviews in relation to duplication and retention safeguards.
- 14.99 We have found that there is often no automated or semi-automated method to set and track reviews across fragmented systems and devices. The few forces that have been tracking reviews are doing so by using Excel schedules that require constant resource to manage and are prone to human error.
- 14.100 Currently most forces are unable to perform any RRD of covert material for CD and CHIS held within case management systems such as Charter, Pegasus, CyComms and Optica. In the long term, we have suggested that it would be preferable for forces to procure a single data asset management system that would provide a single, secure environment for all covert material. This would allow for officers and staff to be given access to the material when operationally needed without the need for material to be duplicated or moved to other systems, and for consistent RRD automatically to be applied. In the interim, we expect forces to establish effective methods of applying RRD processes and policies which overcome the limitations of these systems and can help ensure compliant handling of relevant data.

Duplication

- 14.101 Duplication must be minimised and, if operationally necessary, accounted for. Forces will not be able to demonstrate compliance with this requirement until data pathways have been mapped in full. Fragmented systems and processes currently necessitate some duplication, but forces commonly reported unnecessary duplication, often due to cultural distrust of the workflow system. We have suggested that forces should review where and why material is unnecessarily duplicated, and conduct an exercise to minimise data holdings in reflection of the requirements of the CoP.

Access to covert material

- 14.102 Our inspections have identified that, in general, covert teams and units have good physical security regimes which go through routine penetration testing. Typically, forces use access control levels (ACLs) to restrict access to sensitive material and the CAB/SPoC manage systems access rights. However, access and access rights are not routinely audited or rescinded.

Training and guidance

- 14.103 Weaknesses in staff training, which in general did not adequately address data safeguarding, are compounded where written guidance is insufficient. Information management, systems and role-specific training for applicants and AOs, as well as wider staff who may also handle covert material, does not, other than in one or two cases, adequately cover data safeguards.

Covid-19 restrictions and changes to working patterns

- 14.104 Changes in working practices due to the pandemic have affected how data is accessed. For example, we encountered DSAs being worked on at home and an increased use of encrypted USBs in the cyber, undercover and analytical space. Where data safeguards are specifically referenced in authority wording or risk assessments, these should be updated to reflect the changes to working practices. We have suggested that the Operational Security Officer (OpSy) support should be utilised when deviating from normal working practice, and a policy log should be created to document the reasons for the changes, as well as any additional risk mitigation, training and compliance that will be implemented as a result.

15. Wider Public Authorities

Overview

- 15.1 Several other public authorities have the statutory power to use certain covert tactics. We refer to these authorities as Wider Public Authorities (WPAs) and include a full list in Annex A. The nature and extent of the powers used differs across the WPAs dependent on their functions. Several WPAs are empowered to authorise the use of directed surveillance and the acquisition of communications data (CD). Property interference and intrusive surveillance powers, which require a higher level of authorisation, are limited to a smaller number of WPAs.
- 15.2 The WPAs deploy covert tactics in support of a broad range of investigations which reflect the diverse nature of the investigative and enforcement functions they perform. Principally these are:
- investigation and prosecution of breaches of company and insolvency legislation;
 - investigation of fraudulent benefit claims;
 - tackling environmentally damaging pollution; and
 - regulation of medicines, medical devices and equipment used in healthcare.

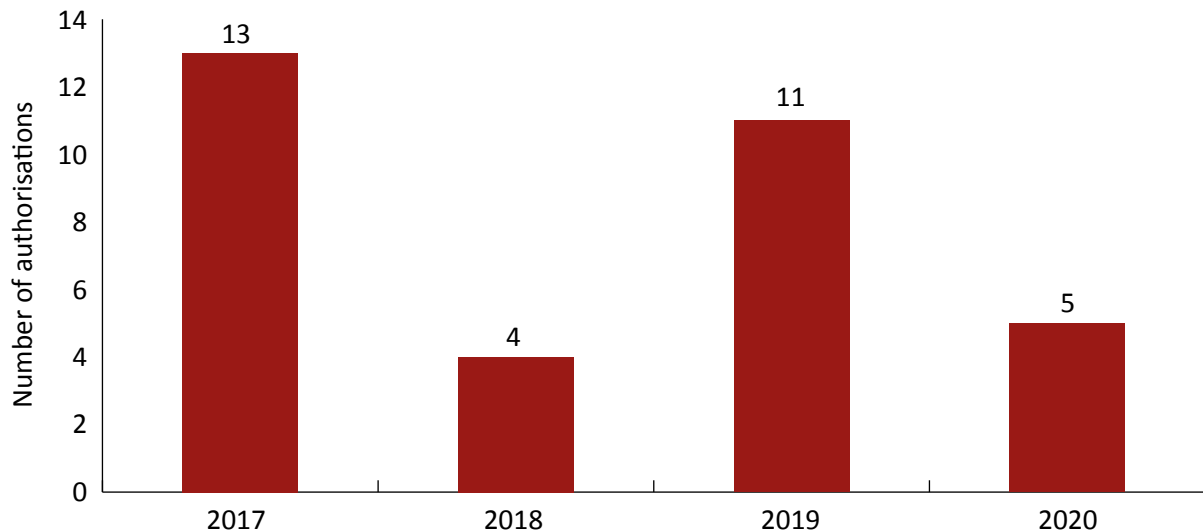
Findings

- 15.3 In 2020, we conducted 16 inspections of WPAs. Several of the 2020 inspections were conducted remotely as a result of the Covid-19 restrictions, through telephone or video meetings and the provision of documents for review.
- 15.4 In our 2019 report, we undertook to review the risk from ambiguous phrasing in WPA surveillance applications. We were concerned that this might lead to unauthorised surveillance activities inadvertently being conducted. We were pleased not to identify any vulnerabilities in this area during 2020.
- 15.5 The casework we inspected demonstrated in 2020 that WPAs use covert tactics only when available overt means of achieving their objectives have been considered or tried. We suggested, however, that necessity, proportionality and collateral intrusion considerations should be articulated to a higher standard. We believe that, in some cases, infrequent use of the powers is resulting in a lack of familiarity with the requirements for documenting considerations. In general, authorising officers who have a background in law enforcement tend to be more familiar with the human rights principles engaged by the processes under the Regulation of Investigatory Powers Act 2000 (RIPA) and will often attain higher standards of compliance than their colleagues.

Covert human intelligence sources (CHIS)

- 15.6 Many WPAs which have the statutory power to authorise CHIS, in fact choose not to exercise it, citing (among other reasons) a lack of appropriately qualified and trained staff to fulfil the roles of handler and controller, or an ability to achieve their objectives by pursuing less intrusive means.

Figure 15.1 Covert human intelligence source authorisations, 2017 to 2020



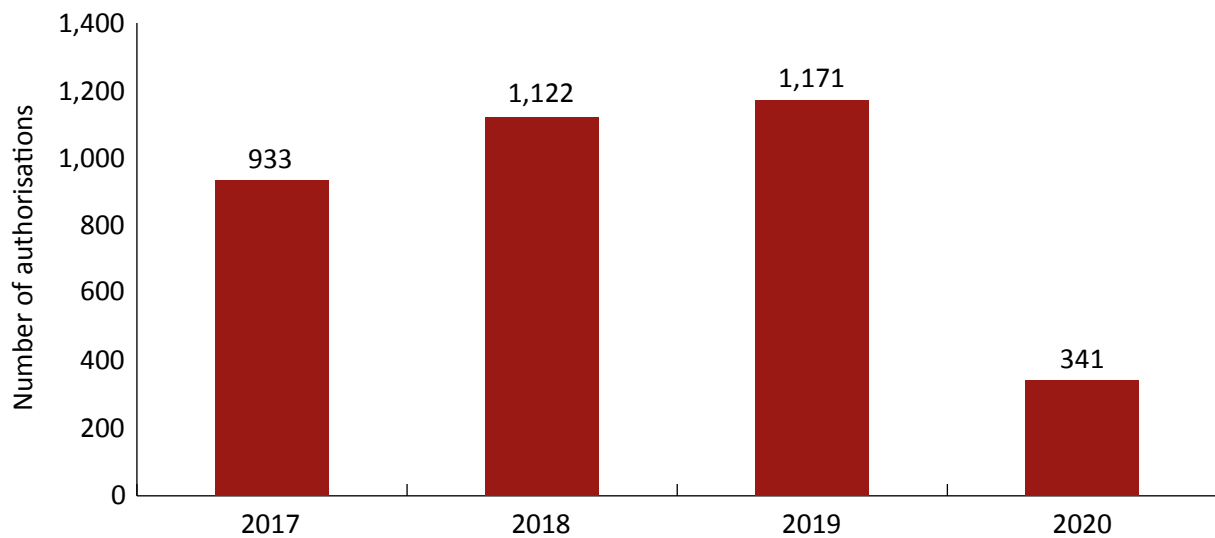
- 15.7 The Royal Mail Group (RMG) conducted three undercover deployments. One of those focused on activity outside of the Universal Service Provision,³¹ and was considered, therefore, not to be an application under RIPA. The remaining two were treated by the RMG as full RIPA applications.
- 15.8 Concentrating on the two deployments that had been deemed by the RMG to fall under the provisions of RIPA, there is a wider compliance concern. The RMG, as a public body, no longer has the power to authorise CHIS following legislative change. Paragraph 28E of Part 2 of Schedule 1 to RIPA confirms that a Universal Service Provider is a relevant authority only for the purposes of section 28 RIPA (directed surveillance). Accordingly, the RMG is not able to authorise the use of CHIS, which would include the use of undercover officers, under RIPA.
- 15.9 As set out in section 80 RIPA, and as confirmed in *C v Police and Secretary of State IPT/03/32/H*, the Act itself does not mandate that a RIPA authorisation must be in place for activity to be lawful. The Investigatory Powers Commissioner's (IPC's) functions regarding CHIS are set out in section 229(3)(e) of the Investigatory Powers Act 2016 (IPA) and state that the IPC must keep under review "the exercise of functions by virtue of Part 2 or 3 of the Regulation of Investigatory Powers Act 2000". As the RMG does not have any such functions in respect of CHIS, such activity was assessed as falling outside of IPCO's remit and therefore did not constitute a "relevant error" as defined in section 231(9)(a) of the IPA. The IPC nonetheless advised the RMG to seek its own independent legal advice as to any legal risk in undertaking covert investigative activity outside the protections afforded by RIPA.

31 The business area of the RMG in which covert activities can be authorised in accordance with the RIPA Schedule.

Covert surveillance and property interference

15.10 The level of use of directed surveillance as an investigative technique varies significantly from one WPA to another. At one end of the scale, there are WPAs who have not sought to authorise any directed surveillance activity for at least 10 years (for example, the Charity Commission and OFSTED); at the other, one organisation (the RMG) had granted in excess of 60 directed surveillance authorisations (DSAs) in 2020. Our Inspectors dip sampled authorisations to ensure that the statutory and Code of Practice (CoP) requirements were met and that the issues of necessity, proportionality and collateral intrusion have been properly considered.

Figure 15.2 Directed surveillance authorisations, 2017 to 2020



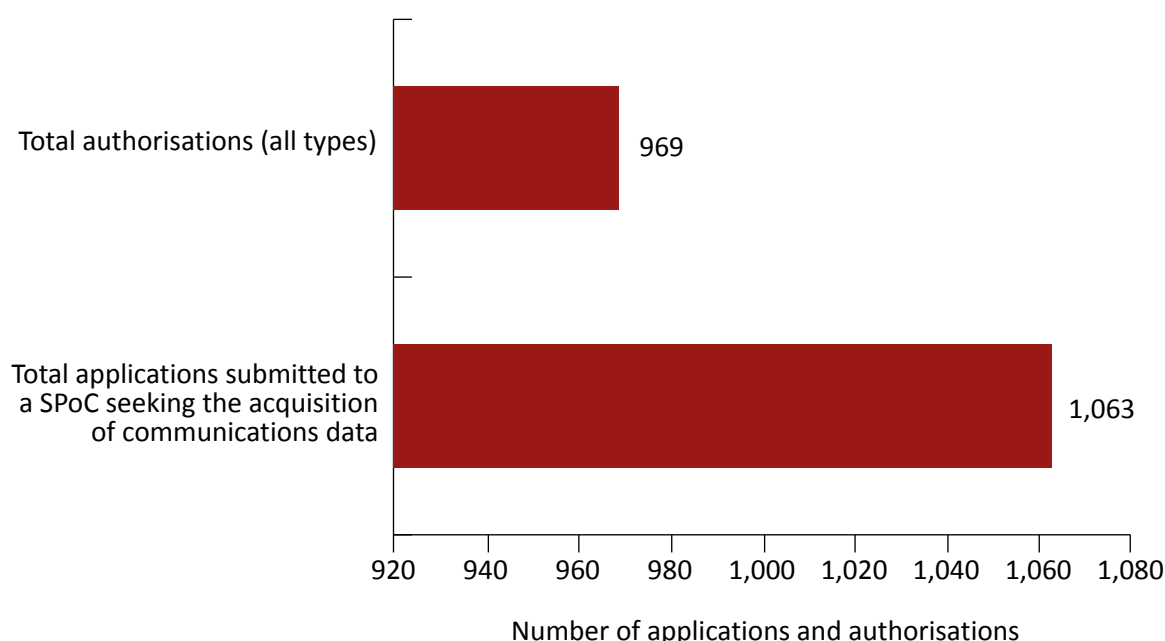
15.11 Our inspection of directed surveillance at the RMG found that both applicants and authorising officers (AOs) were confused when completing reviews and renewals. We reminded applicants that a review simply informs the AO what has happened since the activity was last authorised, reviewed or renewed. A renewal, however, should be treated as a standalone document and should provide a comprehensive overview. The AO must consider on the basis of the information in the renewal application whether it is necessary for the authorisation to continue for the purpose for which it was given. There were several examples in review documents where applicants had simply 'cut and pasted' surveillance logs into the body of the form as an update and where renewal applications contained limited information. A 'cut and paste' approach by AOs was evident in reviews and renewal authorisations. We made a recommendation that applicants and AOs should address the purpose and requirements of reviews and renewals and signposted them to guidance within Chapters 4 and 5 of the Covert Surveillance and Property Interference CoP.

15.12 Examples of good practice were often seen on inspections and one WPA (the Environment Agency) was praised for good standards noted within the DSAs reviewed by the Inspector. This included detailed articulation of the statutory considerations of necessity, proportionality and collateral intrusion. We were encouraged to find that several applications were submitted but not deemed suitable for authorisation, which leads us to conclude that the AOs were being stringent in their considerations.

15.13 In 2020, there were no applications made for property interference or intrusive surveillance.

Communications data (CD)

- 15.14 Our 2020 CD inspections of the WPAs were disrupted as a result of the pandemic, with only six inspections completed compared to 13 in 2019. Most of the inspections that took place were conducted remotely. Of the WPAs inspected, most had used their powers to acquire CD in some capacity to fulfil their regulatory or oversight functions. However, it is apparent that the pandemic has resulted in what is a generally low use of CD powers by these public authorities being reduced further.
- 15.15 All WPAs must apply to the Office for Communications Data Authorisations (ODCA) for authority to acquire CD. While a smaller number can still call on internal authorisation in cases of urgency, we rarely see this option being exercised (only three urgent authorisations were made in 2020). The statutory purposes for which a WPA can acquire CD are tailored to its regulatory functions and, as a result, are limited in number in comparison to those that can be relied on by police and law enforcement agencies.
- 15.16 A number of these authorities retain their own internal CD Single Point of Contact (SPoC) officers while others utilise the services of the National Anti-Fraud Network (NAFN). As discussed in Chapter 16 (Local Authorities), in our view, the NAFN offers an effective and efficient alternative to internal units, while maintaining good standards of compliance and offering additional resilience and expertise that would be difficult to maintain using small standalone units.
- 15.17 Despite the low volume use, our inspections of CD acquired by WPAs identified a generally good standard of compliance. From the records we sampled, we were satisfied overall that the documentation justified the principles of necessity, proportionality and collateral intrusion and provided a sufficient outline of what can, in many cases, be quite complex investigations. We made a small number of recommendations, most of which related to administrative procedures.
- 15.18 It is our intention to conduct preliminary inspections in 2021 of the five additional authorities that were added to the IPA schedule in 2020, namely: UK National Authority for Counter Eavesdropping; the Pensions Regulator; the Insolvency Service; the Civil Nuclear Constabulary; and the Environment Agency.

Figure 15.3 Communications data applications and authorisations, 2020

Data assurance

- 15.19 As we have noted elsewhere in this report, we are currently engaged in a data assurance programme which aims to investigate and embed principles of data safeguarding in the authorities we oversee. While we have not conducted standalone data assurance inspections of WPAs, we have discussed and recommended good practice during our inspections.

Training and oversight for non-users of powers

- 15.20 Training and guidance are a focus of our inspections of infrequent and non-users of covert powers. As well as general RIPA awareness, we advise that all staff should be trained on the use of the internet to guard against inadvertent drift into activity that could constitute directed surveillance. The existence of a regular training programme should assist to develop good levels of knowledge and maintain compliance with the legislation, particularly within organisations that do not frequently use covert powers. There is also a need to maintain a minimum level of competence within an organisation; this ensures that, if there is an increase in the use of covert techniques, WPA staff are aware of the necessary statutory considerations they are required to address.
- 15.21 Several WPAs take a positive view of training as a safeguard to avoid inadvertent RIPA activity. As an example of good practice, Natural Resources Wales scheduled a series of training inputs for practitioners. When that was put on hold due to the Covid-19 restrictions, several covert practitioner workshops were organised to discuss the potential use of covert activity, to educate staff on legislative matters and to develop 'tabletop' training scenarios. However, we were disappointed that our previous observation, identifying a need for the Senior Responsible Officer to undertake RIPA training, had not been addressed; this is now a formal recommendation.

16. Local Authorities

Overview

- 16.1 Local authorities may only authorise the use of directed surveillance, covert human intelligence sources (CHIS) or the acquisition of communications data (CD). In England and Wales, once a request for directed surveillance or CHIS has been considered and agreed by a nominated authorising officer (AO), it requires the approval of a magistrate. In Scotland, judicial approval is not required for such powers. The acquisition of CD must be authorised by the Office for Communications Data Authorisations (OCDA).
- 16.2 Due to the Covid-19 pandemic, it was necessary to adapt our inspection methodology to minimise physical visits where possible. We have found remote inspections to be a productive way of maintaining oversight in most cases; where we were not able fully to review the relevant documents, we have planned to do a site visit in 2021.
- 16.3 Applications for CD (which are now governed by the Investigatory Powers Act 2016 (IPA)) are made via the National Anti-Fraud Network (NAFN). The NAFN ensures that applications for CD meet the required standards and enable consistency across local government. As highlighted in our 2019 report, we inspect the adequacy of data retention safeguards, which place an obligation on all authorities to ensure that any data retained following the use of investigatory powers is stored properly. This includes copies of CD material acquired via the NAFN and retained locally on council computer systems and files.

Findings

- 16.4 Local authorities continue to be low users of investigatory powers. In part, this is due to reliance on the use of overt enforcement tactics and in 2020, numbers may have been affected further by the diversion of local authority resources to dealing with the Covid-19 pandemic. However, it is not always possible to obtain evidence using overt methods and, as such, the enduring availability of covert tactics, such as surveillance and CHIS, remains important.
- 16.5 We continue to encounter an increasing number of partnership arrangements between neighbouring councils for countering fraud. For example, a single Counter Fraud Unit (CFU) undertakes a wide range of enforcement and investigation work on behalf of the following five councils in the south west of England: Cheltenham and Tewkesbury Borough Councils; and Cotswold, Forest of Dean and West Oxfordshire District Councils. The CFU is also responsible for the management and oversight of any covert investigatory powers exercised under the Regulation of Investigatory Powers Act 2000 (RIPA) and the IPA by these five local authorities.
- 16.6 It is entirely understandable why resource-stretched councils should seek innovative ways of sharing these investigative and enforcement functions. We support this approach, provided that the Elected Members of each local authority still review the authority's use

of the powers and set the policy at least annually in accordance with paragraph 4.47 of the 2018 Covert Surveillance and Property Interference Code of Practice. Inspectors have identified that, where collaboration agreements are in force, compliance standards are generally strengthened as specialist staff increase their knowledge and awareness of the relevant legislation.

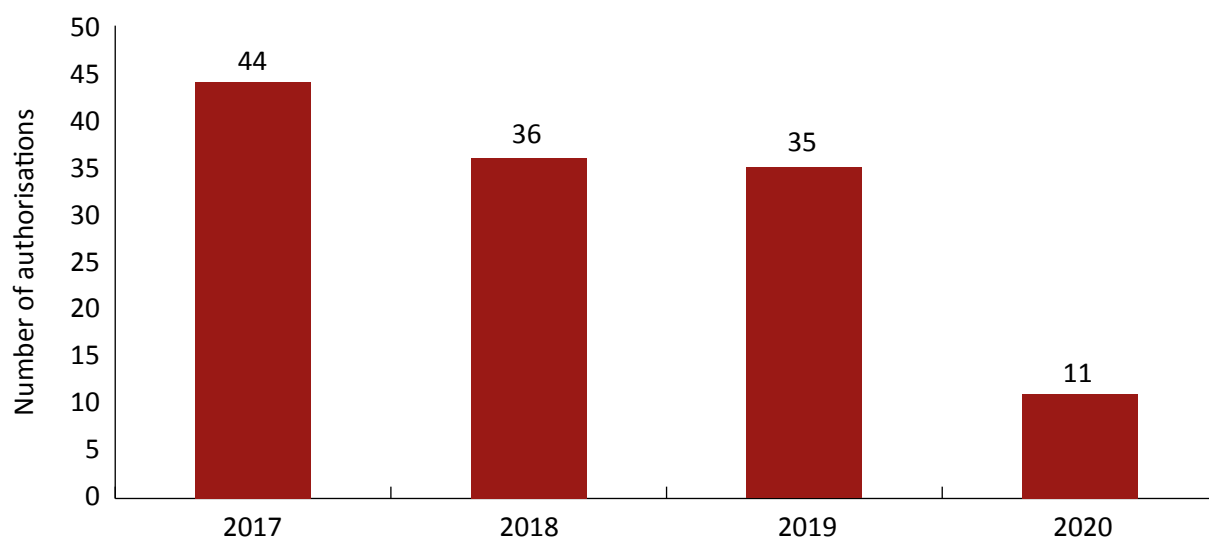
Covert human intelligence sources (CHIS)

16.7 It remains unusual for councils to resort to the use of a CHIS. In the rare case an authorisation is sought, it is often to facilitate more complex test purchase activity.

Example: test purchase activity

The use of a CHIS may be necessary where it is likely that prolonged correspondence or interaction with a seller is required to secure the sale of dangerous or prohibited items. This type of activity is often undertaken by Trading Standards or in partnership with Neighbourhood Policing Teams utilising police authorisation processes.

Figure 16.1 Covert human intelligence source authorisations, 2017 to 2020



Internet and social media

16.8 In our 2019 report, we noted the continuing growth of local authority use of the internet and social media to engage with their communities. Privacy International, an organisation which seeks to protect the right to privacy for all, has continued to engage with us on this topic, highlighting its concerns about the effectiveness of this form of surveillance on decision making. In 2020, it suggested that the Investigatory Powers Commissioner's Office (IPCO) should publish a series of guidelines on a range of issues,³² including:

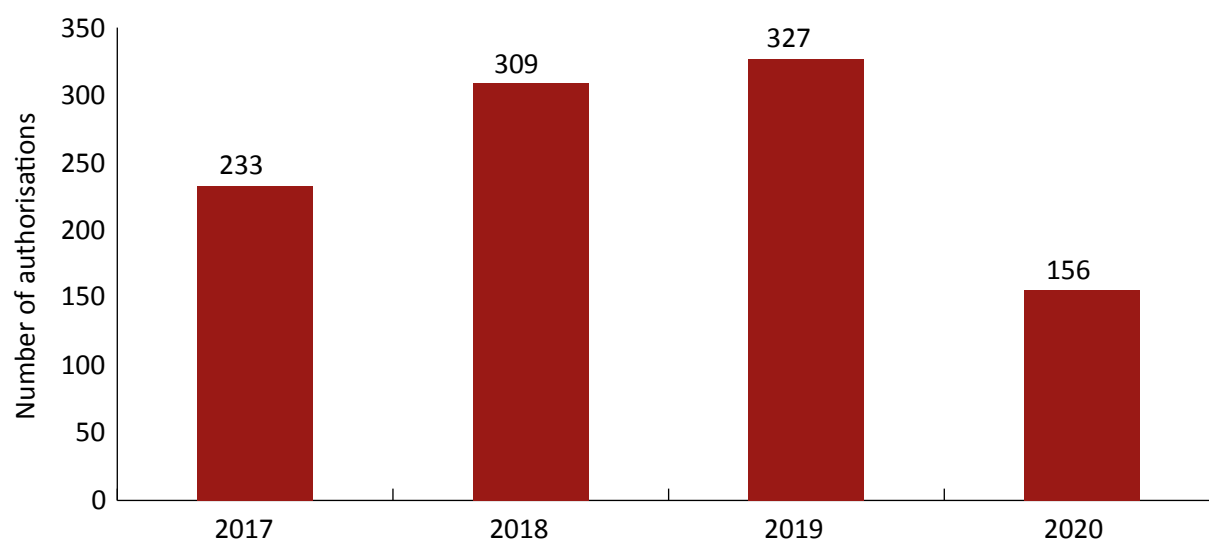
- how local authorities can assess what constitutes a legitimate aim for local authorities to rely on in order to conduct overt social media monitoring;
- in what circumstances overt social media monitoring is just and proportionate; and

32 See: www.privacyinternational.org/report/3584/when-local-authorities-arent-your-friends

- whether repeated or persistent viewing constitutes directed surveillance.
- 16.9 Our response highlighted that the first two recommendations fall outside the Investigatory Powers Commissioner's (IPC's) remit, as the overt use of social media monitoring involves the processing of personal data. It is therefore subject to regulation by data protection legislation, which is overseen by the Information Commissioner's Office. In relation to the third point, this guidance, which includes illustrative examples, is already provided by the CoP issued by the Home Office. Our Inspectors will continue to recommend that a council's RIPA policy is updated to signpost the reader to the relevant sections of the CoP.
- 16.10 Most local authorities provide training to their staff on the use of the internet and social media. The majority rely on training courses delivered by well-established companies, but some councils have developed their own in-house training to great success. Southend-on-Sea Borough Council, for example, has designed an IT-hosted RIPA questionnaire designed for use by all members of staff. The questionnaire is user friendly, contains relevant information and appears to be pitched at an appropriate level.
- 16.11 In addition to regular training, it is important that guidance on the use of the internet and social media is readily accessible on the council's intranet; this information should also be subject to regular review to ensure its accuracy and currency. Although the staff engaged in either investigative or enforcement roles often demonstrate a good understanding of the circumstances when an authorisation should be considered, inspections have regularly recommended that procedures are strengthened to ensure that all online activity is recorded and periodically scrutinised for oversight purposes. In the absence of such an audit trail, it is difficult for the councils' Senior Responsible Officers (who are responsible for the integrity of the process in place) to have the necessary reassurance that the internet is being used in a controlled and well understood manner.

Surveillance

- 16.12 The use of more conventional surveillance tactics, such as the deployment of covert cameras, continues to be an effective method of obtaining evidence of offences such as fly tipping. There is a noticeable trend towards investigations into circumstances where the mass disposal of dangerous and environmentally harmful waste is taking place on private land in an unsafe and unregulated manner; this may be in part due to the rising cost of commercial and domestic waste disposal.

Figure 16.2 Directed surveillance authorisations, 2017 to 2020

- 16.13 Surveillance tactics are also used to prevent fraud arising from the sale of council owned properties under the Right to Buy scheme. Where it is suspected that a proposed buyer has not met the qualifying criteria, for example because they are not residing at the address in question, surveillance can be a helpful method of proving their occupation or otherwise. In more rare circumstances, councils sometimes use surveillance to investigate and detect fraud by its own members of staff.
- 16.14 The most common compliance recommendations made by our Inspectors involve the requirement to update policies (for example, to reflect updated CoP or good practice) and the need to maintain RIPA training. The latter is especially critical to ensuring that inadvertent directed surveillance does not take place, for example through the repeated examination and use of information found on social media. It is understandable that some training and awareness-raising activity has been paused during 2020 while local government adapted to the demands of providing services during the pandemic. We have taken a pragmatic approach during this period and will encourage such activity to recommence once a degree of normalcy is regained. Given the infrequency with which investigatory powers are used, it is critical that training for AOs and other key personnel is maintained in the long term.

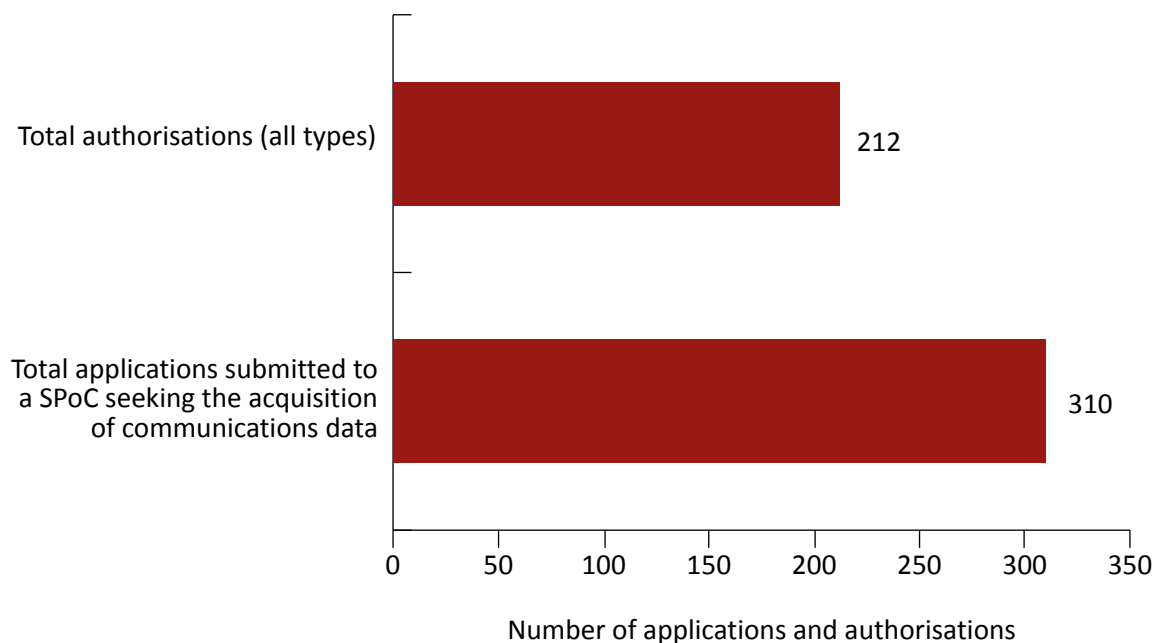
Communications data (CD)

- 16.15 We reported in 2019 that, following the introduction of the IPA, local authorities now acquire CD through the independent authorisation by OCDA (see Chapters 7 and 8). The transition to OCDA has been successful, providing independent authorisation via a more efficient service than the need to seek the prior validation by a magistrate. Local authorities can also acquire events data, for example call billing or cellular location details, if the appropriate thresholds are met. Previously, local authorities were restricted to acquiring entity data, such as to identify the user of a telephone. However, local authorities can only rely upon the statutory purpose of 'applicable crime' and cannot make an application that requires the processing of internet connection records.
- 16.16 Unlike other public authorities, local authorities seeking to acquire CD must use the services of the NAFN, which acts as a centralised Single Point of Contact (SPoC) service. The NAFN will quality assure an application to address any omissions or failings before

submitting the application to OCDA. If the authorisation is granted by OCDA, the NAFN SPoC will acquire the CD from the relevant telecommunications provider and forward the data to the applicant from the requesting authority. Although there are currently 356 local authorities registered with the NAFN, only 72 sought to acquire CD during 2020. It was envisaged that the expansion of datasets available to councils would see a rise in the use of CD by local authorities but, to date (possibly related to the pandemic), this has not been the case.

- 16.17 The disparity that now exists between the process for local authorities to acquire CD and that for the use of surveillance and CHIS, is glaringly apparent. While the use of the NAFN negates the need for the training and continuous professional development of specialist officers within each authority to maintain their proficiency and competence, it provides an effective and efficient general training and awareness programme to local authority staff, as well as offering an effective and efficient means for us to bring about a national consistency of approach. We note that no similar function exists for the other powers that are covered by RIPA. This is something the IPC will consider further and may discuss with the Home Office as appropriate.
- 16.18 The compulsory requirement to use centralised SPoC services means that we can inspect all applications and authorisations for local authorities through a single inspection at the NAFN. We found the remote access, necessary for audit and review purposes, particularly useful to enable continued oversight through the pandemic. The NAFN processed 212 applications during 2020 and 195 of those were examined as part of the 2020 inspection. Overall, we found applications were completed to a very good standard. The acquisition of entity data (for a single entity which is the subject of the investigation) carries minimal (if any) risk of obtaining unrelated private information, whereas the risk of such collateral intrusion when seeking events data is higher. Understandably, given that this was the first year of acquiring events data, we made a recommendation for local authorities to provide a more detailed explanation of that risk and the steps taken to minimise such intrusion within applications. Our inspections will assess the progress made in this regard during 2021.

Figure 16.3 Communications data applications and authorisations, 2020



Data assurance

- 16.19 From 2020, our inspections have also addressed the adequacy of data retention safeguards at individual councils, noting that the IPA and the CoP place an obligation on all authorities to ensure that any data they retain is stored properly and subject to a review, retention and disposal (RRD) process. All local authorities have received a letter from the IPC reminding them of their obligations to safeguard data obtained under their powers. Those authorities which have not exercised their powers since the updated CoP for investigatory powers were published in 2018, have been reminded of their obligations to safeguard data in the event that they do exercise the powers in future. A local authority which has been an “active user” of the powers since 2018 is required to provide its safeguarding policy (or relevant extracts) during our inspection and is tested on its implementation of this policy during the discussions.
- 16.20 Inspections have identified that, where there is a retention and disposal period specified, it is usually a ‘minimum retention period.’ There is little evidence to suggest that councils are proactively considering the necessity of retaining RIPA or IPA material and disposing of that material as soon as it is no longer needed for the authorised purpose or when there are no legal proceedings. This is an area that will receive greater scrutiny during 2021 and councils will be expected to demonstrate that sufficient progress is being made to secure compliance with the Acts and the CoP.

17. Prisons

Overview

- 17.1 We inspect individual prisons as well as Her Majesty's Prison and Probation Service (HMPPS), the Northern Ireland Prison Service (NIPS) and the Scottish Prison Service (SPS). Our oversight responsibilities for prisons are different to the other authorities we oversee as they are governed by different rules and legislation. In England and Wales, the interception of prisoners' communications (telephone calls and mail) is governed by the Prison Rules 1999 (as amended), the Young Offender Institution (YOI) Rules 2000 and the Secure Training Centre Rules 1998, which are made under the Prison Act 1952. Scottish Prisons use the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and prisons in Northern Ireland are governed by the Northern Ireland Prisons Act 1953.
- 17.2 Our continued engagement with HMPPS has been critical to establishing and maintaining compliance across England and Wales. A series of meetings have been held between the Investigatory Powers Commissioner (IPC), the Chief Executive Officer of HMPPS, Dr Jo Farrar, and her team. These meetings have provided the opportunity for debate about the proper use of interception in prisons within the context of the ongoing challenges across the prison estate in England and Wales. Dr Farrar provided reassurance that the required measures were being implemented with the appropriate strategic support and we will continue to keep this under close review.
- 17.3 In the early stages of the pandemic, on-site prison inspections were suspended to allow prisons to focus on the safety and welfare of prisoners and staff. We worked, however, with HMPPS to develop a means of maintaining oversight through the remote examination of records and video interviews with staff involved in the authorisation and management of the interception process. While we had intended to conduct 140 inspections in 2020, we were only able to carry out 15 inspections before the Covid-19 restrictions came into force, and no on-site inspections were conducted between April and December. Oversight of covert human intelligence sources (CHIS) and surveillance activity forms part of the annual inspection of HMPPS and, despite the impact of the pandemic, a full inspection was carried out using a combination of both remote access and physical attendance at HMPPS headquarters.

Scottish Prison Service

- 17.4 In 2019, we implemented a prison inspection regime of the SPS to assess compliance with the legislation and procedures governing the use of interception of communications under the provisions of the Investigatory Powers Act 2016 (IPA), the Prisons (Scotland) Act 1989, the Prisons and Young Offender Institutions (Scotland) Rules 2011 and the Scottish Prison Rules (Telephones) Direction 2011.

- 17.5 As we set out in our 2019 report, a programme of inspection for all 15 Scottish prisons began in October 2019 and was concluded in February 2020. As a result of the pandemic no further inspections of Scottish prisons took place between April and December 2020. These will therefore be a focus for 2021, once travel and social distancing restrictions allow.

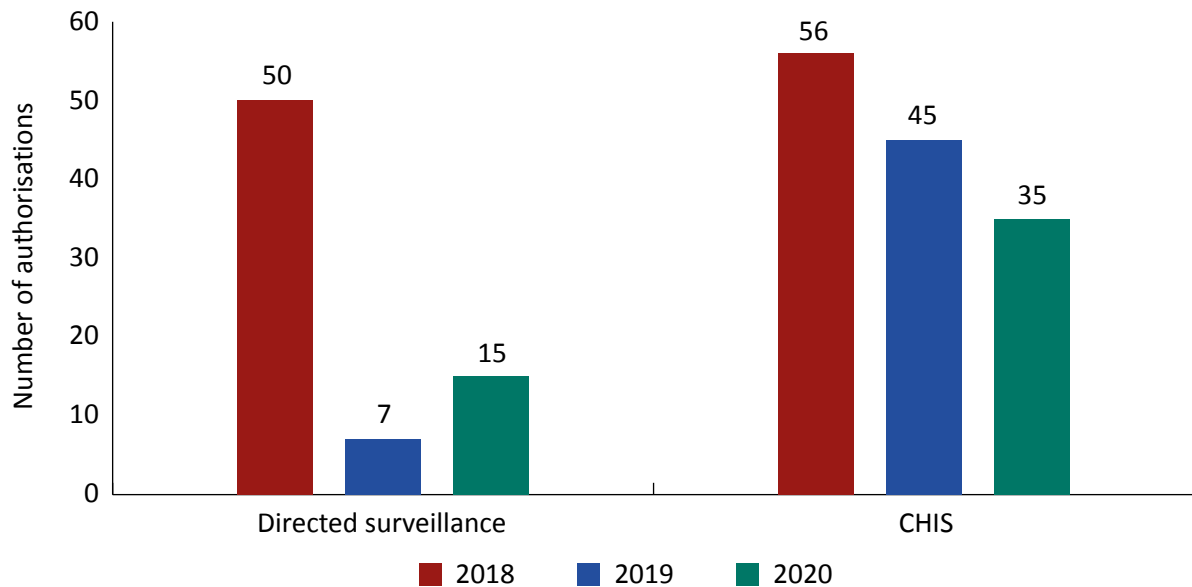
Findings

- 17.6 In our 2019 report, we noted the decline in the use of directed surveillance and the increase in England and Wales of the use of Prison Rule 50A and YOI Rule 54, which allows for the overt monitoring of prisoners using CCTV. In our inspections this year, we have seen this trend continue and, as a result, have recommended a full review of its use across HMPPS.
- 17.7 While the arrangements in respect to the interception of communications are compliant with the rules in general, we found that in some cases the demand for monitoring, particularly with the increase of in-cell phones, far exceeds the available resource. This can have a direct impact on operational practices. This continues to be a concern for us (see paragraph 17.20) and we will continue to work with HMPPS to address this.

Covert human intelligence sources (CHIS) and surveillance

- 17.8 In our 2019 report, we detailed a number of frustrations that contributed to poor compliance levels and a perceived lack of progress. This included an antiquated authorisation management process, outdated policy and Prison Service Instruction (PSI) guidance documents and a lack of operational competence for authorising officers. The continued delay in the development of a regional structure was becoming even more of an issue as it was seen as a key factor in compliance improvement. The consequence of this was that several recommendations and observations from our HMPPS inspection remained unresolved.
- 17.9 It is pleasing to report that the proposed regional structure has now significantly advanced and recruitment of staff is almost complete. The regional units will provide professional applicants with a more consistent approach to the use of covert activity. Trained regional authorising officers should also result in an improvement in authorisations and compliance. An overarching 'Policy Framework', supported by several individual 'Operational Guidance' documents, has now been endorsed and approved by the organisation's Operational Policy sub-board. The search for a commercial IT software management system has not been successful, largely due to technical challenges and, as an interim measure, an internal electronic system has been developed. This, together with a better resourced Central Authorities Bureau (CAB), has enabled tighter control and management of authorisations.
- 17.10 We have seen little change in number of authorisations for the use of CHIS powers and fluctuations in the low numbers of directed surveillance authorisations (DSAs) between 2018 and 2020 which we believe reflect the appropriate use of those powers. The use of Prison Rule 50A and YOI Rule 54, rather than a DSA, continues to be a concern and we have again recommended a full review of its use across the organisation to ensure that unauthorised activity is not taking place.

Figure 17.1 Covert human intelligence sources and directed surveillance activity at Her Majesty's Prison and Probation Service, the Scottish Prison Service and the Northern Ireland Prison Service, 2018 to 2020



- 17.11 The number of HMPPS authorised CHIS continues to be manageable but there is still variance across the different parts of the estate as to appropriate application, handling and management processes. We will further explore this issue during our upcoming thematic inspections. HMPPS also continue to work closely with its partners on the awareness and management of CHIS used by prisons by other agencies. As joint Chair of the Prison Source Working Group, it is well placed to ensure the unique risks associated with the management of CHIS in prisons are properly understood.
- 17.12 We have seen several other innovative developments that will also contribute to the improvement in compliance, including the professionalised approach to the management of technical surveillance equipment. We will review the success of these measures at future inspections.

CHIS in Scottish Prisons

- 17.13 The strong partnership between Police Scotland and the SPS continues to deliver high levels of compliance in the management of CHIS in prisons, despite the significant reduction in authorised CHIS due to the pandemic. Management of CHIS across the prison estate falls to the Police Scotland Prison Source Handling Unit, oversight of which is captured during our inspection of Police Scotland.

Interception

- 17.14 Powers for prisons to carry out interception are provided under section 49 IPA and in the Prison Rules 1999, the YOI Rules 2000 and the Secure Training Centre Rules 1998. We usually oversee the security measures, safeguards and arrangements in place by conducting a revolving programme of inspection visits, but these were suspended in 2020 due to the pandemic. Nonetheless, we continued to work with HMPPS to discuss key areas of oversight and to ensure that policies brought in response to the challenges of the pandemic were compliant.

- 17.15 The ability for prisoners to make phone calls, send emails or write letters is important to maintain family connections and to access channels of help and support. As a result of the pandemic, physical visits to prisoners had to be suspended and were replaced by video calls, a procedure known as “secure social video calls”.

Definition: secure social video calls

Secure social video calls are video calls used in prisons to enable prisoners to maintain family connections when physical visits are suspended. They are categorised as a “communication” so any monitoring of these calls requires an authorisation to be granted under the Prison Rules and is subject to oversight by the Investigatory Powers Commissioner's Office (IPCO).

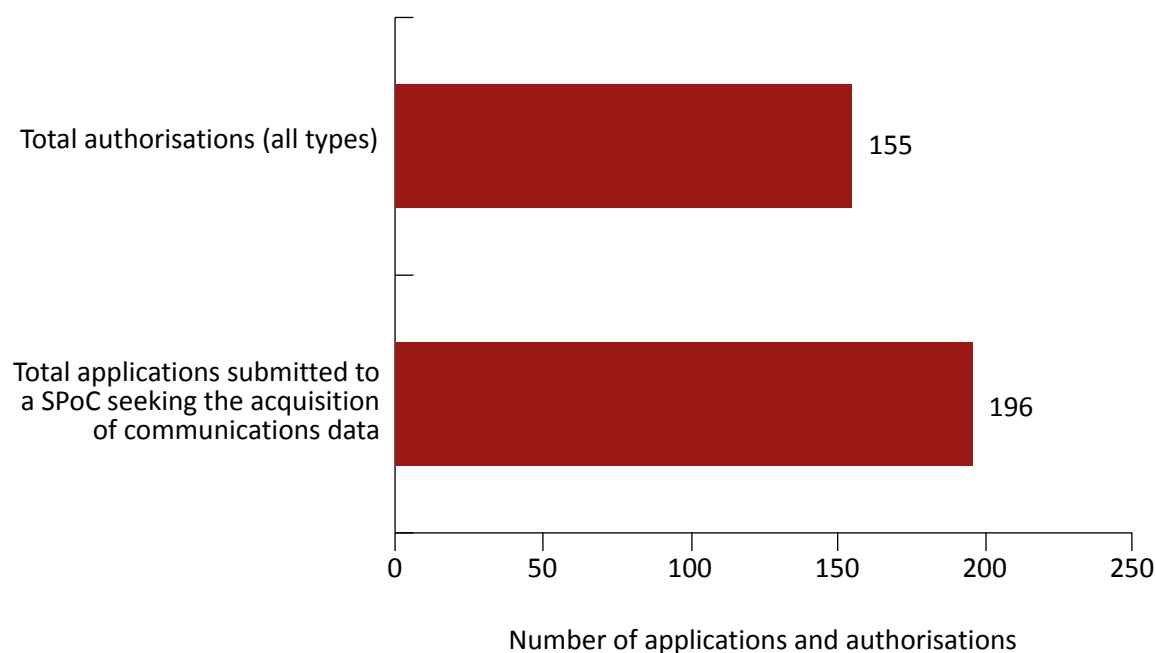
- 17.16 The arrangements for the interception of communications in prisons exist to prevent inappropriate use of telephones and letters to, for example, harass victims or witnesses or facilitate criminal conduct. There a number of grounds under Prison Rule 35A(4) and YOI Rule 11(4), for which prison governors may authorise the monitoring of telephone calls and/or correspondence, for example the prevention and detection of crime, national security, or where public protection concerns exist. Monitoring is authorised by a senior manager and must regularly be reviewed to ensure its continuing appropriateness.
- 17.17 Prisoners' communications with their lawyers, Members of Parliament (MPs) and several other organisations are 'privileged' or confidential and should not be read or listened to, other than in the most exceptional circumstances. Although the relevant legislation prohibits the deliberate interception of such communications, the applicable safeguards for the handling of the inadvertent interception of such material only feature in the relevant Prison Service Instruction (which is a policy document) and therefore not subject to parliamentary scrutiny. This also means that, unlike interception under a warrant, there is no statutory obligation to notify and seek authorisation from a Judicial Commissioner in respect of such privileged or confidential material obtained from interception under the Prison Rules. A key element of all inspections is a review of the safeguards in place to maintain the privacy of such calls. For 2020, as with other covert powers, our focus has also been directed towards the retention, review and subsequent deletion of records and material obtained as a result of prison interception.
- 17.18 Overall, the arrangements we saw for the monitoring of communications are in accordance with Prison Rules, the YOI Rules, the Secure Training Centre Rules and PSI 04/2016. There is a generally consistent approach to ensuring prisoners are informed that their communications may be subject to interception, with suitable measures in place to configure the PIN phone systems³³ to ensure that legal and certain confidential calls from prisoners are not recorded or listened to. As was the case in 2019, several examples were identified where the authorising senior manager failed to record sufficient consideration as to why the monitoring was deemed necessary and proportionate, or why the decision had been made to continue or discontinue monitoring. If supporting evidence/intelligence had been considered during the senior manager's assessment, this was not always readily accessible or recorded within the authorisation. IPCO will work with the prisons and HMPPS during 2021 to improve this situation.

33 A PIN phone system allows a prisoner to use a Personal Identification Number (PIN) to make restricted calls to an approved telephone list only. All calls are recorded and stored for 90 days, except for those entered on the system as legal or confidential.

- 17.19 Where prisons have adopted a fully electronic process for their approval and monitoring processes, these were found to be more compliant than those that still relied on paper procedures. We have therefore continued to recommend (as we did in 2019) that all prisons progress to a fully electronic system with centrally shared access to relevant documentation for all personnel involved in the interception process.
- 17.20 The most common finding from our inspections of prisons is that the requirement for monitoring, particularly with the increase of in-cell phones, results in a demand that far exceeds the available resource. In some cases, this means that authorised monitoring either does not take place, is undertaken sporadically with insufficient detail, or is completed with significant delay to the expected timescales. All of this undermines the case of necessity and proportionality of any authorisation granted, as well as the effectiveness of the call monitoring process. We have repeated our advice that, with limited resource, it is crucial that senior managers take a more targeted intelligence-led approach and review the need for continuous monitoring more regularly. We are also hopeful that a review of PSI 04/2016, which is due to take place in 2021, will simplify and consolidate the prison interception regime, giving senior managers flexibility to adopt a more targeted approach.
- 17.21 It remains our view that the arrangements within prisons within England and Wales, where the reliance is upon the prisoner to inform the recipient of a telephone call that their discussion is being recorded and may be monitored, is not satisfactory. We will continue to work with HMPPS through 2021 to explore the use of a recorded announcement that would remove the responsibility from the prisoner and provide an option for the recipient to consent. This would also reduce the risk of legal and certain confidential calls (e.g. to medical professionals) being recorded in error.

Communications data

- 17.22 The acquisition and disclosure of communications data (CD) is limited to HMPPS Headquarters and is primarily sought for internal investigations such as misconduct in a public office, offences under the Offender Management Act 2007, or theft and supply of illicit drugs. All requests for CD made by individual prisons are processed by the central Single Point of Contact (SPoC) Unit within HMPPS. Unless a case meets the urgency criteria, all applications for CD are considered independently by the Office for Communications Data (OCDA) and we are satisfied that the applications being made are necessary and proportionate.

Figure 17.2 Communications data applications and authorisations, 2020

Data assurance

- 17.23 To date, we have not conducted a meaningful review of data safeguarding across the prisons we oversee. This results in part from the restrictions that the pandemic has placed on our resources, but also from the risk-based approach that has led us to prioritise higher-volume users of covert powers. We have engaged with HMPPS to initiate a centrally-driven review of policies and procedures and we expect to dedicate more resources to inspecting the adequacy of data holdings across the prisons estate from 2021.

18. Warrant Granting Departments

Overview

- 18.1 We continue to oversee the pre-authorisation challenge function provided by the Secretary of State and through the Warrant Granting Departments (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. 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.
- 18.2 At the Home Office and the Foreign, Commonwealth and Development Office (FCDO), inspections cover interception, equipment interference and bulk powers under the Investigatory Powers Act 2016 (IPA) as well as property interference and overseas powers under the Intelligence Services Act 1994 (ISA). At the Northern Ireland Office (NIO), we inspect interception and equipment interference and, at the Scottish Government, interception. The differences are due to the intelligence agencies or law enforcement bodies that use the respective WGDs and the powers available to them, as well as the fact that the Scottish Government is not involved in national security authorisations.
- 18.3 We would usually conduct annual inspections at each department, reviewing casework across the powers they authorise. However, as a result of the Covid-19 pandemic, our inspection at the FCDO was deferred until 2021.

Findings

Home Office

- 18.4 On the whole we were satisfied that the Home Office was providing good challenge and advice to agencies on warrant applications and providing relevant advice to the Secretary of State on warrants which should be reviewed. We saw a good audit trail for urgent warrants sought out-of-hours. We do, however, recommend that the Home Office takes a more proactive approach with the agencies when new technical capabilities are being considered, particularly where there may be an impact on targeted interception (TI) safeguards.

Foreign, Commonwealth and Development Office (FCDO)

- 18.5 Our postponed FCDO inspection took place in March 2021. Overall, we concluded that the FCDO continued to perform its duties to a very high standard. Further improvements had been made to working practices in response to recommendations made on our previous

inspection and the advice provided to the Secretary of State continued to be rigorous, detailed and objective.

- 18.6 We noted that, in some cases, the Foreign Secretary imposed conditions on authorisations issued to the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) under section 7 of the ISA, as they are empowered to do under section 7(4). In a small number of cases these conditions could cause uncertainty. We recommended that, where the Foreign Secretary imposes conditions which might give rise to any such uncertainty, FCDO officials ought to clarify the intended effect of any conditions with the Foreign Secretary. The FCDO has actioned this recommendation and advised the Foreign Secretary accordingly.
- 18.7 We also discussed with FCDO officials the findings of our investigation into allegations of mistreatment at a detention facility overseen by FCDO (see paragraph 13.38). We were satisfied the FCDO has taken appropriate remedial action.

Northern Ireland Office (NIO)

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

Scottish Government

- 18.9 There was good evidence demonstrated of added value to applications to Scottish Ministers. In a particular operation, we saw monthly progress reports that had been requested from Police Scotland to show the continued necessity and proportionality due to the nature of the activity. This is good practice. We saw good clear comprehensive notes in relation to urgent out-of-hours applications.

19. Errors

Overview

- 19.1 Investigation of errors and breaches reported to us by the authorities we oversee is an important part of our work. We may also discover potential errors during our inspections. These are then investigated by the authority concerned and formally reported to us. We investigate all matters reported, considering both the impact the error has had on the human rights of any individual affected and whether the report reveals any failings in the processes and safeguards in place at that authority. Our website includes details about the type of errors we investigate.³⁴

UK intelligence community (UKIC) errors

- 19.2 For 2020, the errors reported did not suggest systemic failures of safeguards or an attempt to act unlawfully or circumvent safeguards. The tables and graphs below show the relevant errors reported by UKIC to the Investigatory Powers Commissioner's Office (IPCO) since 2017.

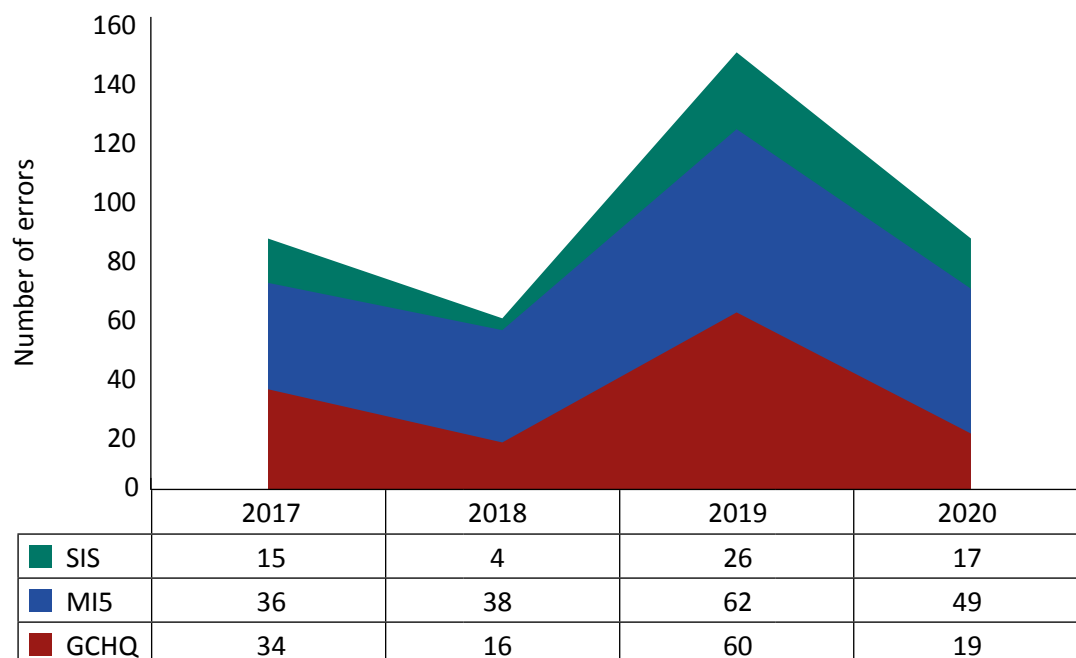
Definition: relevant error

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 (JC); and b) of a description identified for this purpose in a code of practice under Schedule 7.

³⁴ See: <https://www.ipco.org.uk/what-we-do/errors/>

Table 19.1 UK intelligence community (UKIC) errors, 2020

	Agency			Total
	MI5	SIS	GCHQ	
Covert human intelligence sources (CHIS)	3	1	0	4
Directed surveillance (DSA)	7	1	0	8
Property interference and intrusive surveillance (PI/IS)	1	0	0	1
Bulk personal data (BPD)	11	6	3	20
Section 7 Intelligence Services Act 1994 (s7 ISA)	0	1	0	1
Targeted interception (interception)	25	8	4	37
Bulk interception (interception)	0	0	9	9
Targeted equipment interference (EI)	2	0	0	2
Bulk equipment interference (EI)	0	0	3	3
Communications data (reportable) (CD)	14	1	1	16
The Principles	0	0	0	0
Systems	7	0	13	20
Total	70	18	33	121

Figure 19.1 UKIC errors (excluding systems and communications data), 2017 to 2020

- 19.3 In 2020, 121 errors were reported by UKIC to IPCO, substantially less than the 218 errors reported in 2019. However, the Covid-19 pandemic had a significant impact on the ability of all three UKIC agencies to investigate potential errors and confirm whether these were relevant errors which required reporting to the Investigatory Powers Commissioner (IPC). As such, there is likely to be a backlog of errors which occurred in 2020 but which had not yet been confirmed as relevant errors by the relevant internal processes by the end

of 2020. On that basis, it is not possible to draw any reliable conclusions from comparing errors statistics for 2020 against previous years.

- 19.4 As in our 2019 report, we have used the “systems” category to describe errors involving IT systems handling different types of warranted data. Thirteen of the errors in this category were reported by the Government Communications Headquarters (GCHQ), following a review of its approach to the categorisation of over-retention incidents as errors. GCHQ concluded that its previous approach needed to be revised and, as such, some incidents were re-categorised as relevant errors and reported to IPCO.
- 19.5 During GCHQ’s review, it assessed that some incidents were relevant errors under the Investigatory Powers Act 2016 (IPA), while others were reportable errors under the Regulation of Investigatory Powers Act 2000 (RIPA). In some instances, over-retention errors occurred across the threshold between the IPA and RIPA regimes. Most of these incidents and errors related to technical failures of automated deletion tools, with data accessible only to a small number of people.

Figure 19.2 Reportable UKIC communications data errors, 2018 to 2020

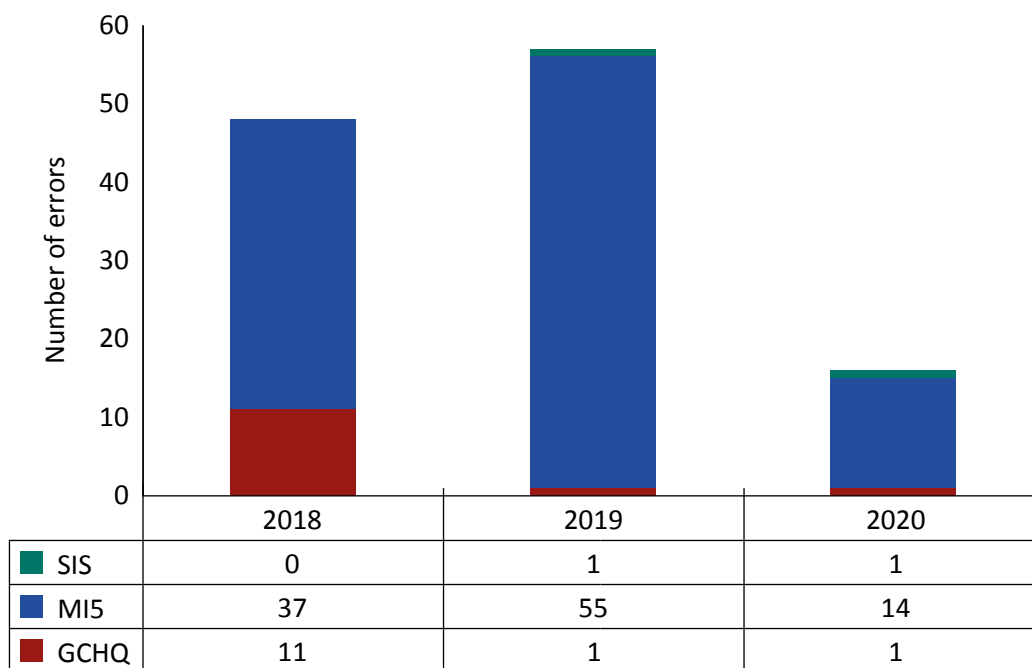


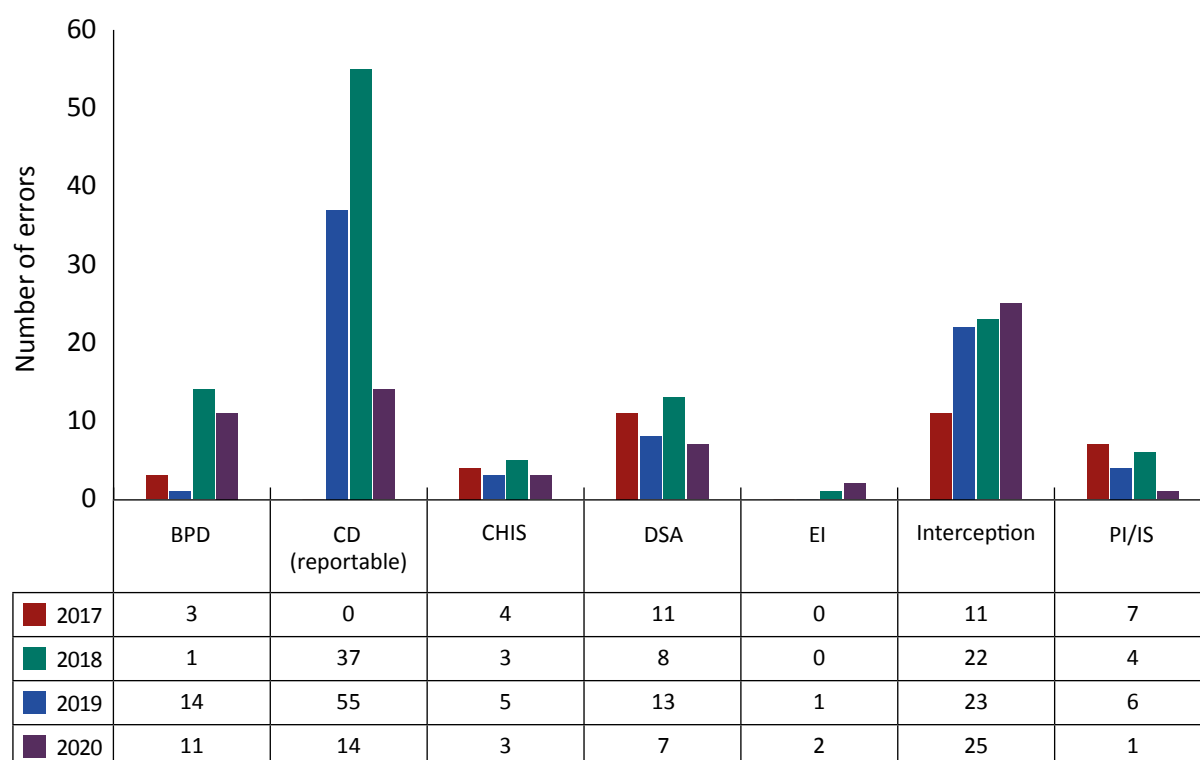
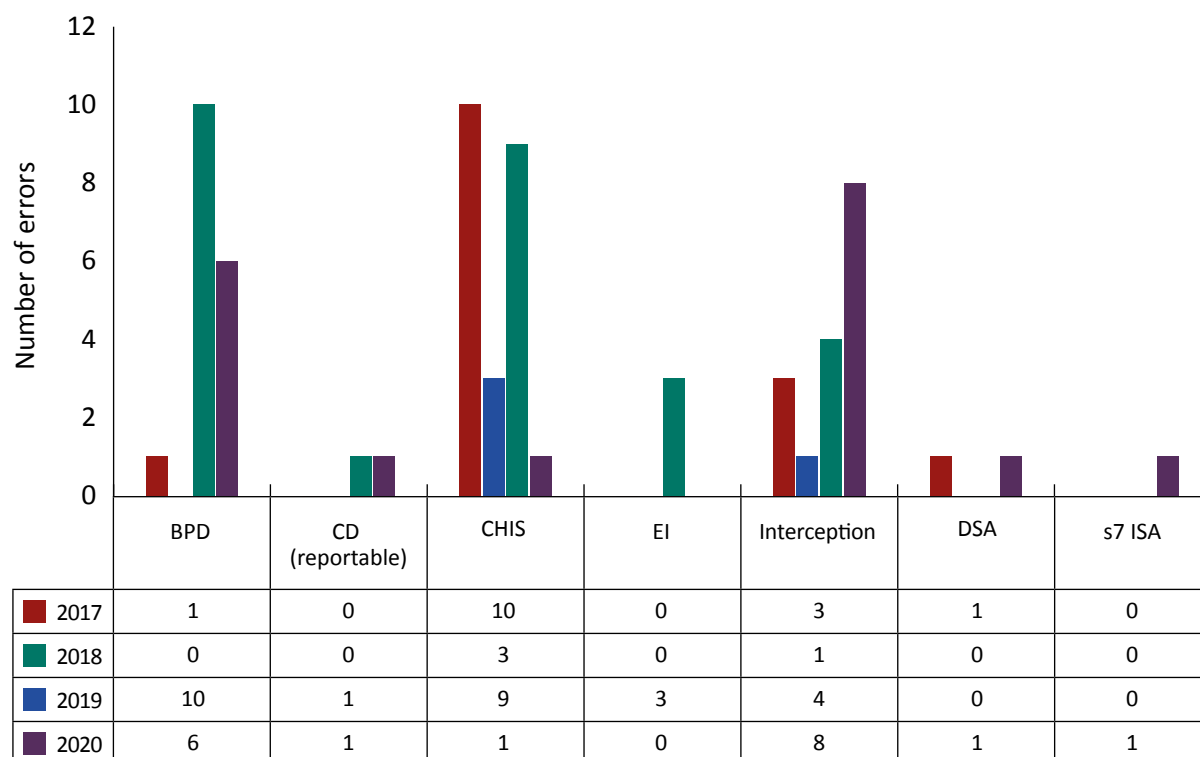
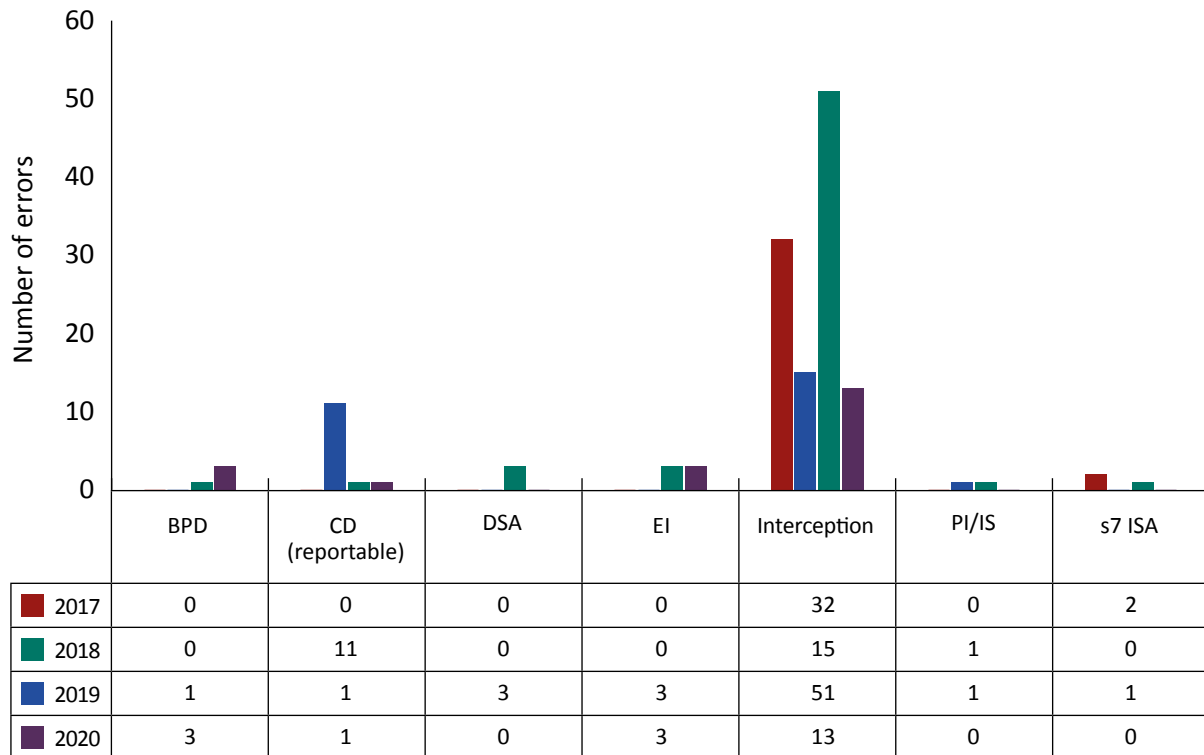
Figure 19.3 MI5 errors, 2017 to 2020**Figure 19.4 Secret Intelligence Service (SIS) errors, 2017 to 2020**

Figure 19.5 Government Communications Headquarters (GCHQ) errors, 2017 to 2020



Interception: UKIC and law enforcement

- 19.6 In comparison to 2019, the overall number of interception errors reported to us in 2020 decreased. We believe there are two main contributory factors; first, the intercepting agencies have worked hard to put systems in place to reduce the likelihood of errors reoccurring once they have been identified; and secondly, Covid-19 restrictions have reduced the activity which can lead to errors.
- 19.7 All of the intercepting agencies kept compliance staff numbers in place as essential during lockdowns to ensure the IPA and Codes of Practice (CoP) were being adhered to.
- 19.8 Once a public authority establishes that they have committed a relevant error, it must report it to the IPC within 10 working days. An Inspector will then investigate the circumstances that led to the error. In all of the relevant errors that were reported in 2020, we were satisfied that the agencies concerned have taken reasonable steps to mitigate the risk of reoccurrence of the same type of error. Most of the relevant errors reported in 2020 related to administrative process issues.
- 19.9 As in 2019, the most common error on interception related to the collection of material beyond the point of authorisation. In several cases, there was a delay between the authority notifying the telecommunications operator (TO) and the data flow from the intercepted device being stopped after the warrant had been cancelled. Typically, this latency resulted in up to 48 hours of unauthorised collection, although technical safeguards at each relevant authority meant that data was not ingested into monitoring systems for analysis.

- 19.10 Last year was the first full year of IPA relevant errors reported to us by GCHQ and set a baseline which had been an increase on previous years. In 2019, 51 relevant errors relating to interception were reported to us. This year, 13 interception errors were reported, a mixture of targeted intercept and bulk intercept. Many of these were caused by technology failures in relevant interception systems. We note that GCHQ has invested in resource, technology and systems to improve its ability to identify, trace and fix errors that are mainly caused by complex data flows. A rise in numbers last year was anticipated as they developed better methods for finding and fixing errors. It is not possible to say accurately if these errors were happening before but undetected. However, with now two years of full data, we will be able to track this in future through oversight and inspection.
- 19.11 In 2019, there were 24 interception errors reported by the five law enforcement agencies (LEAs) that are permitted to carry out interception under the IPA, a significant increase in comparison to 2018 when 13 were reported. We undertook to monitor this closely in 2020 and note that the number of reported errors has reduced to 15.
- 19.12 There were no serious errors reported in 2020 in relation to interception.

Data handling errors relating to interception material

- 19.13 As reported in earlier chapters, both the Police Service Northern Ireland (PSNI) and the National Crime Agency (NCA) reported data retention errors to us in relation to interception material. We continue to work with them to monitor progress on these matters. We are satisfied that interim measures have been introduced to ensure there is no impact on new warranted activity.
- 19.14 We have started to see compliance issues in the IT system used by LEAs to apply for and manage intercepted material, some of which have caused relevant errors. We will be monitoring this more closely next year. We are aware that there are advanced plans in place to replace this system and urge that momentum is maintained on this work.

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

- 19.15 The overwhelming majority of errors are reported promptly by the relevant authorities. It is pleasing to see that the strong culture of self-reporting identified in our previous annual reports continues and it is rare for errors to be identified during our inspections. In fact, many public authorities will err on the side of caution and report a "potential" error, either pending further investigation by the authority itself or seeking a determination from ourselves. 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 reoccurrence. All public authorities take errors seriously and compliance with the remedial measures is examined at the time of the next inspection.
- 19.16 The number of errors in proportion to the number of authorisations and renewals granted in 2020 continues to be reassuringly small. The 60 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; continuing the activity or leaving the equipment in situ after the authorisation has been cancelled; or exceeding the parameters of the

authorised activity. We are satisfied that material obtained from unauthorised activity is handled with appropriate care, including its destruction.

- 19.17 As set out in table 19.2, there were 92 errors under this heading reported during 2020; this is consistent with figures from previous years. None of these errors, when examined, were found to constitute a serious error as defined under section 231 IPA, in that no significant prejudice or serious harm was suffered by any individual as a result of the activity.

Table 19.2 Total surveillance, property interference, covert human intelligence sources (CHIS) and equipment interference errors for law enforcement agencies (LEAs), public and local authorities and prisons, 2020

Investigatory Power	Number of Errors
Directed surveillance	60
Property interference	8
Intrusive surveillance	3
CHIS (including undercover officers)	6
Equipment interference	15

- 19.18 As highlighted above, CHIS errors continue to form a very small fraction of the total number reported and are predominately associated with “status drift”; this means the failure to identify and authorise the use and conduct of a source timeously. In the rare instances when this has occurred, our Inspectors will stress how important it is that individuals are authorised as soon as they meet the criteria of a CHIS and that authorising officers (AOs) are appraised when an assessment period is likely to be protracted.
- 19.19 We recognise that human error is inevitable in the course of complex and often time critical investigations. However, it remains the case that many errors could be avoided if greater attention was paid to the legislation and the specific parameters of approvals to ensure the appropriate authorisations are in place in advance of an operation. We believe that this underlines the necessity for continuing high quality training, particularly when key officers (such as Covert Authorities Bureau (CAB) Managers and AOs) with specific covert surveillance responsibilities retire or move on to different areas of work. Changes in personnel may increase the likelihood of errors occurring or reduce the overall standards of compliance. It is vital that inexperienced officers are given the necessary support and supervision to mitigate these risks.

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

Reportable and recordable errors

- 19.20 There are two categories of error for CD: recordable and reportable.

Definition: Reportable error

Reportable errors occur when, as a result of a mistake, incorrect CD is acquired or disclosed.

Definition: Recordable error

Recordable errors concern cases where the mistake has not resulted in the acquisition of CD, either because the data requested simply does not exist, or the mistake was identified prior to the acquisition or disclosure being fulfilled.

- 19.21 We expect the authorities we oversee to be tracking both types of error to identify and rectify common themes and prevent future mistakes. The review of errors is also a key focus of our inspections. The appropriate Senior Responsible Officer (SRO) must have sight of error reports to enable any necessary strategic changes to policy or procedures. There is no obligation for authorities to notify the IPC of recordable errors and so these are not tracked in our annual statistics. However, these will be reviewed during inspections, at which point the SRO will be expected to provide reassurance that appropriate measures have been put in place to reduce the likelihood of reoccurrence.

Reportable errors

- 19.22 In 2020, 1,041 CD errors were reported to the IPC by the authorities we oversee. We investigated each error and re-categorised 36 of those as recordable, making a total of 1,005 reportable errors (see table 19.3). This is a very slight decrease in comparison to 2019, during which 1,011 were reported.
- 19.23 In 2020, the number of reportable errors caused by law enforcement and other public authorities decreased by 14 in comparison to the previous year. The transition to the IPA required workflow providers to make significant changes to their systems. This in turn led to 12 workflow errors being reported to us in 2019. In 2020, the systems have bedded in, resulting in just a single error involving workflow being reported.
- 19.24 The number of TO errors continue to increase, with a further 23 errors in 2020 with 253 in total. In our 2019 report, we referred to the collaborative work being undertaken between the NCA, the Knowledge Engagement Team (KET) and IPCO. Based on the ethos to always check and challenge results, public authorities are clearly reporting their concerns to this group. This in turn has led to a series of serious error investigations (Annex C, cases 1, 20, 21, 22, 26, 27 and 29).
- 19.25 Swift assessment and early notifications to the Single Point of Contact (SPoC) community, as evidenced in the cases above, have without doubt prevented such errors from having a serious impact upon persons unconnected to an investigation.

Table 19.3 Reportable communications data errors, 2018 to 2020

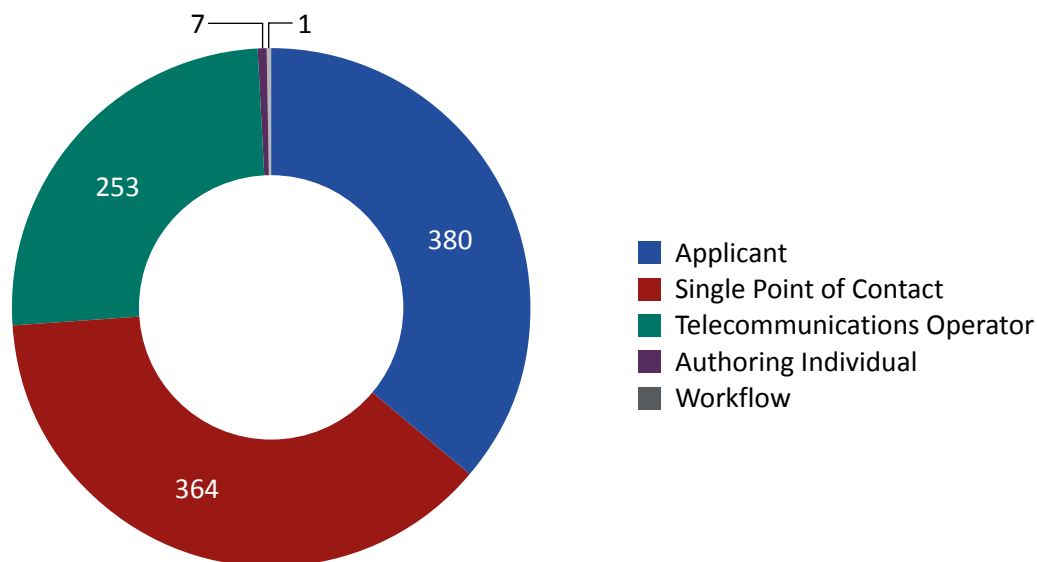
Cause of error	Number of errors		
	2018	2019	2020
Law enforcement agencies	758	755	741
Telecommunications operator	127	230	253
Other Public Authorities	13	14	10
Workflow	5	12	1
Total	903	1,011	1,005*

Notes:

*Two errors were identified during IPCO inspections and subsequently reported.

19.26 Most CD errors reported by LEAs and public bodies continue to relate to the actions of a SPoC or the applicant (74%), as shown by the figure below. This is consistent with the reported errors for 2019 and remains proportionate to the roles these individuals play in handling CD applications and data.

Figure 19.6 Communications data errors by responsible authority or system, 2020



19.27 As shown by the following breakdown, the biggest single cause of an error rests with the applicant seeking CD upon an incorrect identifier (telephone number, username, email address or internet protocol (IP) address). This equates to over 31% of all LEA errors, which is in line with the figures we reported in 2019.

Table 19.4 Breakdown of communications data errors by error type and responsibility, 2020

	Applicant ¹	Single Point of Contact	Telecoms Operator	Authorising Individual	Workflow
Incorrect Identifier	311 (13 IP) ²	86 (14 IP)	81	0	0
Time/Date	26 (11 IP)	181 (58 IP)	48	0	0
Data Type	13	81	22	0	1
Excess/No Data	0	0	90	0	0
System Error	0	0	4	0	0
No Authority	2	28	7	7	0
Other	12	4	1	0	0
Total	364 (24 IP)	380 (72 IP)	230	7	1

Notes:

¹ Includes data provided to the authority by a 3rd Party (44)

² Internet protocol address

Reportable errors: applicant

- 19.28 In 2020, 286 errors were made by applicants when transcribing the identifier into an application. It is again the case of officers' hand typing (especially a telephone number) into an application as the number itself is seldom capable of being electronically copied over. In 2020, we saw a rise in the number of errors based on the details provided by 3rd parties e.g., victims, witnesses, and other organisations.

Reportable errors: Single Point of Contact (SPoC)

- 19.29 The 380 errors made by a SPoC continues to reflect their central role in the acquisition of all CD. Applications made within an authority's own workflow system require the relevant data to be entered into another system once authorised. The identifier, date/time and data type must all be accurately entered by the SPoC into a variety of different online TO portals.
- 19.30 In our 2019 report, we mentioned automatic acquisition (AA), the technology that eliminates the manual transfer of data from workflow into a TO's portal. Without AA, an accurately approved application within workflow faces the risk of error during the transference of the identifiers into the TO's portal.
- 19.31 In 2020, two thirds of all acquisitions were acquired via AA. This rise is a result of the increase in services available via AA rather than an increase in the number of public authorities using it. While the expected take up of AA by more public authorities has not materialised, we have been advised that progress is now back on track. AA is an important technological advancement that reduces the risk of SPoC transposition errors. The take up by others will be closely monitored in 2021.
- 19.32 For those able to use AA, 87% of all data is now being acquired in this way. For the remaining 13%, while certain services cannot use AA, for most it's the urgency that precludes the use of AA.

Reportable errors: telecommunications operators (TOs)

- 19.33 We continue to work closely with TOs whenever an error is identified to determine the cause and impact of the issue. Of the 230 TO-reported errors, we classified 13 as falling within the IPA's definition of serious; in nine incorrect data was supplied and four were the result of technical issues.
- 19.34 In 2020, we strengthened our links with the Information Commissioners Office (ICO). Currently, a TO needs to report the same error to both IPCO (as incorrect data) and to ICO (as a breach of data protection). We have started conducting quarterly reviews with the ICO, looking at all TO errors to help TOs develop processes to minimise errors. The reviews are encouraging, and we are planning to initiate a single reporting process from mid-2021.

Serious error investigations

- 19.35 We investigate all relevant errors that are reported to us which we judge may fall within the definition of a serious error as set out in the IPA:
- circumstances which we judge to be potentially serious remain;
 - technical errors relating to the communications service provider (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 dataset.

19.36 We undertook 29 investigations in 2020 and a summary of each of these appears in Annex C.

Table 19.5 Serious errors by cause, 2020

Error Type	Relevant Public Authorities	Telecoms Operator
Identifier	6	0
Intelligence	5	0
Time Date/Time Zone	3	0
Incorrect Data Supplied	0	5
System	0	6
Misleading Data	1	2
Breach of Code	1	0
Total	16	13

- 19.37 We adjudged significant harm in four of the 29 cases investigated. Under the provisions of section 231 IPA a 'relevant error' only applies to errors made by a public authority.
- 19.38 Three of these cases involved the upload of indecent images and the fourth was a crime in action. Common to all was the need to resolve details of the customer allocated to an IP address at a specified time and date.
- 19.39 Errors made around Internet Protocol Address Resolutions (IPAR) continue to pose the greatest risk of a serious error. An IP address can move between customers and could be supplied with a time stamp from anywhere in the world. Of the 1,005 reportable errors, 109 fell into this high-risk category. This represents a significant drop from the 506 IPAR-related errors reported to us in 2019. In this regard, credit must go to the SPoCs adhering to the Error Reduction Strategy (ERS) which was produced by the National Police Chiefs Council (NPCC)'s Data Communications Group in consultation with IPCO.
- 19.40 Through a series of peer reviews, anomalies are being picked up before approval. There is no requirement under the CoP to report any error to IPCO if it has been identified before the application is approved. Our 2020 inspections found many examples of returns for amendment with issues over accuracy apparent. The collation of this activity remains difficult to quantify. We have therefore encouraged public authorities to implement a process to better capture this essential guardian and gatekeeping role of the SPoC.
- 19.41 The drop in IP-related reportable errors is most welcomed. Our examination of all IP-related errors identified that 57 of the 109 IP-related reportable errors concerned the SPoC submitting an incorrect time frame into the various TO portals. In effect, it is possible to have an accurate fully approved request that results in an error when the SPoC enters the wrong time and date into a TOs portal to acquire the CD. While the use of AA is slowly being extended to IPAR requests this risk remains.

- 19.42 Errors involving erroneous data supplied by a TO remain the most difficult to detect. At the end of 2020, the redrafting process to update the ERS was commenced. The update is in response to new technologies and the findings from our 2020 investigations. It will be published in 2021.
- 19.43 A central facet of the revised ERS requires public authorities to mitigate against TO errors by seeking some form of corroboration to the CD identifier or address provided. Our advice is that uncorroborated internet-based CD should only be used for action on an exceptional basis.
- 19.44 The most common incident that led to officers contacting people unconnected to the incident involved concern for welfare. Each has used the emergency provisions under section 61A IPA and had been verbally approved. In such cases, a more manual process is used. Identifiers are often passed by word of mouth via a reporting person, among members of the public authority and across to the TO. Other causes involved incorrect information being supplied by a 3rd party (three) and inputting errors found within historical records (three).
- 19.45 The overriding aim is the protection of life and any error that delays the search can have serious consequences. Fortunately, in 2020 delays due to an error with the CD did not have a serious outcome.
- 19.46 Although low in number, basic errors still occur. In Annex C, cases 12, 16 and 28 are examples of how such errors can lead to people being accused of crimes and highlight that everybody involved must remain vigilant.

20. Statistics

Overview

- 20.1 The Investigatory Powers Commissioner's Office (IPCO) collects a wide range of statistics on the use of investigatory powers, including those required to be published in this report under section 234 of 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. Over the last year, we have reviewed and streamlined the way we collect information from the organisations we oversee to ensure that the process is as efficient and reliable as it can be to produce an accurate picture. Further details of this exercise are set out below.
- 20.2 Our objective is to collect data that can be used by IPCO, and as far as possible, published. We continue to welcome the challenge we receive on the value of statistics we publish and we strive to improve the level of transparency we offer to Parliament and the public through our report. As an organisation, we are committed to ensuring that we do not provide statistics which would be partial or misleading or those which could cause any damage to the ongoing operations of the authorities we oversee and to national security. For these reasons, we provide limited statistics in relation to the functions of the intelligence agencies, where we would not be able to give sufficient contextual detail to enable those figures to be analysed effectively by readers. It is also worth noting here that while we do collect statistics, we do not take a structured or statistically-driven approach to oversight, which we believe is best conducted on the basis of compliance risk and areas of clear public interest.
- 20.3 We have selected statistics for publication which we believe will give an accurate picture of the extent to which the different categories of authority that we oversee are using their powers, and to which specific powers are used. The context within which they are being used, and our findings from recent oversight, are given in the previous chapters. Where possible, we have sought to present statistics in the same format as our previous reports to enable comparisons to be drawn. However, year-on-year comparisons have not been feasible across all statistics this year because of the changes to the data we have collected.

Methodology for collecting statistics

- 20.4 At the end of 2020, we sent out a detailed questionnaire to all public authorities seeking data on each power available to them. All responses were quantitative and where applicable, nil returns (indicating a non-use of a power) were required.
- 20.5 In comparison to previous statistical collections, some questions previously asked by IPCO, such as on cancellations, or the number of authorisations extant at the end of the year, were dropped. Questions relating to communications data (CD) in particular were rationalised to focus only on the data of most value to us.

20.6 The following definitions relate to the statistics that appear throughout this report:

- Applications are defined as any time the use of a power in the form of a warrant or authorisation was formally sought from an issuing authority, including renewals of extant authorisations. It does not include modifications or cancellations.
- Authorisations are defined as any time the use of a power came into effect. For example, when a warrant has both been granted by a Secretary of State and then approved by a Judicial Commissioner (JC). Authorisations are the basic unit of measure in these statistics and indicate the degree to which each of the powers were authorised.
- Refusals are defined as any application to use a power formally refused by the person who has the authority to grant the use of the power (e.g., an authorising officer, or a Secretary of State), or, in the case of a JC, to approve the use of the power. It does not include revisions to preliminary versions of the application.

- 20.7 It must be kept in mind that the authorisation to *use* a power does not in itself mean that the conduct authorised then actually occurred, with information gathered or intrusions to privacy made. In some cases, the need for the authorisation may have fallen away, or the operational circumstances did not permit the conduct to be undertaken (e.g., the target of a directed surveillance moving overseas). Nor does an individual authorisation indicate the scale of the intrusion that then occurred where conduct was carried out; some authorisations may have resulted in only a fleeting intrusion or limited intelligence gain, whereas others using the same investigatory power may have resulted in a far deeper, more sustained intrusion. It is not possible to distinguish such differences from these statistics and care should be taken when drawing inferences from the data.
- 20.8 As well as measuring the number of authorisations across the powers, this year we have collected and included data on the use of urgency provisions (when available in law) and authorisations that involved more sensitive or confidential information, such as whether legally privileged material was sought or likely to be obtained.
- 20.9 All returns were quality assured on receipt by IPCO. This was to ensure returns had been given when required in the correct format. Any obviously anomalous values were queried and corrections obtained where necessary. It was not possible to verify the accuracy of all individual values in the returns, as this would require examining records at source and it is likely that errors in the data exist due to failure to follow guidance correctly, data input errors in the returns and other mistakes. The centralised records maintained by public authorities on which the statistics are based are examined on inspection by IPCO and deficiencies noted and corrected then. This means that there are likely to be some errors in the data, but the overall quality of the data will be within acceptable margins of error, and we can have confidence that they are an accurate overall representation on the use of the investigatory powers.
- 20.10 CD statistics remain the area where the greatest errors in accuracy occur. This is a function of the volume of activity occurring, differing record keeping practices and technology in use between differing public authorities which obtain CD, and the changes made this year to how CD statistics have been collected. For example, an 'authorisation' means for the purpose of these statistics an application that has been approved. A single such CD 'authorisation' may include a number of 'authorities', meaning the legal instrument given by the public authority to the telecommunications operator, with the number depending on how many telecommunications operators are required to supply the data. This can

lead to errors in statistics with some public authorities recording 'authorities' rather than 'authorisations' in their returns to IPCO.

Warrants and authorisations

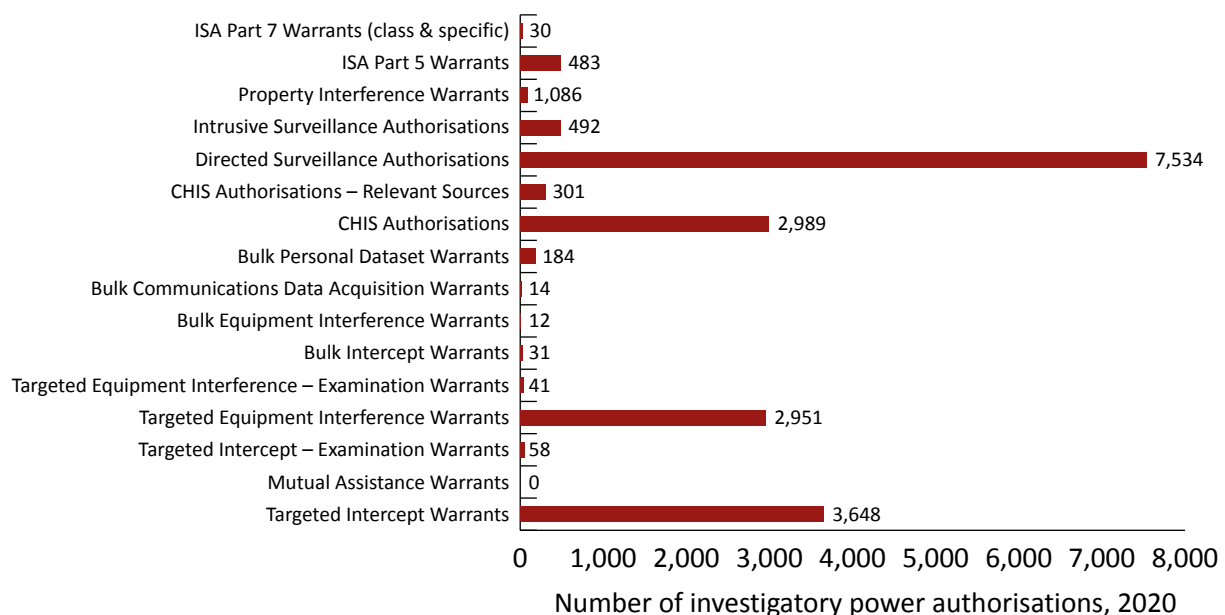
20.11 In 2020, 271,712 warrants and authorisations were issued. Table 20.1 shows how these break down across the different sectors. The high number of authorisations by law enforcement agencies (LEAs) is a result of their frequent use of CD powers.

Table 20.1 Investigative and other powers authorised by public authority sector, 2020

	UKIC	LEAs	WPAs	Local Authorities	Prison Services	Total
Number of authorisations	18,119	251,674	1,130	588	181	271,712

20.12 Figure 20.1 sets out the distribution of investigatory powers used in 2020. This figure excludes the 251,866 CD authorisations that were issued.

Figure 20.1 Investigatory power authorisations (excluding communications data authorisations), 2020



20.13 Table 20.2 gives total numbers for the warrants and authorisations issued, considered and approved for the period 1 January 2020 to 31 December 2020. It also provides the total number of certain notifications made to IPCO during this period and the number of applications refused by JCs (12).

20.14 JCs have the option to seek clarification on the detail of an application. This could involve internal discussions with the legal team but in most cases requires further detail to be provided by the applicant. In 2020, JCs requested further information in 50 cases. Of these, three were subsequently withdrawn (or no decision was required), two were refused and

one resulted in a final decision from the JC for the destruction of records as it was not considered necessary or proportionate for the LPP material to be detained.

Table 20.2 Breakdown of authorisations, notifications and refusals, including those considered by a Judicial Commissioner, 2020

	Considered by a Judicial Commissioner	Approved, issued or given	Refused by a Judicial Commissioner
Covert human intelligence sources (CHIS) including juveniles and relevant sources	N/A	3,282	N/A
Directed surveillance	N/A	7,534	N/A
Intrusive surveillance	N/A	492	N/A
Property interference under the Intelligence Services Act section 5	N/A	483	N/A
Property interference under the Police Act 1997	N/A	1,086	0
Bulk personal datasets – class warrant	108	108	0
Bulk personal datasets – specific warrant	77	76	1
Directions under section 219 of the Investigatory Powers Act 2016	0	0	0
Directions under section 225 of the Investigatory Powers Act 2016	2	2	0
Bulk communications data acquisition warrant	14	14	0
Communications data authorisation	N/A	251,866	N/A
Bulk interception warrant	31	31	0
Targeted examination of interception warrant	59	58	1
Targeted interception warrant	3,649	3,648	1
Bulk equipment interference warrant	12	12	0
Targeted examination of equipment interference warrant	41	41	0
Mutual assistance warrant	0	0	0
Targeted equipment interference warrant	2,957	2,951	6
Relevant source notifications ¹	–	636	0
Request to retain legal professional privileged material ²	167	161	2
Notification under section 77 of the Investigatory Powers Act 2016	18	17	1

Notes:

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

2. The discrepancy of four between the number of applications and the number of approval and refusals may be accounted for by year-end counting rules but is more likely to be undetected reporting errors by public authorities.

Covert human intelligence sources

20.15 Covert human intelligence sources (CHIS) authorisations in this section refer to any authorisation to use a person as a CHIS, but not subject to the relevant source order for law enforcement undercover officers. The statistics in this section relate to the use of both members of the public as a CHIS and also officers of public authorities not subject to the relevant source order acting undercover. This includes members of public authorities acting as a CHIS online.

20.16 As shown by figure 20.2, a total of 2,137 CHIS authorisations were made in 2020 across LEAs, the wider public authorities (WPAs), local authorities and prisons. Of the 2,086 authorisations to LEAs, six of these were urgent.

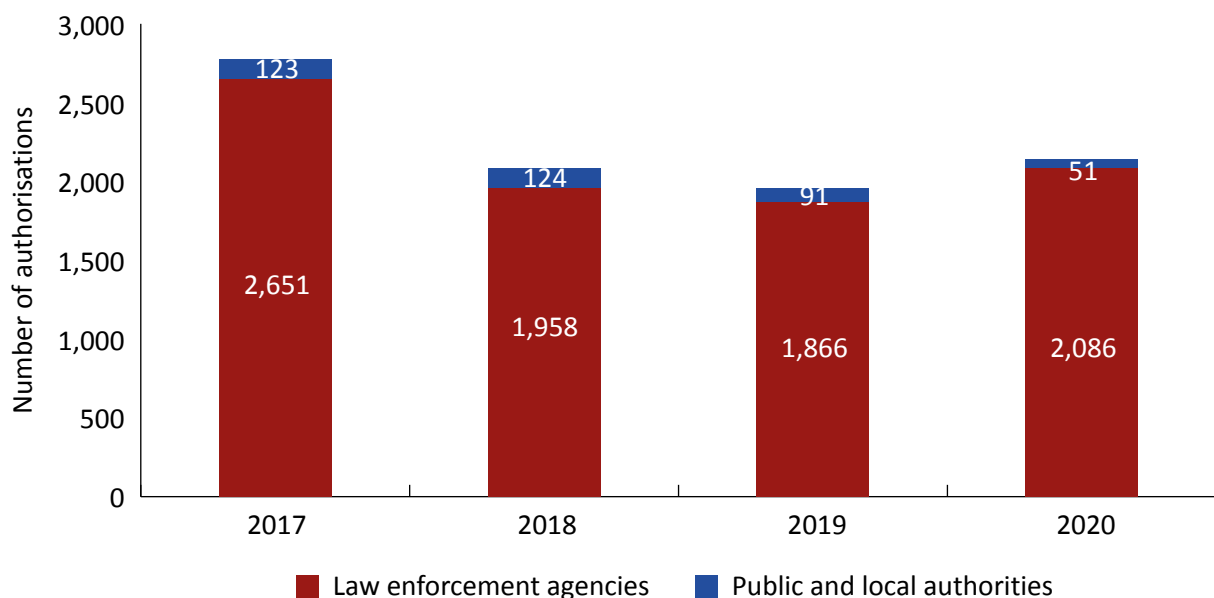
Participation in crime

20.17 Participation in crime (PIC) authorisations continue to be a small but significant proportion of the total number of CHIS authorisations granted to LEAs, WPAs, local authorities and prisons, with 146 authorisations granted in 2020, including 16 under urgent provisions.

Juvenile CHIS

20.18 Of the 2,137 CHIS authorisations granted, only three related to juveniles. None of these were under the age of 16 at the time the authorisation was granted.

Figure 20.2 Covert human intelligence sources of law enforcement agencies, public and local authorities, 2017 to 2020



Note:

UKIC authorisations are not included.

Relevant sources

20.19 Law enforcement (and some other public authority) officers acting undercover as CHIS are referred to as relevant sources and applications are authorised for 12 months. A renewal must be approved by a JC. At the nine-month point, the authority must notify the

Investigatory Powers Commissioner (IPC) of their intention to renew that authorisation if and when it reaches the 12-month point; upon this notification one of our Inspectors will carry out a review of the operation to date and their report will be available both to the authorising officer (AO) and the JC. Such notification is not a guarantee that the public authority will still actually seek to renew but, if they choose not to, then the authorisation must be cancelled.

Table 20.3 Relevant sources authorisations and applications, 2020¹

Total Applications (incl. renewals) ²	Total Authorisations (incl. renewals)	Urgent	Renewals (long term authorisations)	JC refusals ³
301	293	2	75	0

Notes:

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

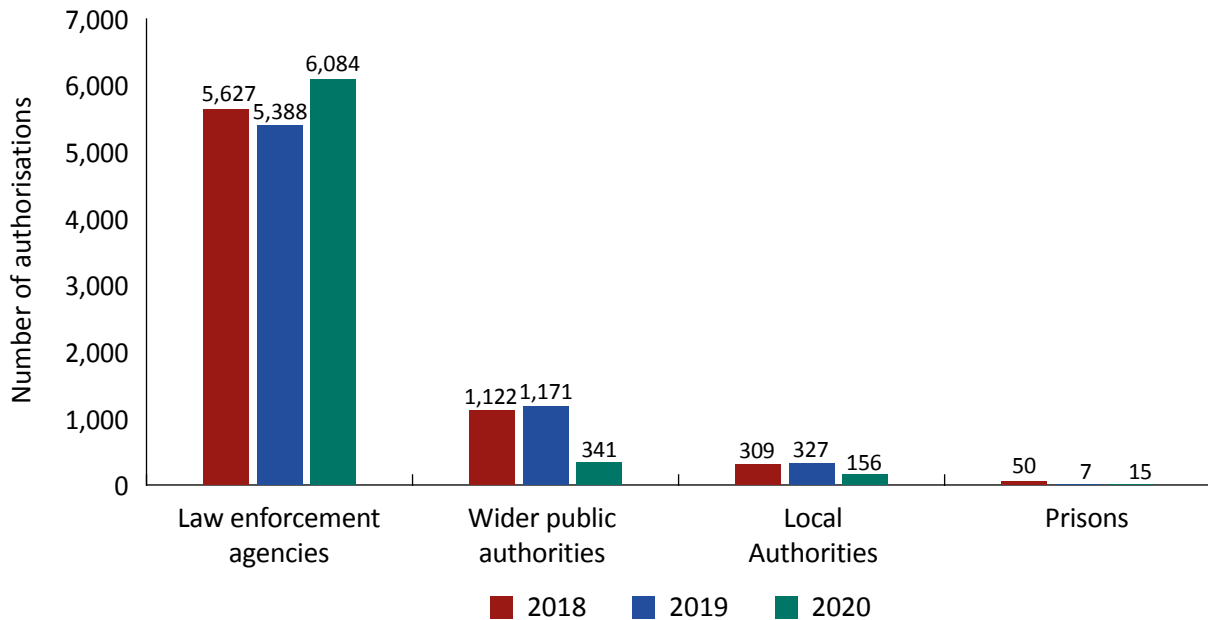
2 Applications include notifications to IPCO of authorisations and applications to renew authorisations after 12 months.

3 Refusals relate to applications to renew only.

Directed surveillance

- 20.20 As noted in previous chapters, directed surveillance is a critical investigative tactic for the range of authorities that we oversee and is available to public and local authorities as well as law enforcement. Directed surveillance has evolved in recent years to include online tactics as well as traditional physical surveillance methods. The number of directed surveillance authorisations (DSAs) in 2020 remains broadly consistent with previous years.
- 20.21 Figure 20.3 shows that a total of 6,596 directed authorisations were made in 2020 across LEAs, WPAs, local authorities and prisons. Of these authorisations, 456 authorisations were made under the urgent provisions.

Figure 20.3 Directed surveillance authorisations across law enforcement agencies, wider public authorities, local authorities and prisons

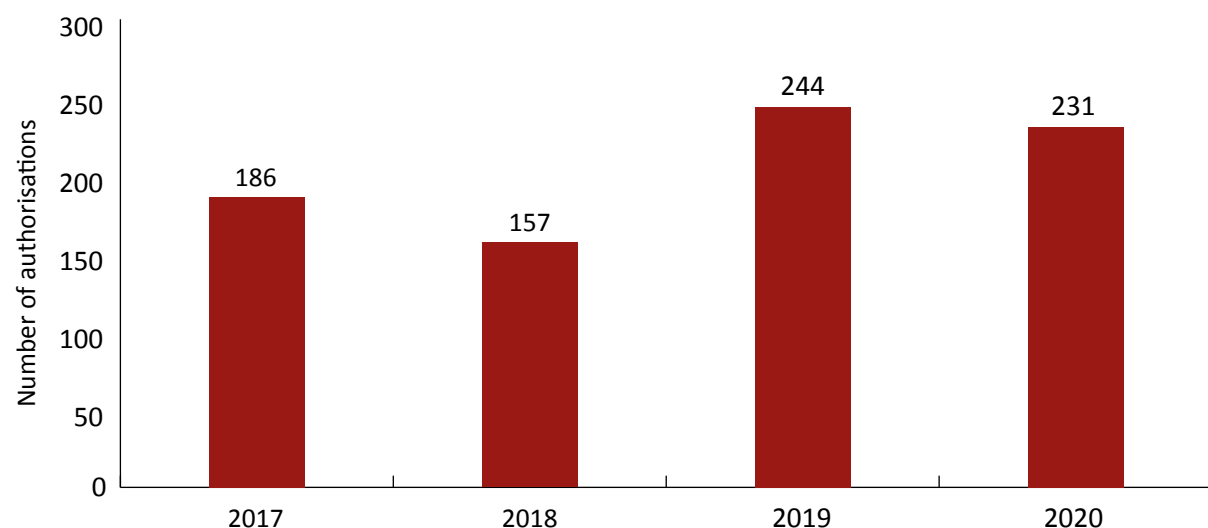


20.22 Only seven DSAs were granted that either sought or were likely to obtain confidential or privileged material which was other than material subject to legal professional privilege (LPP) and three DSAs were granted where LPP was either sought or likely to be obtained.

Intrusive surveillance

20.23 In 2020, 231 authorisations were granted to LEAs. Of these, 28 were urgent authorisations. Only one of these authorisations either sought or were likely to obtain confidential or privileged material which was other than LPP and a further 12 were granted where LPP was either sought or likely to be obtained.

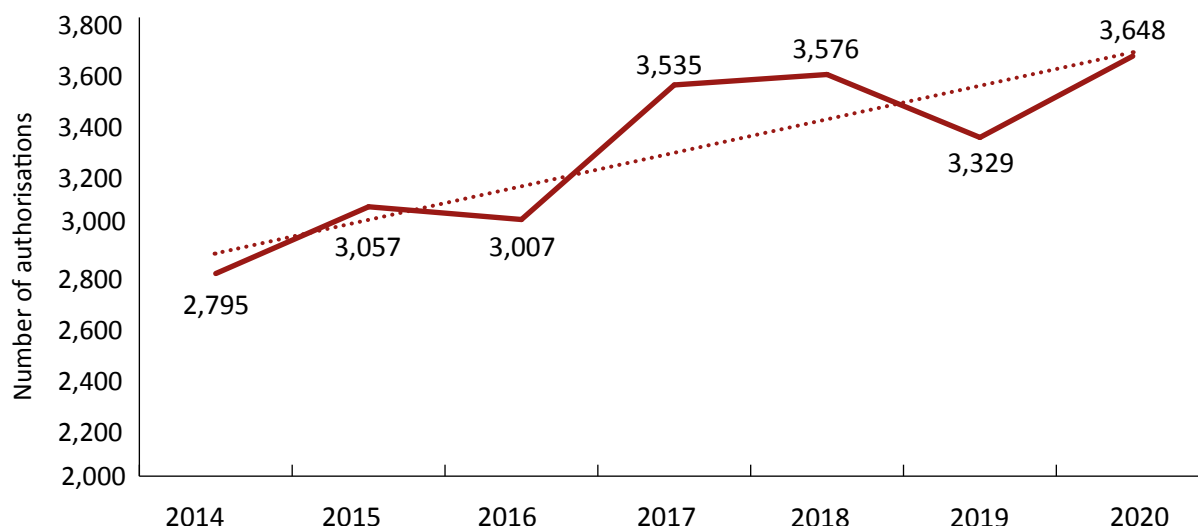
Figure 20.4 Intrusive surveillance authorisations for law enforcement agencies, 2017 to 2020



Targeted interception

20.24 The number of targeted interception (TI) warrants granted increased by 9.8% in 2020 in comparison to 2019. Of the warrants approved, 1,470 were renewals and 59 were obtained under urgency provisions.

Figure 20.5 Targeted interception authorisations for the UK intelligence community, the Ministry of Defence and law enforcement agencies, 2014 to 2020



20.25 Table 20.4 sets out the number of warrants granted that involved either deliberate attempts to obtain legally privileged material (LPP – sought) as part of the purpose of the intercept warrant, warrants where it was likely or possible that LPP would be obtained (LPP – possible) or warrants relating to sensitive professions. Any warrant which involved such confidential material is subject to additional scrutiny at inspection and the material produced by such warrants subject to additional safeguards as set out in the Code of Practice.

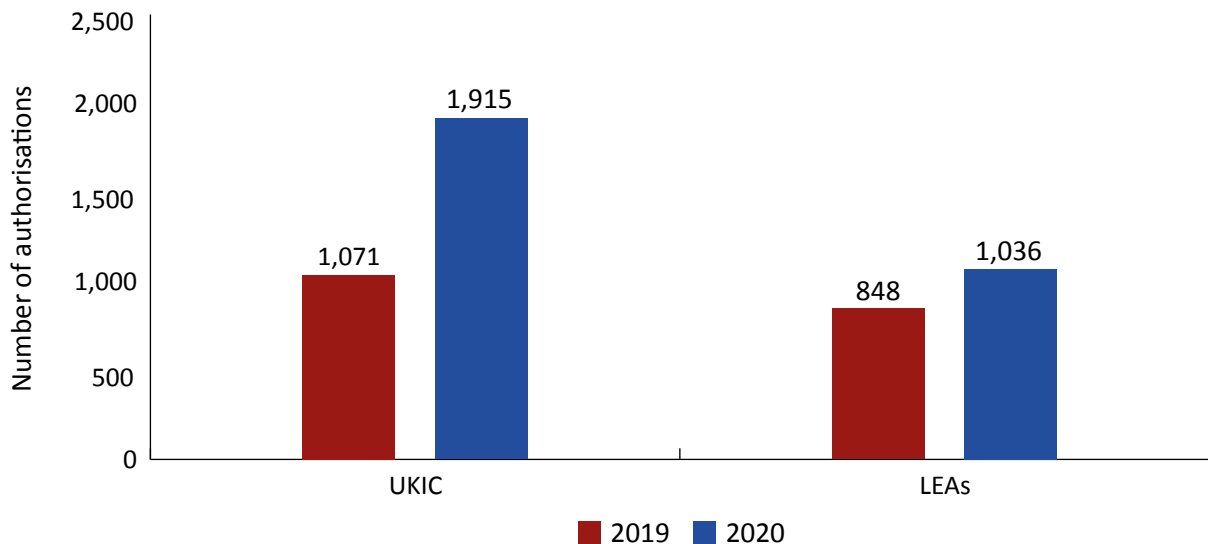
Table 20.4 Targeted intercept warrants involving confidential material, 2020

LPP – sought	LPP – possible	Sensitive professions
12	359	35

Targeted equipment interference

20.26 In 2020, 2,951 authorisations were granted to use targeted equipment interference (TEI) powers, a significant increase of 54% compared to 2019, when 1,919 authorisations were granted. Of the 2,951 authorisations issued, 363 were made under urgent provisions. The three WPAs who have access to TEI powers made no use of them in 2020.

Figure 20.6 Targeted equipment interference authorisations for the UK intelligence community and law enforcement agencies, 2019 to 2020



20.27 As shown in table 20.5, confidential material was only sought or likely to be obtained in a small number of warrants.

Table 20.5 Targeted equipment interference warrants involving confidential material, 2020

LPP – sought	LPP – possible	Sensitive professions
14	207	66

Communications data

20.28 Table 20.6 sets out the total number of authorisations made either under Section 60A (authorised by the Office for Communications Data Authorisations (OCDA)), those authorised under Section 61 (national security – not authorised by OCDA) or under the urgent provisions.

20.29 In total, 251,866 CD authorisations of all kinds were made in 2020. LEAs were the greatest user of the power, with 239,086 authorisations, which was 94.9% of all authorisations made.

Table 20.6 Communications data authorisations, 2020

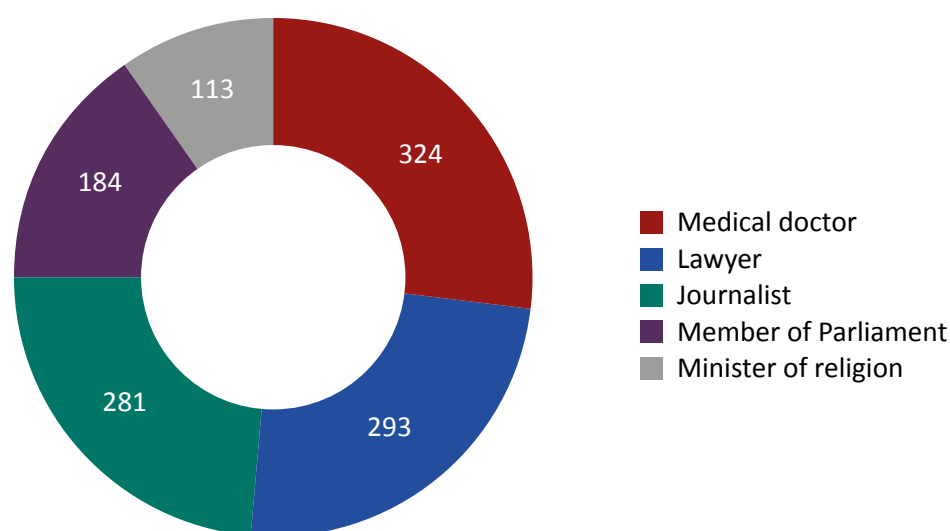
	UKIC	LEAs	WPAs	Local Authorities	Prison Services
Total authorisations (all types)	11,444	239,086	969	212	155

20.30 CD applications are used to request one or more data items. Unfortunately, the systems used to process that data are not able to provide precise statistics and we believe that there is a margin of error of around 10% on the number of data items obtained. However, the nature of our oversight means that this does not reduce the level of confidence that we

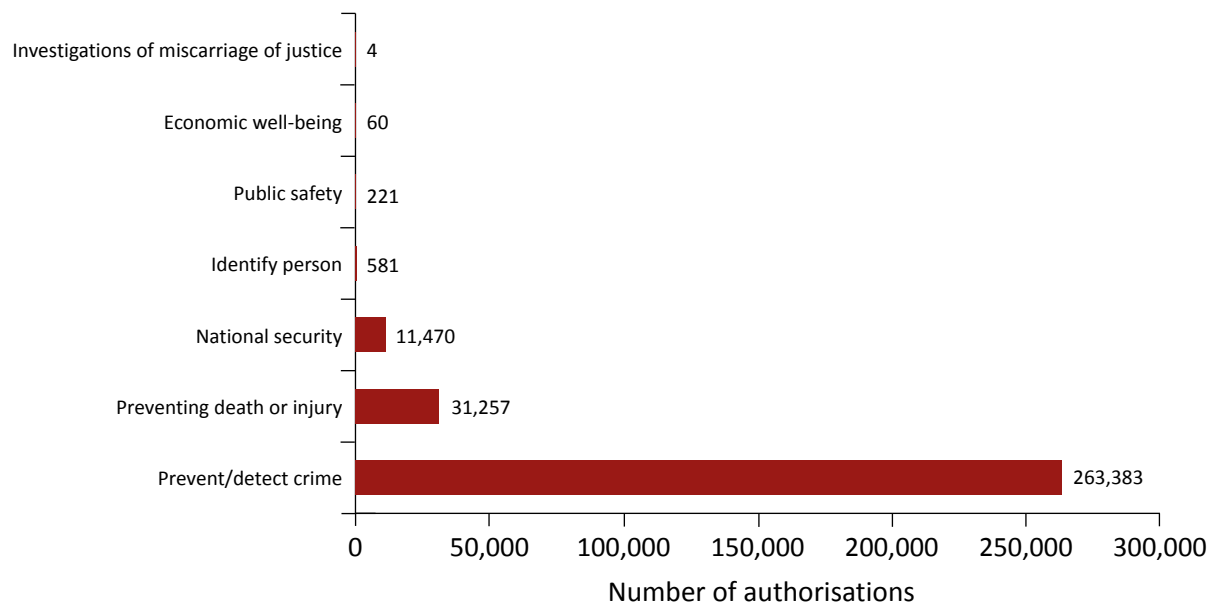
have in the compliance of those authorities. In 2020, in the region of one million CD items were obtained.

- 20.31 Figure 20.7 sets out the number of authorisations obtained in relation to sensitive professions. CD acquired and disclosed under the IPA does not include content. Nonetheless, there must be considerations as to whether there is a risk that acquiring the data will thereby create an unwarranted risk that sensitive professional contacts will be revealed, or that there will be other substantive adverse consequences which are against the public interest. The Communications Code of Practice (from paragraph 8.8) requires applicants to give special consideration to requests for CD that relate to persons who are members of professions which handle privileged or otherwise confidential information. This can include, for example, lawyers, journalists, members of parliament, ministers of religion or doctors. Public authorities must record the number of such applications and report to the IPC annually. Most applications relating to sensitive professionals were submitted because the individual had been a victim of crime. For example, it might be the case that a member of parliament or a lawyer received threatening or malicious calls and CD requests were made in an attempt to attribute phone numbers or email addresses to perpetrators.

Figure 20.7 Communications data authorisations involving members of a sensitive profession, 2020



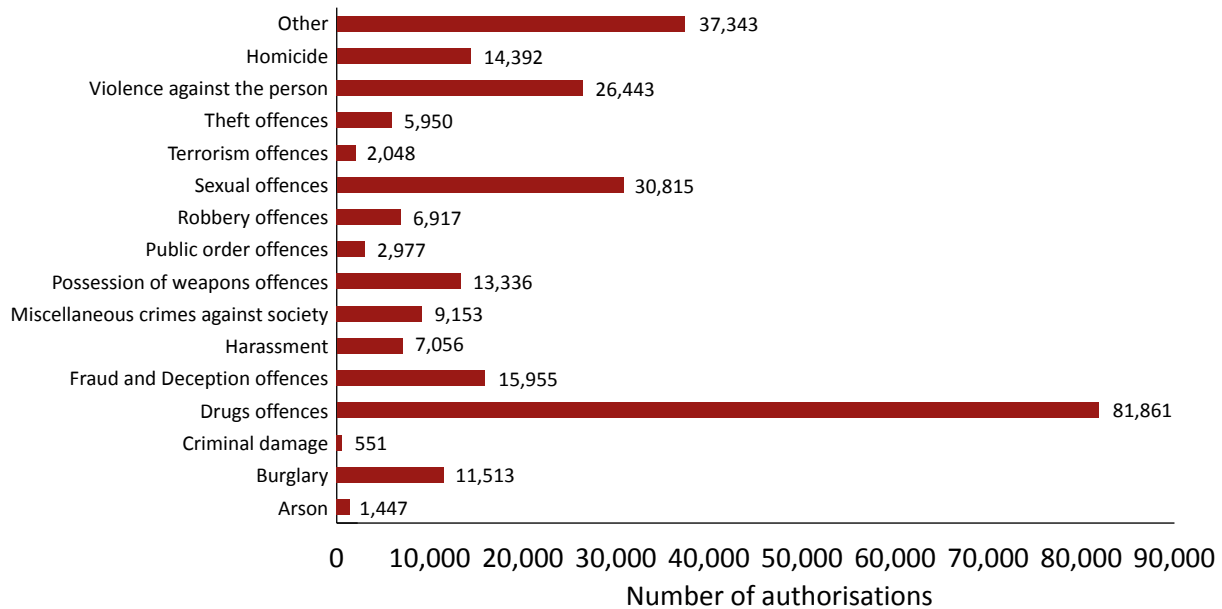
- 20.32 In 2020, 17 authorisations were obtained to confirm or identify a journalist's source, none of which were urgent. One application was refused by a JC.
- 20.33 Figure 20.8 shows the number of authorisations for each of the seven statutory purposes. Prevention and detection of crime is the largest, representing 85.8% of the total reported authorisations with LEAs being the main user.

Figure 20.8 Communications data authorisations by statutory purpose, 2020

20.34 For each CD authorisation, where the statutory purpose is 'prevention and detection of crime', public authorities who can use this purpose are required to keep a record of what types of crime the authorisation relates to. One authorisation may relate to more than one of the crime categories (as shown in detail in figure 20.9), which is why the total number of crime types exceeds the number of authorisations shown in table 20.6 above.

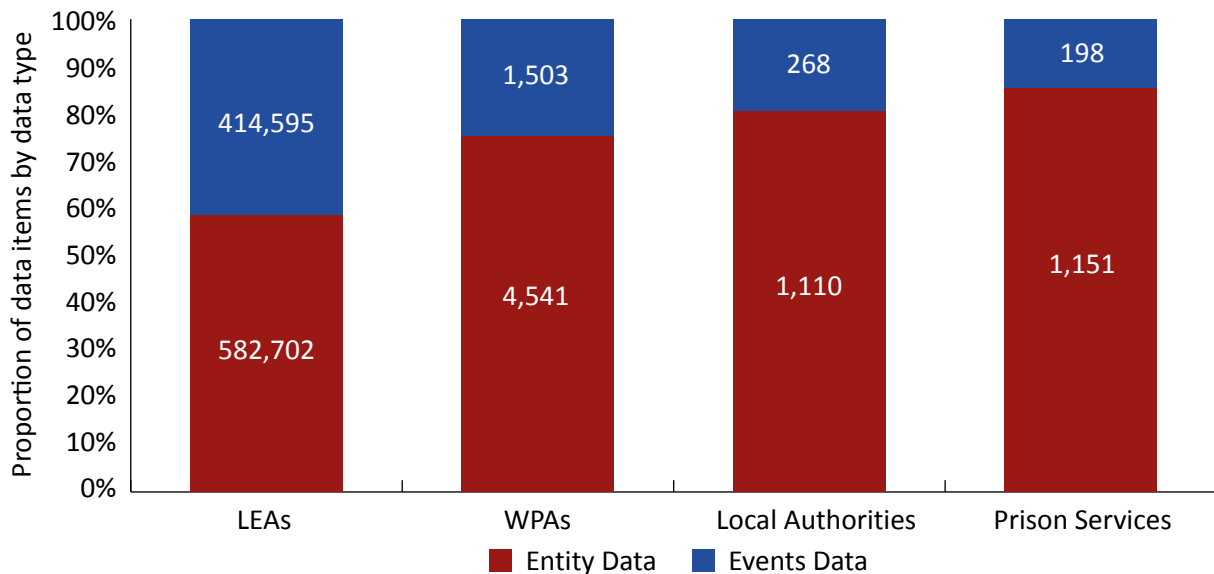
20.35 Figure 20.9 shows the number of authorised applications, where the CD is being sought for an 'applicable crime' purpose, as set out at section 60A(7), 61(7) or 61A(7) of the IPA, against the crime type. As LEAs rely primarily on this statutory purpose, they make up the overwhelming majority of authorisations. Local authorities are limited to what types of crimes they may obtain CD for. Drugs offences are the single largest specified category (29.9%), followed by sexual offences (11.4%) and violence against the person offences (10.2%). The second largest overall are unspecified offences, recorded as 'other', accounting for 13.6% of all CD authorisations under the statutory purpose of preventing and detecting crime.

Figure 20.9 Communications data authorisations by crime type under the 'prevent and detect crime' statutory purpose, 2020



20.36 Figure 20.10 shows the total number of items of CD sought in authorised applications, by whether the items of data were categorised as either 'events' data or 'entity' data, by sector.³⁵

Figure 20.10 Communications data items by data type, 2020



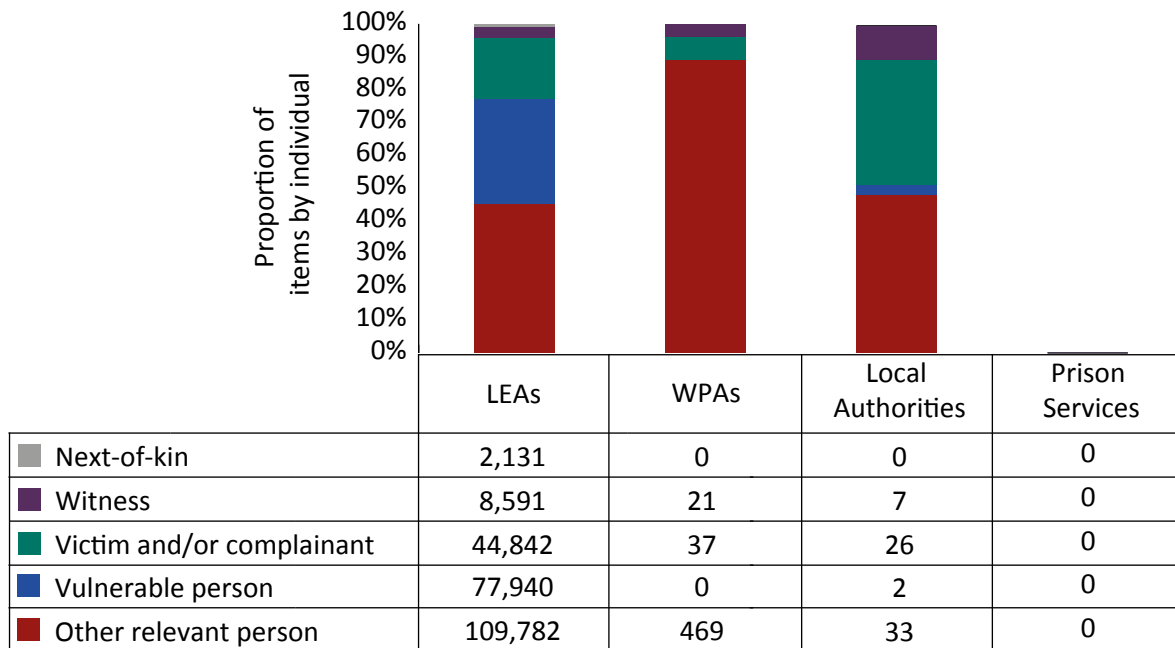
Note:

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

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

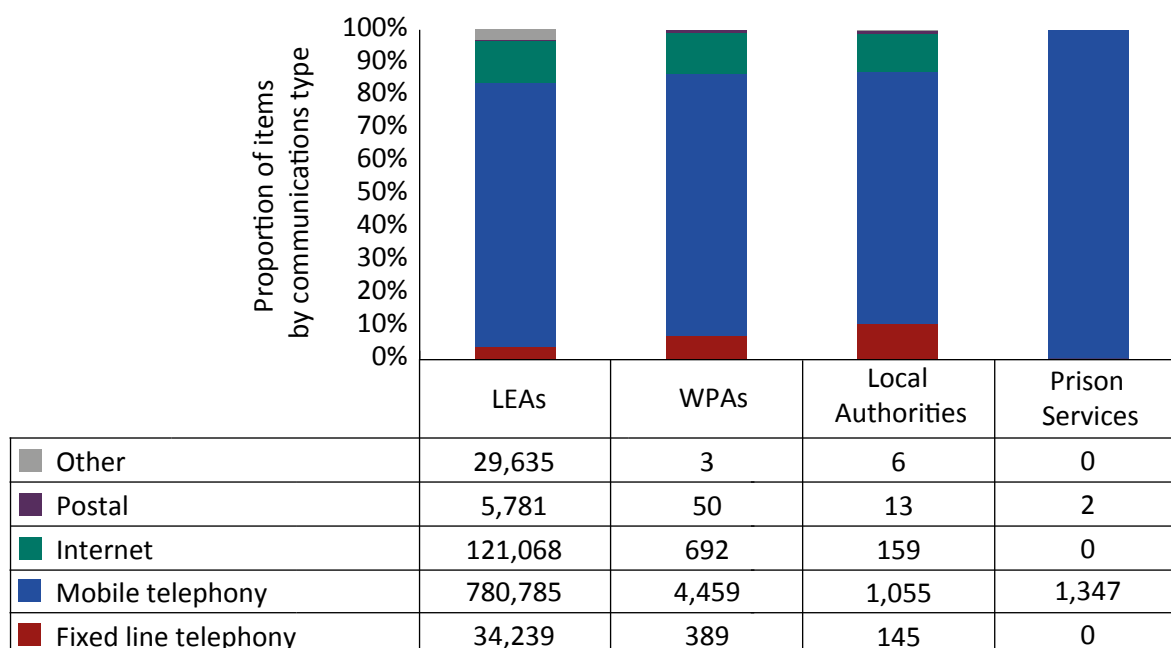
20.37 Figure 20.11 sets out the number of items of CD sought in authorisations, by the subject/s of the authorisation. One authorisation may relate to more than one category of subject. Suspects were overwhelmingly the main subject of CD authorisations at 69.8% of the total.

Figure 20.11 Communications data items by individual (subject), 2020



20.38 Figure 20.12 shows the total number of items of CD sought in authorised applications/notices categorised by the type of data being sought. An authorisation may involve several different data types and multiple items. It should be noted that just because the items of CD data were sought, it does not mean that they were subsequently obtained.

20.39 CD related to mobile telephony continues to be the main form of CD sought, accounting for 79.2% of all items of CD sought in authorisations and with law enforcement being the main sector obtaining such data.

Figure 20.12 Communications data items by communications type, 2020

Office for Communications Data Authorisations (OCDA)

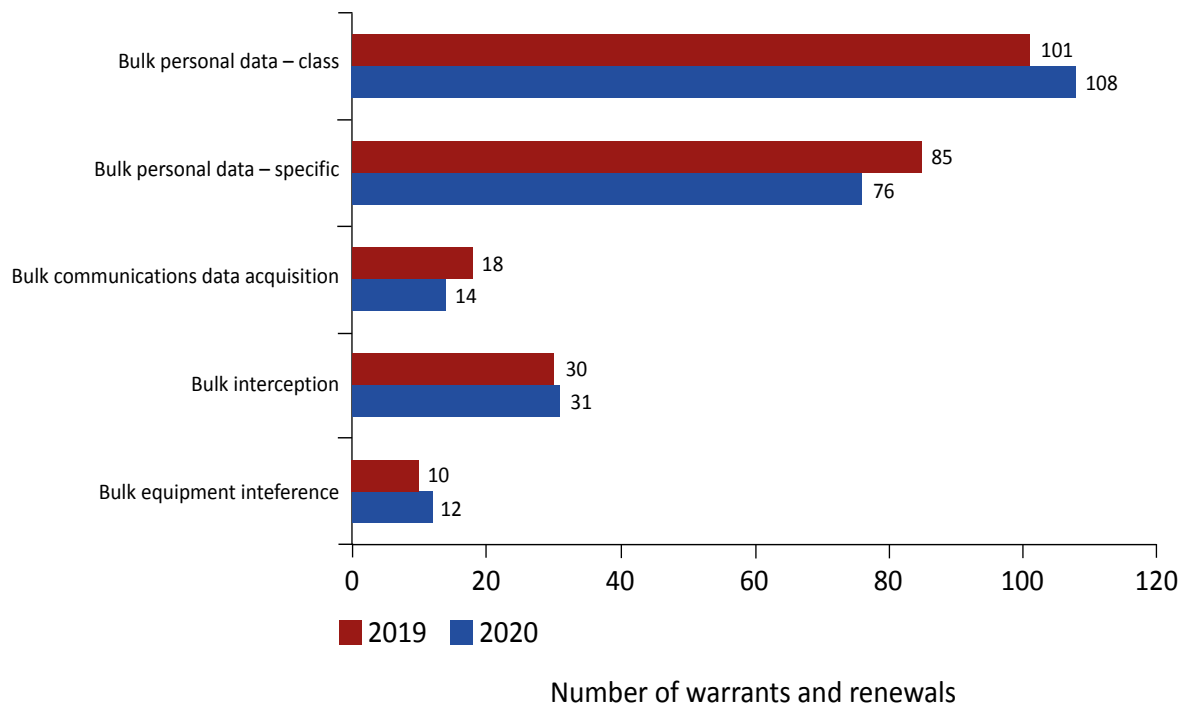
20.40 Table 20.7 sets out the details of volume of applications received by OCDA during 2019 and 2020. It should be noted that the figures are not wholly comparable given OCDA only became functional in March 2019.

Table 20.7 Applications submitted to OCDA, 2019 to 2020

		2019		2020	
Total applications		71,610		226,383	
Decisions made		71,208	99.4%	223,322	98.6%
Of which	Authorised	63,688	88.9%	199,482	88.1%
	Not authorised	7,520	10.5%	23,840	10.5%
Of which	Returned			23,596	10.4%
	Rejected			244	0.1%
Withdrawn		385	0.5%	3,051	1.3%
Applications with no decision at year end (31 December) 2020		17	0.0%	10	0.0%

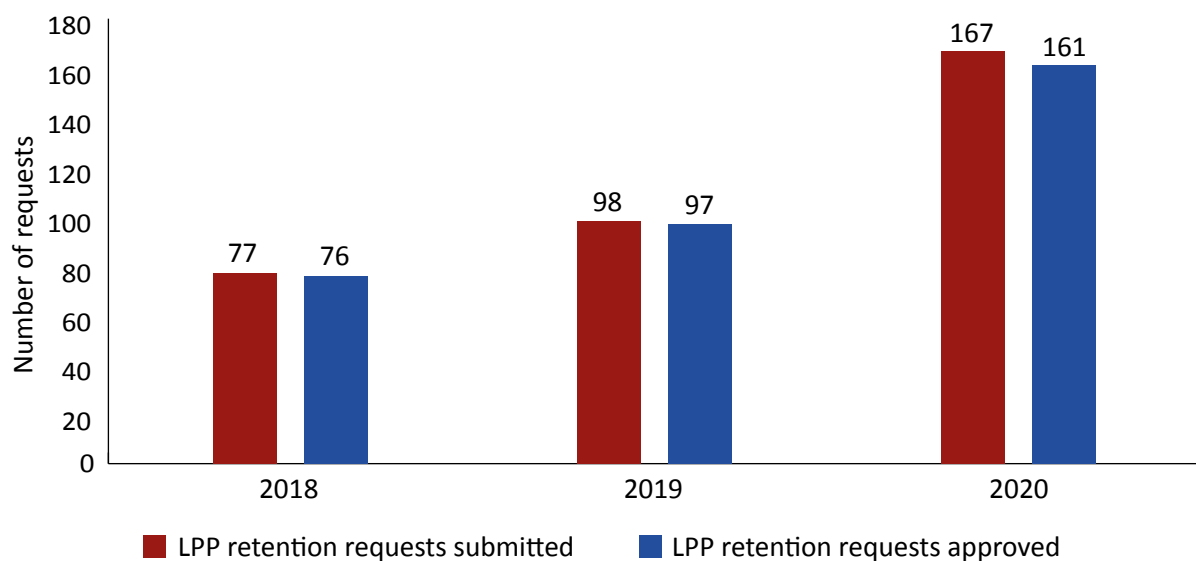
Bulk Powers

20.41 While the underlying capabilities are not new, the IPA introduced specific warrants for bulk collection powers. Bulk warrants are often long standing so the number of applications for new warrants is not a good measure of the level of activity. Figure 20.13 shows the number of new applications and renewals for each class of bulk warrant for 2019 and 2020.

Figure 20.13 Bulk warrants and renewals by type, 2019 to 2020

Legal professional privilege material

20.42 Public authorities must inform IPCO if they think it is necessary to retain LPP material and apply to a JC for permission to retain the LPP material. In 2020, a total of 161 approvals from 167 applications were made. 2020 has seen a significant increase compared to 2019, when 98 applications were submitted and 97 approved, which amounts to a 42% increase in approved applications.

Figure 20.14 Number of requests submitted and approved for LPP material, 2018 to 2020

The Principles

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

Table 20.8 Cases reviewed under The Principles, 2020

Number of cases reviewed		
Cases reviewed on inspection		93
Cases reviewed proactively due to contentious legal or policy issues		
Triggers: Total number of all cases (not limited to those reviewed on inspection)	Personnel knew or believed torture, unlawful killing or extraordinary rendition would occur	8
	Personnel identified a serious risk of torture and submitted for approval despite the presumption not to proceed in such cases	2
	Personnel identified a serious risk of cruel, inhumane or degrading treatment (CIDT) and submitted for approval	15
	Personnel identified a serious risk of rendition and submitted for approval	3
	Personnel identified a real risk of lack of due process and submitted for approval	28

Annex A. Definitions and glossary

This annex is divided into three parts:

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

Definitions

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

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

Term	Definition
Double lock	<p>Public authorities must have authorisation to use the most intrusive investigatory powers. Authorities will therefore submit applications for the use of investigatory powers to a Secretary of State or a senior officer; this decision is then reviewed and authorised by one of our Judicial Commissioners – only with authorisation from one of our Commissioners can a warrant be issued.</p> <p>This is the double lock process. It ensures a two-stage approval for the use of investigatory powers.</p>
Equipment interference	<p>Equipment interference is the process by which an individual's electronic equipment may be interfered with to obtain information or communications. Activity could include remote access to a computer or covertly downloading a mobile phone's contents.</p>
Interception	<p>Interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.</p>
Intrusive surveillance	<p>This is surveillance which is carried out, for example, using eavesdropping devices in residential premises or in private vehicles. It may involve the covert presence of a listening device to capture conversations and ensure that the individual being observed is unaware that surveillance is taking place</p>
Modification	<p>A modification is a change to a warrant authorising the use investigatory powers. It is requested after the warrant has been issued. A modification to a warrant could be, for example, adding an additional individual so that their communications can be lawfully intercepted.</p>
National Security Notice	<p>Under section 252 of the Investigatory Powers Act 2016, a Secretary of State, with approval from a Judicial Commissioner, can issue a National Security Notice to direct a UK telecommunications operator to act in the interests of national security.</p> <p>This covers actions to assist the security and intelligence agencies, which may additionally be authorised under a warrant. National Security Notices could, for example, ask a company to provide access to a particular facility.</p>
Property interference	<p>Property interference is the covert interference with physical property, but also covers wireless telegraphy. This may be for the purpose of conducting a covert search or trespassing on land. For example, police may trespass to covertly install a listening device in a person's house.</p>
Relevant Error	<p>A "relevant error" is an error made by a public authority when carrying out activity overseen by IPCO. A relevant error is defined in section 231(9) of the Investigatory Powers Act.</p>

Term	Definition
Section 7 of the Intelligence Services Act	Section 7 of the Intelligence Services Act 1994 enables the Foreign Secretary to authorise activity by the intelligence agencies outside the UK that would otherwise be unlawful under domestic law.
Serious Error	Section 231(2) of the Investigatory Powers Act defines a serious error as one where significant prejudice or harm has been caused to an individual as a result of a relevant error.
Targeted interception	Targeted interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.
Technical Capability Notice	<p>Under section 253 of the Investigatory Powers Act 2016, the Secretary of State, with approval from a Judicial Commissioner, may issue a Technical Capability Notice to require telecommunications or postal operators to ensure they are able to provide assistance with the acquisition of communications data, interception and equipment interference.</p> <p>After a Technical Capability Notice has been issued and implemented, a company can act quickly and securely when a warrant is authorised.</p>
Thematic Warrants	<p>Thematic warrants are warrants that have more than one subject. There are two types of thematic warrant:</p> <p>The first individually names/describes all the subjects. Any additional subjects can only be added by a "modification" – for law enforcement agencies, a modification requires prior approval by a Judicial Commissioner, or retrospective approval if the modification is urgent.</p> <p>The second does not individually name/describe each subject, because this is not reasonably practicable. For this type of warrant, the authority does not need to add subjects by modification: action may be taken against a person, organisation or piece of equipment (depending on the type of thematic warrant) included within the general description of the subjects.</p>
The Principles	<p>"The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees" are more commonly referred to as "The Principles". These are published by the Cabinet Office and apply to the intelligence services, the National Crime Agency, the Metropolitan Police Service, the Armed Forces and the Ministry of Defence.</p> <p>The Principles are intended to ensure that the treatment of detainees overseas, and the use of intelligence on detainees, is consistent with the UK's human rights and international law obligations.</p> <p>The document seeks to provide clear guidance to staff often operating in legally complex and challenging circumstances. The Principles came into force on 1 January 2020.</p>

Term	Definition
Urgency provisions	<p>Urgency provisions are the conditions under which, due to time-sensitive operational reasons (such as an imminent threat to life), legislation permits a departure from the normal authorisation process. For an investigatory power that typically needs to be subject to the “double lock”, the urgency provisions mean this can be used without a Judicial Commissioner’s approval in advance.</p> <p>If an urgency provision is used, the person who decided to issue a warrant to use the investigatory power must inform a Judicial Commissioner that it has been issued and the power has been used. A Judicial Commissioner must then either:</p> <p>decide whether to approve the decision to issue the warrant and notify the authority of the Judicial Commissioner’s decision; or</p> <p>decide to refuse to approve the decision, in which case activity under the warrant must stop and the Commissioner may direct that any information obtained under the urgent warrant be destroyed.</p>

Further details on the authorisation process for each of these powers can be found on our website.³⁶

Glossary of authorities

Intelligence Agencies	<ul style="list-style-type: none"> • Security Service (MI5) • Secret Intelligence Service (SIS) • Government Communications Headquarters (GCHQ) <p>References to ‘UKIC’ mean the United Kingdom intelligence community.</p>
Defence	Ministry of Defence
Law Enforcement Agencies (LEAs)	<ul style="list-style-type: none"> • All territorial police forces in the UK • All other police forces including the British Transport Police, Ministry of Defence Police, Royal Military Police, Royal Air Force Police, Royal Navy Police, Civil Nuclear Constabulary, Port of Dover Police, Port of Liverpool Police • Her Majesty’s Revenue and Customs (HMRC) • National Crime Agency (NCA) • The Home Office (Border Force and Immigration Enforcement)

³⁶ See: <https://www.ipco.org.uk/investigatory-powers/the-powers/>

<p>Wider Public Authorities (WPAs)</p>	<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, Energy and Industrial Strategy (Insolvency Service) • Department for Levelling Up, Housing and Communities (DLUHC) • Department for Work and Pensions (DWP) • Department for the Economy for Northern Ireland • Department for the Environment, Food and Rural Affairs (DEFRA) • Department for Transport – Air Accidents Investigation Branch (AAIB) • Department for Transport – Driver and Vehicle Standards Agency (DVSA) • Department for Transport – Marine Accident Investigation Branch (MAIB) • Department for Transport – Maritime and Coastguard Agency (MCA) • Department for Transport – Rail Accident Investigation Branch (RAIB) • Environment Agency • Financial Conduct Authority (FCA) • Food Standards Agency • Food Standards Scotland • Gambling Commission • Gangmasters and Labour Abuse Authority (GLAA) • General Pharmaceutical Council • Health and Safety Executive • Health and Social Care Northern Ireland • Her Majesty's Chief Inspector of Education, Children's Services and Skills (OFSTED) • Her Majesty's Prison and Probation Service (HMPPS) • Independent Office for Police Conduct (IOPC) • Information Commissioner's Office (ICO) • Marine Scotland • Maritime Management Organisation • Medicines and Healthcare Products Regulatory Agency
--	---

	<ul style="list-style-type: none"> • National Anti-Fraud Network (NAFN) • National Health Service (NHS) Business Services Authority • National Health Service (NHS) Counter Fraud Authority • Natural Resources Wales • Department of Justice in Northern Ireland (Prison Service for Northern Ireland) • Office of Communications (Ofcom) • Office of the Police Ombudsman for Northern Ireland (PONI) • Police Investigations and Review Commissioner (PIRC) • Prudential Regulation Authority • Royal Mail Group • Scottish Accountant in Bankruptcy • Scottish Criminal Cases Review Commission • Scottish Environmental Protection Agency (SEPA) • Scottish Prison Service • Serious Fraud Office • Social Security Scotland • The Pensions Regulator • Transport Scotland • Welsh Government
Local Authorities	All UK local authorities
Prisons	All prisons in England, Wales, Scotland and Northern Ireland
Fire and Rescue Services	All separately constituted Fire and Rescue services in the UK
Ambulance Services	All UK Ambulance Services

Abbreviations

AA	Automatic acquisition
ACL	Access control levels
AO	Authorising officer
APCC	Association of Police and Crime Commissioners
CAB	Covert Authorities Bureau
CDR	call data records
CFU	Counter Fraud Unit
CIDT	Cruel, inhuman or degrading treatment
CJEU	Court of Justice of the European Union
CMA	Computer Misuse Act 1990
CoP	Code of Practice
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CSP	Communications service provider
DPA	Data Protection Act 1998

DSA	Directed surveillance authorisation
DSO	of Designated Senior Officer
DSU	Dedicated Source Unit
EION	European Intelligence Oversight Network
ERS	Error Reduction Strategy
FIORC	Five Eyes International Oversight Review Council
HMGCC	Her Majesty's Government Communications Centre
ICR	Internet Connection Records
IIOC	indecent images of children
IP	internet protocol
IPA	Investigatory Powers Act 2016
IPAR	Internet Protocol Address Resolutions
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
ISA	Intelligence Services Act 1994
JC	Judicial Commissioner
KET	Knowledge Engagement Team
LPP	Legal professional privilege
MPS	Metropolitan Police Service
NCMEC	National Centre for Missing and Exploited Children
NFC	Near Field Communications
NGO	Non-governmental organisation
NPCC	National Police Chief's Council
NSWG	National Source Working Group
OCDA	Office for Communications Data Authorisations
OpSy	Operational Security Officer
PCC	Police and Crime Commissioner
PIC	Participation in crime
PSI	Prison Service Instruction
PSNI	the Police Service of Northern Ireland
RfRs	Returns for Rework
RIPA	Regulation of Investigatory Powers Act 2000
RIP(S)A	Regulation of Investigatory Powers (Scotland) Act 2000
ROCU	Regional Organised Crime Units
RRD	Retention, review and deletion
S4E	Selection for examination
SIO	Senior Investigating Officer
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
TAP	Technology Advisory Panel

TO	Telecommunications operator
UPCI	The Undercover Policing Inquiry
UTC	Universal co-ordinated time
WGD	Warrant Granting Departments

Annex B. Budget

The table below gives a breakdown of the financial statements for the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) for the financial year 2020/2021.

	IPCO 1/04/2020 – 31/03/2021 Budget Total: £6,401,009	OCDA 1/04/2020 – 31/03/2021 Budget Total: £10m
	2020/21 Full Year End Outturn	2020/21 Full Year End Outturn
Pay costs	£4,972,704	£4,424,233
Travel & subsistence	£52,226	£2,838
Office supplies & services	£18,200	£31,193
Training & recruitment	£23,808	£32,386
Estates	£506,189	£541,103
IT & comms	£234,729	£1,260,189
Legal costs (inc. consultancy)	£12,317	£2,836
Other costs & services	£46,722	£6,860
Capital costs	£448	£986,864
Total	£5,867,343	£7,288,502

The annual budget allocation for IPCO is £6.4million. The vast majority of this is spent on staffing. Pay costs are up on previous years as a number of vacant positions have been filled. Spending in other areas has decreased as a result of the pandemic; this is particularly apparent in our travel and subsistence costs as we have conducted more inspections remotely.

The annual budget allocation for OCDA is £10 million (£8.4 million resource RDEL, £1.6 million capital CDEL).³⁷ As OCDA is still in the expansion stage with staffing levels increasing, pay costs were under budget as OCDA continues to recruit up to its designated headcount. This position is expected to continue until the end of the financial year 2021/22. Travel and subsistence costs were significantly under budget due to the pandemic causing travel to cease for the majority of the financial year. This was offset by a slight increase on office supplies expenditure as OCDA supported staff to work from home with an increase in ergonomic equipment procurement. OCDA utilises a bespoke IT platform to receive applications and the run costs and development of this system is budgeted at £2 million per annum which accounts for the majority of spend relating to IT for both resource and capital.

37 Resource departmental expenditure limits and capital departmental expenditure limits.

Annex C. Serious errors

The following errors were investigated by the Investigatory Powers Commissioner's Office (IPCO) as being potentially serious within the meaning of section 231 of the Investigatory Powers Act 2016 (IPA). Further details on serious errors are given in Chapter 19 and, as noted there, our investigations have included potential errors made by telecommunications operators (TOs).

Error Investigation 1

	Overseas Law Enforcement
Human or Technical:	Technical
Classification:	Time Zone
Data Acquired:	Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>An overseas law enforcement agency provided to the UK data relating to the uploading and sharing of indecent images of children (IIOC). The raw data had no identifiable time zone stamp. Checks with other overseas law enforcement agencies suggested the time zone was in Universal Co-ordinated Time (UTC +0).</p> <p>As the disclosure related to historic transactions using UK IP addresses, immediate action was necessary to secure the customer details as UK TOs are only required to retain communications data (CD) for a period of 12 months.</p> <p>Once the actual time zone was confirmed, IP addresses from UK TOs were acquired and further enquires conducted. Where these investigations identified corroborative intelligence to identify a location from where the images had been uploaded, nine search warrants were executed, and evidence of child sexual abuse was recovered.</p> <p>A further 11 cases did not result in the execution of a search warrant as insufficient corroboration was available to identify the correct location and customer details.</p>
Consequence:	The corroboration measures set out in the National Error Reduction Strategy that IPCO expects to be followed in these cases, identified the deficiencies in the original disclosures and prevented the potential of serious errors occurring.

Error Investigation 2

	Police Force
Human or Technical:	Human (Applicant)
Classification:	Identifier
Data Acquired:	Subscriber information relating to telephone number
Description:	<p>A police force investigating a murder sought to trace the user of a telephone number as a potential witness. The officer making the application mistyped one of the digits when completing the application to acquire CD.</p> <p>As a result, subscriber details were obtained from a TO relating to a similar but incorrect telephone number. An officer made contact with the person listed as the subscriber of the incorrect telephone number and after a short conversation quickly realised the error.</p>
Consequence:	<p>Police contacted an individual unconnected to their investigation.</p> <p>The IPC did not consider the error to be serious, as the effect on the person contacted was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 3

	Police Force
Human or Technical:	Human (3rd Party)
Classification:	Intelligence
Data Acquired:	Subscriber information and trace relating to a telephone number
Description:	<p>A public authority seeking to locate an individual due to concern for their welfare had been provided with a telephone number linked to the patient's record by a local hospital.</p> <p>An application was made to establish the location of the telephone concerned and the subscriber details. A police officer subsequently contacted the number provided by the hospital and established the number was that of a relative.</p> <p>The police located the person for whom concern had been raised and found them to be safe and well.</p>
Consequence:	<p>The police force contacted an individual not directly connected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 4

	Police Force
Human or Technical:	Human (3rd Party)
Classification:	Intelligence
Data Acquired:	Subscriber information and trace relating to a telephone number
Description:	<p>A police force seeking to locate an individual due to concern for their welfare applied for CD relating to a telephone number associated to the person on police records.</p> <p>The details of the subscriber and location of this mobile telephone were obtained. A police officer involved in the search called the telephone number and established it belonged to a next of kin.</p> <p>It transpired the telephone number associated to the police record had been previously provided by a 3rd party (hospital) as that of the individual.</p> <p>The police were able to locate the person for whom concern had been raised who was found to be safe and well.</p>
Consequence:	<p>The police contacted an individual unconnected to their search.</p> <p>The IPC did not consider this to be a serious error as the effect on the person contacted was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 5

	Police Force
Human or Technical:	Human (3rd Party)
Classification:	Intelligence
Data Acquired:	Subscriber information and trace relating to a telephone number
Description:	<p>A police force seeking to locate an individual due to concern for their welfare was provided with what was believed to be two telephone numbers for this person by a local hospital.</p> <p>CD was obtained to identify the location of both numbers that led officers to a house to conduct a welfare visit. On speaking with the occupants, the officer established the number belonged a person with the same name but not the individual concerned.</p> <p>The police subsequently went on to locate the person for whom concern had been raised who was found safe and well.</p>
Consequence:	<p>The police visited an individual unconnected to their search. As the effect on the person contacted was assessed not to have caused significant prejudice or harm the IPC did not consider this to be a serious error.</p>

Error Investigation 6

	Police Force
Human or Technical:	Technical
Classification:	Intelligence
Data Acquired:	Subscriber information relating to Internet Protocol Address Resolutions (IPAR)
Description:	<p>A police force responding to a crime in action identified a suspect through the customer details assigned to an IP address at the time of the offence. This in turn led to the execution of a search warrant and the arrest of the suspect.</p> <p>An examination of devices seized from the suspect at the time of their arrest led officers to suspect there had been a mistake made in the provenance of the original data, and that the person arrested was not connected to the crime being investigated.</p>
Consequence:	The IPC made a determination in accordance with Section 231 of the IPA that a serious error had occurred. The individual was advised of their right to refer the matter to the Investigatory Powers Tribunal.

Error Investigation 7

	Public Authority
Human or Technical:	Human
Classification:	Breach of the Code of Practice
Data Acquired:	Incoming call data
Description:	<p>A public authority was investigating a serious crime.</p> <p>Information pertinent to the investigation led officers to apply for incoming call data upon the published number for a firm of solicitors.</p> <p>The application failed to acknowledge the relevant safeguards for sensitive professions set out in paragraphs 8.8 to 8.11 in the CD Code of Practice. Consequently, the attention of the authorising individual was not drawn to the need to assess whether or not the application carried risk of unintended consequence or served the public interest.</p>
Consequence:	As the effect on the person contacted was assessed not to have caused significant prejudice or harm the IPC did not consider this to be a serious error.

Error Investigation 8

	Police Force
Human or Technical:	Human (Applicant)
Classification:	Intelligence
Data Acquired:	Subscriber information and trace relating to a telephone number
Description:	<p>A police force seeking to locate a person due to concern for their welfare undertook research and identified what was believed to be a telephone number for the individual.</p> <p>CD was acquired to identify the location of the mobile telephone and a police officer made a call to the number.</p> <p>The officer established quickly the called person was not involved and having reviewed the information as a result, it was discovered the person contacted had the same name but was not the individual concerned.</p> <p>The authority subsequently located the person for whom concern had been raised and was found safe and well.</p>
Consequence:	<p>The public authority spoke to an individual unconnected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 9

	Police Force
Human or Technical:	Human (Reporting Person/Receiving Person)
Classification:	Identifier
Data Acquired:	Subscriber information and trace relating to a telephone number
Description:	<p>A 111 call became a medical emergency. The caller hung up and steps to trace where the call was made commenced.</p> <p>The number, when passed to police, was either passed or taken down wrong. Its subscriber was identified, and officers dispatched.</p> <p>When the occupant at the address did not respond, Police confirmed via traces that the phone number was active at the address and woke the occupant. When police established the 111 call had not been made by the occupant a review took place. This review found the actual number had been incorrectly passed or taken down.</p> <p>Once the error had been realised, the corrected subscriber check led another set of officers to a house where the person was located.</p>
Consequence:	<p>The public authority visited the premises of individuals unconnected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm and the original caller to 111 suffered no adverse harm as a result of the delay, the IPC did not consider this to be a serious error.</p>

Error Investigation 10

	Police Force
Human or Technical:	Human
Classification:	Time Zone
Data Acquired:	Subscriber information relating to Internet Protocol Address Resolutions (IPAR)
Description:	<p>A police force investigating online grooming required evidence of the IP addresses being used so that the offenders could be identified and located. In accordance with the National Error Reduction Strategy (ERS) that IPCO expects to be followed in such cases, at least two IP addresses for each investigation were submitted. Both were requested in Universal Co-ordinated Time (UTC +0).</p> <p>The CD returned in response to the application listed two different customers, so in compliance with the ERS, the result was challenged. It transpired the original applicant was unaware of their need to express the activity time in British Summer Time (UTC +1) when BST was prevailing. This led to the IP address connected to the second session activity being out by one hour.</p> <p>In that time the IP address (most of which are not fixed in the UK) had moved to another customer.</p> <p>The requirement to use the prevailing time was discovered.</p> <p>A review of previous requests was conducted and in each both results matched the same customer details.</p>
Consequence:	<p>The submission of an IP address using the wrong activity time can easily result in a serious error and wrongful arrest. In all previous related requests it was clear the internet router involved had retained the same IP across the hour difference.</p> <p>This investigation highlighted the importance of public authorities adhering to the ERS. As this did not lead to significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 11

	Police Force
Human or Technical:	Human (Applicant)
Classification:	Misleading Data
Data Acquired:	Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A public authority was investigating the hacking of social media accounts. Having hacked in, the suspect would demand money. The complexity of the activity led the authority to submit a series of CD applications. Analysis of the results led to certain IP addresses being eliminated. However, one of those eliminated was erroneously added to a request for further CD.</p> <p>The customer details obtained led officers to contact what they believed to be a potential victim.</p> <p>The officer quickly established the customer was not a victim.</p>
Consequence:	<p>The public authority contacted an individual unconnected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 12

	Police Force
Human or Technical:	Human (SPoC)
Classification:	Time Date
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A police force received a National Centre for Missing and Exploited Children (NCMEC) report which identified the use of a UK-based IP address to upload indecent images of children (IIOC). The report provided details of a UK IP address involved.</p> <p>Of note the date of the upload was set out in the US format mm/dd/yyyy.</p> <p>When seeking CD to identify the user of the IP address the date of the upload should have been expressed in the UK format dd/mm/yyyy.</p> <p>Throughout the acquisition process the format was not changed nor the error spotted.</p> <p>A corroborative application was made for an associated email address providing investigators with two different addresses for the same offence. No link between the two addresses could be found.</p> <p>With children resident at both addresses and police concerned for their safety, simultaneous warrants were executed.</p> <p>At the first address devices were seized, and the customer subsequently attended a police station to be interviewed. However, no evidence or material was discovered to believe that this person had been connected to or committed any crimes.</p> <p>With evidence identified in relation to actions taken at the second address, investigating officers suspected an error had occurred.</p> <p>A review quickly found that because of the failure to convert the transaction from the US to the UK format, action had been taken based on the customer assigned the IP on a date in August not July.</p>
Consequence:	The IPC made a determination in accordance with Section 231 of the IPA. The individual was advised of his right to refer the matter to the Investigatory Powers Tribunal.

Error Investigation 13

	Police Force
Human or Technical:	Human (SPoC)
Classification:	Identifier
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A police force received information from a 3rd Party (charity) expressing concern for the welfare of a young person. Details were passed on of the Internet Protocol address connected with their online communication. Once an application for data had been verbally approved, the IP address was copied and pasted into an IT data link used to request CD from TOs, alongside the activity time and date.</p> <p>The customer details obtained led officers to an address unconnected to their welfare visit.</p> <p>A review found that during the copy and pasting process the last digit of the IP address had been left off.</p> <p>The police subsequently located the child for whom concern had been raised and who was found to be safe and well.</p>
Consequence:	<p>The public authority contacted an individual unconnected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 14

	Police Force
Human or Technical:	Human (Historic)
Classification:	Identifier
Data Acquired:	Subscriber information relating to telephone number, trace, and call data
Description:	<p>A police force seeking to locate a person due to concern for their welfare used existing data held on police systems to identify an associated telephone number. After several attempts to contact the number had failed, CD was sought to identify the location of the telephone concerned.</p> <p>Once the application for data had been approved, a trace was about to begin when officers advised contact had been made. The contact established this was the wrong number. The actual number had been entered incorrectly into the information held on the person from a previous incident a number of years before.</p> <p>The police subsequently located the person for whom concern had been raised who was found safe and well.</p>
Consequence:	<p>Police contacted an individual unconnected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 15

	Police Force
Human or Technical:	Technical
Classification:	Identifier
Data Acquired:	Subscriber information relating to a telephone number and trace
Description:	<p>A police force received information from a 3rd Party (charity) expressing concern for the welfare of a young person.</p> <p>No details of the telephone number used to call the charity were available. The police obtained CD to identify incoming calls to the charity over the specific period the relevant call was made. One number was returned.</p> <p>The trace placed the number into another area of the UK. Further CD requests by a police force covering that area led officers to an address. A young person was located who confirmed they had rung the charity. Their reason for calling was at variance to what the charity had been concerned about. This led to all the connected CD being rechecked.</p> <p>The incoming data to the charity over the same period was re-run and a second number, not previously seen, was returned.</p> <p>The correct number was traced, and its user found safe and well.</p> <p>This was a latency issue as often a record of any incoming call can take up to two hours to appear in the call data record.</p>
Consequence:	<p>The public authority contacted an individual unconnected to their search.</p> <p>As the effect on the person contacted was assessed not to have caused significant prejudice or harm, the IPC did not consider this to be a serious error.</p>

Error Investigation 16

	Police Force
Human or Technical:	Human (Applicant)
Classification:	Identifier
Data Acquired:	Subscriber information relating to a telephone number
Description:	<p>A report was made to a public authority of a threat contained in a text over social media. The telephone number associated to the username sending the text was identified and the police sought to identify the user. When making the application, the telephone number was mistyped by one digit. The details returned identified a subscriber living in another area of the UK so the matter was passed to the police force covering that area. Upon receipt of the information, the second police force risk assessed the matter and sent a 'letter to desist' to the named subscriber.</p> <p>Upon receipt, the person receiving the letter made a formal complaint to the police.</p> <p>The matter was investigated, and the error identified.</p>
Consequence:	After some follow up questions by the IPC, the error was not assessed to be serious as the effect on the person contacted was not considered to have caused significant prejudice or harm.

Error Investigation 17

	Telecommunications operator (TO)
Human or Technical:	Human (Disclosure Team)
Classification:	Incorrect Data Supplied
Data Acquired:	Subscriber information relating to telephone number
Description:	<p>A police force investigating the importation of controlled drugs into the UK identified two telephone calls had been made to an address of interest and acquired CD to identify the subscribers of the numbers concerned.</p> <p>One of the results led officers to contact the relative of its subscriber. During the conversation it soon became clear the subscriber was not involved and an error was suspected.</p> <p>With no apparent error in the application the relevant TO was contacted.</p> <p>This review discovered the subscriber details for a completely unrelated number had been provided by the TO in error.</p>
Consequence:	<p>An individual unconnected with the inquiry was questioned but no serious harm resulted.</p> <p>Under Section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.</p>

Error Investigation 18

	Telecommunications operator (TO)
Human or Technical:	Human (Disclosure Team)
Classification:	Incorrect Data Supplied
Data Acquired:	Subscriber information relating to telephone number and trace
Description:	<p>A police force was trying to locate an individual due to concern for their welfare. The reporting person provided the individual's telephone number.</p> <p>Under an urgent verbal authority, subscriber details and a trace on the number was approved. To expedite matters the contact number provided for the customer by the TO was called.</p> <p>When answered this contact confirmed their ownership of the number had ceased in 2018.</p> <p>Subsequent follow up with the TO established the TO had provided details of the previous subscriber and not that of the its current user.</p> <p>While no details of the current owner were known to the TO, the public authority was able to locate the actual individual, who was found to be safe and well.</p>
Consequence:	<p>An individual unconnected with the inquiry was questioned but no serious harm resulted.</p> <p>Under Section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p> <p>In this case no error by the public authority was made.</p>

Error Investigation 19

	Telecommunications operator (TO)
Human or Technical:	Human (Disclosure Team)
Classification:	Incorrect Data Supplied
Data Acquired:	Subscriber information relating to telephone number
Description:	<p>A police force was investigating an online sexual offence that involved the use of an email address. As part of the ERS, to seek further corroboration, the subscriber of a telephone number associated with this email address was obtained.</p> <p>The details led officers to contact the subscriber and established they were not involved.</p> <p>With no apparent error in the application, the relevant TO was contacted.</p> <p>A review by the TO discovered the subscriber details for a completely unrelated number had been provided to the police in error.</p>
Consequence:	<p>An individual unconnected with the inquiry was questioned but no serious harm resulted.</p> <p>Under Section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.</p>

Error Investigation 20

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Misleading Data Supplied
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>Several police forces began receiving NCMEC reports which identified two different IPs as being connected to the same upload of indecent images of children. Closer examination showed them to be supplied by two different providers and used in different locations across the UK so the data could not be relied on.</p> <p>Where conflicting information is identified, the ERS advises the investigation is halted until the issue is resolved or further corroboration is obtained.</p>
Consequence:	<p>This investigation was supported by the National Crime Agency given the TO supplying the data was from overseas and an early circulation to all police forces was sent as soon as the issues were discovered.</p> <p>This investigation highlighted the importance and effectiveness of adherence to the ERS and the principles of check and challenge that ensured no action was taken without further corroboration.</p>

Error Investigation 21

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data Supplied
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A NCMEC report was received by a police force that provided details of an IP address used to upload indecent images of children.</p> <p>The IP address was resolved to the customer and the report advised that these images had been uploaded in 2020.</p> <p>When conducting the final peer review check, the SPoC noted the same IP address appeared later in the report along with a date in 2012.</p> <p>Contact with the TO (overseas) confirmed they had confused the incident time with the time and date it was reported to NCMEC.</p>
Consequence:	<p>Another investigation that highlights the importance and effectiveness of adherence to the ERS and the principles of check and challenge that ensures no action is taken without further corroboration.</p>

Error Investigation 22

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Misleading Data Supplied
Data Acquired:	None Acquired
Description:	<p>A NCMEC report was received by a police force that provided details of an IP address used to upload indecent images of children.</p> <p>The receiving police force became concerned as to the provenance of the time zone in which the activity took place and as a result of these concerns, liaison with the overseas TOs identified an ability for the offender to set the time zone manually.</p> <p>The implications of resolving the IP address using a time manually set by the offender had clear consequences.</p>
Consequence:	This IPCO investigation was supported by the National Crime Agency and the Home Office Knowledge Engagement Team who briefed police forces on a series of corroborative measures that could be taken to mitigate the wrong customer being identified.

Error Investigation 23

	Telecommunications operator (TO)
Human or Technical:	Human
Classification:	Incorrect Data Supplied
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A NCMEC report was received by a police force that provided details of an IP address used to upload indecent images of children.</p> <p>The IP address was resolved to the customer assigned the IP at the time the offence was alleged to have been committed and police attended the address as part of a safeguarding visit.</p> <p>Officers who attended quickly established that nothing was untoward and assessed a possible error in the information supplied.</p> <p>Contact with the overseas TO led to the identification of human error with details of another IP address wrongly associated to the activity.</p> <p>This IPCO investigation was supported by the National Crime Agency and led to the TO introducing an automated reporting tool to remove the need for human involvement.</p>
Consequence:	Under Section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.

Error Investigation 24

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	System
Data Acquired:	Internet Connection Records (ICR)
Description:	<p>An application for CD seeking to acquire internet connections records for a specific period resulted in the TO providing data in excess of that which had been authorised.</p> <p>The subsequent investigation determined the cause was a result of technical configurations and has since been corrected.</p>
Consequence:	Once identified the TO was able to apply fixes to prevent a recurrence.

Error Investigation 25

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	System
Data Acquired:	Subscriber information relating to a telephone number
Description:	<p>A police force was investigating a subject of a Serious Crime Prevention Order. As part of their investigation a request was made for the subscriber details for a certain telephone number.</p> <p>Once the details of the subscriber were returned, police made contact and quickly identified the person was only the subscriber of the number up until 2018.</p> <p>Enquires with the TO involved confirmed these details had been erroneously provided and that the police had mistaken the historic subscriber as the current user of the telephone number.</p> <p>Further investigation revealed the number had been in use as an unregistered prepaid mobile telephone since 2018.</p>
Consequence:	<p>The public authority contacted an individual unconnected to their investigation.</p> <p>This was a hybrid error between the TO and a public authority and was therefore a 'relevant error'.</p> <p>The error was not considered serious by the IPC, as the effect on the person contacted was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 26

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	System
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A police force had obtained details from a TO of a customer based upon an application to acquire CD to identify the user of an IP address. Before its release, and in line with the ERS, the SPoC conducted a Peer Review.</p> <p>The details in the result were compared with those in the application and source of the information.</p> <p>There was concern that the time in the result was now in the wrong time zone and clarification was sought from the TO.</p> <p>The TO did confirm the correct time zone but acknowledged the application process could cause confusion.</p>
Consequence:	<p>The guidance provided to SPoCs acquiring CD on behalf of public authorities was updated and published on the TOs page contained within the national Communications Data Services portal.</p> <p>IPCO was supported in this investigation by the Home Office Knowledge Engagement Team who circulated a national bulletin advising SPoCs of the updates made by the TO.</p>

Error Investigation 27

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	System
Data Acquired:	Location data
Description:	<p>A public authority had obtained details from a TO of a series of call data records including locations. Analysis put one of the numbers in a location at variance to other call data records (CDR).</p> <p>The result was challenged with the TO who undertook an internal investigation.</p> <p>They reported that under certain conditions the CDR could provide the incorrect location.</p> <p>While the circumstances when this could occur were deemed as very rare a decision to brief out the issue was taken and circulated via the national Communications Data Services.</p>
Consequence:	Within a month the TO had fixed the technical issue and the bulletin circulated rescinded.

Error Investigation 28

	Telecommunications operator (TO)
Human or Technical:	Human
Classification:	System
Data Acquired:	Subscriber information and trace relating to a telephone number
Description:	<p>A NCMEC report was received by a police force that provided details of an IP address used to upload indecent images of children.</p> <p>An application to acquire CD was approved and customer details sought from the TO. The data supplied advised the name and address of the customer assigned this IP across the time the activity took place.</p> <p>Officers attended the address and spoke to the occupants and seized for examination five internet enabled devices.</p> <p>Initial triage found nothing incriminating and an error was suspected.</p> <p>No error within the CD application was apparent. When the TO was advised they discovered the wrong house number had been associated to the customer when the account was first set up.</p>
Consequence:	<p>Two individuals unconnected with the inquiry were questioned and had internet enabled devices seized for examination.</p> <p>Under Section 231 (9) of the IPA, the IPC is only able to make a determination if the relevant error is made by a public authority.</p>

Error Investigation 29

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	System
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>The National Crime Agency (NCA) was advised by an overseas TO that the activity time within their NCMEC reports could be out by up to five hours.</p> <p>The error dated back to January 2020 meaning every report this TO supplied to NCMEC was at risk (656).</p> <p>Urgent steps were instigated by the NCA to trace the status of each report.</p> <p>The ERS has long recognised the risk of IP addresses moving between customers. Every shift therefore runs the risk of the customer before or after the activity taking place becoming the suspect.</p> <p>To combat the risk, session times (how long an IP address has stayed with the same customer) has great significance. If the session covers five hours either side of the activity details of the customer involved will be the same.</p> <p>When all cases were examined, in 544 of them the session time covered more than five hours each side of the activity so the information could be relied on.</p> <p>The ERS advises, where possible, to seek corroboration especially when the basis of suspicion rests in the resolution of a single IP address.</p> <p>In the remaining 112 cases, only those where other corroboration existed were put forward for action to be considered and the remainder were quarantined.</p>
Consequence:	Adherence to the ERS prevented action being taken upon persons not involved with the uploading of indecent images of children.

Annex D. Public engagements

The Investigatory Powers Commissioner (IPC) undertook several public engagements in 2020. Details of those engagements are given below.

Meetings with Ministers, MPs and Lords

Date	Meeting
9 July	Rt Hon James Brokenshire MP, Security Minister, Home Office
27 July	Humza Yousaf MSP, Cabinet Secretary for Justice, Scottish Government
12 October	Nick Thomas Symonds MP, Shadow Home Secretary
26 October	Rt Hon Priti Patel MP, Home Secretary
21 December	Lord Falconer of Thoroton and Lord Rosser

Engagement with NGOs and academics

Date	Event
16 January	Meeting with Liberty
3 February	Meeting with Reprieve

Engagement with Public Authorities

Date	Meeting
28 January	Chief Constable Ian Hopkins, Greater Manchester Police
12 February	Prof Paul Wiles, Biometrics Commissioner
24 February	Jonathan Hall QC, Independent Reviewer of Terrorism Legislation
27 February	Lisa Osofsky, Director, Serious Fraud Office
14 October	Masterclass to FCDO staff
28 October	Dame Cressida Dick, Commissioner, Metropolitan Police
10 December	Chief Constable Iain Livingstone, Police Scotland
14 December	Paddy Tipping, Chairman of the Association for Police and Crime Commissioners (APCC) and members of the APCC

Engagements with overseas bodies

Date	Event
20-21 January	International Oversight Working Group (Oslo, Norway). The IPC was represented by a member of the Technology Advisory Panel and an IPCO Inspector
28 May	European Oversight Bodies Conference planning committee
24 July	European Oversight Bodies Conference planning committee

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