IPCO

Investigatory Powers Commissioner's Office

Annual Report

2017

HC 1780

Annual Report of the Investigatory Powers Commissioner 2017

Including pre-September 2017 oversight by the:
Chief Surveillance Commissioner
Intelligence Services Commissioner
Interception of Communications Commissioner

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 31 January 2019

Laid before the Scottish Parliament by the Scottish Ministers 31 January 2019

HC 1780

SG/2019/8

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 978-1-5286-0971-5

CCS0119377508

Printed on paper containing 75% recycled fibre content minimum

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

Contents

Letter to the Prime Minister

The Rt Hon. Theresa May MP
Prime Minister
10 Downing Street
London
SW1A 2AA

December 2018

Dear Prime Minister,

I enclose my first Annual Report covering the work of the three precursor organisations, namely the Office of the Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Intelligence Service Commissioner (IScomm), from 1 January 2017 until 31 August 2017, and the Investigatory Powers Commissioner's Office (IPCO) from 1 September until 31 December 2017.

I have continued the tradition of writing the Report in two parts. The Confidential Annex contains details, including techniques and operational matters, which should not be published for reasons of national security.

It is for you to determine, after consultation with me, how much of this open report should be published without releasing any 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 public authorities subject to my review.

I wish to pay tribute to the fine work undertaken by the three bodies who preceded IPCO and to the last Commissioners who led them: Lord Judge (OSC), Sir Mark Waller, succeeded by Sir John Goldring (IScomm) and Sir Stanley Burnton (IOCCO). They provided the critical foundations for the creation of IPCO and what I hope will be the successful oversight of investigatory powers.

Yours sincerely

The Rt Hon. Lord Justice Fulford
The Investigatory Powers Commissioner

1. Introduction by the Investigatory Powers Commissioner Lord Justice Fulford

1.1 One of my statutory obligations, which I am very pleased to discharge, is to report to the Prime Minister annually about "the carrying out of the functions of the Judicial Commissioners". My Report must address a range of issues, including:

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

1.2 On the surface for 2017 this appears to be a deceptively straightforward task. The reality has been a positive refinement of complication because three quarters of the period (viz. prior to 1 September 2017) relates to the work of our three precursor organisations, the Office of Surveillance Commissioners (Lord Judge), the Intelligence Services Commissioner (Sir John Goldring) and the Interception of Communications Commissioner (Sir Stanley Burnton). In addition, many of the powers contained in the IPA did not come into effect until 2018, and thereby fall outside the ambit of this Report. Otherwise, we have been involved in setting up my new organisation, putting in place the people, infrastructure and systems that have enabled us to function; for instance, with the TAP, although work has been started by that body in 2018, in 2017 we were recruiting its members and beginning the process of applying for their security clearance.

1.3 One of the dominant features of 2017 (extending into 2018) has been the task of unifying these three very different organisations into a single structure. There were marked differences in how they carried out their work, to say nothing of the variety of powers over which they each had oversight. A cursory glance at their annual reports reveals the divergence in style and content as between my predecessor organisations. That is not meant to sound any kind of critical note; to the contrary, the work of each of them was exemplary but fusing their separate, and impressive, legacies into a single, coherent structure has been a formidably challenging task.

1.4 In one sense, therefore, this Preface contains an apology and an excuse. This 2017 Report has undoubted limitations, mainly as a consequence of the difficulties I have just described. Most particularly, it is uneven as regards the content on the different investigative powers and there is a lack of balance between the security services, on the one hand, and the law enforcement agencies, on the other. This is particularly evident because we have structured the Report around the different types of investigatory powers, in part to reflect the unified approach to oversight that is to be adopted. Although our inspectors have different areas of expertise, we will ensure the boundaries between the three precursor organisations are not replicated within IPCO.

1.5 In what follows, we have attempted to provide relevant background information and a summary description of each of the powers.

1.6 Although there was some concern as to whether IPCO would be ready to begin operating on 1 September 2017, and whether we would delay the security and law enforcement agencies in their work, I am confident that on our record to date we have dispelled those anxieties. I have received no complaints that the applications for warrants have been handled inefficiently, and we have complied with – indeed, we routinely and significantly exceed – the agreement as to the length of time the Judicial Commissioners will take to resolve the applications. There has been no suggestion that the arrival of IPCO has hampered the law enforcement and security agencies in their work and I am delighted at the arms-length but cooperative relationship that has been developed with all the organisations for which we have oversight responsibility. I am very grateful for the generous approach of all and the considerable assistance that was provided in helping set up this new organisation. The Home Office, the Foreign Office, the Security Services and all the law enforcement agencies have been highly co-operative. The practical and administrative support, along with the many extremely effective briefings that were laid on for the Judicial Commissioners and our staff, have been time consuming for those involved in providing this help and of incalculable benefit to IPCO.

1.7 Although in 2017 I was principally focused on meeting the domestic public authorities who utilise investigatory powers, during October I led a team from IPCO to the 'Five-Eyes' Conference in Ottawa in Canada (the United Kingdom, the United States, Australia, Canada and New Zealand), which was an extremely useful first step in establishing what I hope will be a lasting and mutually supportive relationship between the Oversight Bodies in our closely-allied countries. I gave a speech in Washington at the Centre for a New American Security. I visited the Foreign Intelligence Surveillance Court and I met with various representatives of the American intelligence Community, including the Office of the Director of National Intelligence and the Department of Justice. In November I visited the Dutch Oversight Body (CTIVD), as the first instalment in a series of meetings with the oversight bodies of EU countries.

1.8 It has been during 2018 that my engagement with international bodies, the media and civil society has developed but it is to be noted that we involved key representatives from civil society in the induction and training programme for the Judicial Commissioners in November 2017.

1.9 Overall, I have been extremely pleased at what IPCO achieved in 2017, and I am cautiously optimistic that, with the considerable assistance of others, we laid foundations for the successful oversight of investigatory powers in the years to come.

2. IPA Implementation and the Establishment of IPCO

2.1 I was appointed the first Investigatory Powers Commissioner (IPC) on 27 February 2017. My immediate focus was on setting up the office – the 'Investigatory Powers Commissioner's Office' or 'IPCO' – and recruiting Judicial Commissioners, Inspectors and the diverse other members of staff needed for us to operate effectively. IPCO did not come into existence until 1 September 2017 when I inherited all the oversight powers and responsibilities of the three precursor bodies, the Office of the Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Intelligence Service Commissioner (IComm) I also took on substantial additional responsibilities, the principal of which is the 'double-lock' function (as explained hereafter). This report focuses on the oversight carried out during 2017 and, as set out above, unavoidably covers a period of eight months before I took over responsibility. Naturally there will be variation in how the three different bodies carried out their duties and recorded their findings and, as a consequence, there is some unevenness in what I am able to address in this Report. There is inevitably reference to some events that have taken place during 2018.

2.2 In this chapter I seek to set out the decisions we have taken to establish IPCO, and the principles that have guided them.

Guiding principles

2.3 There are five principles underpinning the decisions I have taken, and the plans and processes that have been put in place, which I believe are vital to effective oversight. These principles are:

- **Independence:** everyone who works at IPCO must be fearlessly independent, unstintingly fair in their approach and beyond reproach as regards their integrity, ethics and honesty.
- **The law:** IPCO has a clearly defined statutory role given to us by Parliament. We must discharge that function rigorously and impartially, wherever that leads us.
- **Transparency:** in the post-Snowden world, the security and law enforcement agencies can no longer expect to work in the shadows, in the sense that material which can properly be made public should be widely available for scrutiny.
- **Engagement:** we should engage with all those who have a legitimate interest in what we do, including the NGOs, civil society and academics.
- **Security:** I will strive to ensure that my office is not the source of the improper disclosure of any secret or personal information.

Designing IPCO

2.4 The work designing IPCO was started by a number of Home Office officials before my appointment. I am extremely grateful for the extensive and robust underpinnings that were then provided; whilst we have made various changes to this initial work in the light of experience, the core structure of IPCO remains as it was originally envisaged. There are three delivery functions and three complementary supporting functions. All these components need to be in place and properly resourced for IPCO to run efficiently and effectively.

2.5 The delivery functions are:

- The judicial review of the use by public authorities of their investigatory powers. This work is carried out by 15 Judicial Commissioners ('Commissioners' or 'JCs'), assisted by a team of officials who manage and run the review process;
- The inspections of the use by public authorities of their investigatory powers. In the future, a number of JCs will lead this work, which is carried out primarily by a team of IPCO inspectors; and
- Engagement with the Government, Parliament, international partners, civil society, academia and the media, in order to explain IPCO's role and how we carry out our responsibilities. This work will be run by a small engagement team once they are in post, but last year it fell primarily to the Interim Chief Executive and myself, with the considerable support of an inspector who agreed to lead on this function.

2.6 The support functions are:

- Technological advice to those in IPCO performing our oversight function, namely the JCs when considering applications for warrants and the inspectorate when investigating post-facto compliance. In the main, this is provided by the Technology Advisory Panel (TAP), although I hope there will be a permanent member of staff who will assist in this area;
- Legal advice to the Commissioners and Inspectors. This is provided by a small legal team, supported by our standing counsel; and
- Administrative and secretariat support. This is provided by officials in the secretariat and the review team.

2.7 Our focus since September 2017 has centrally been on setting up the processes which will ensure the efficient judicial review of applications for warrants. Once the Investigatory Powers Act 2016 (the Act) is fully in force, we expect the review team to receive about twelve thousand applications a year, through a number of different IT systems, some of which are antiquated and extremely unreliable. The JCs have undergone a detailed and substantial induction programme to ensure they are familiar with the relevant technology and operational techniques. They have received presentations by Government and civil society on the necessity and proportionality of a range of the investigative opportunities that are used by the law enforcement and intelligence agencies.

2.8 During the course of a number of 'judicial seminars', the Commissioners have considered, in some significant detail, a number of the legal issues which will be of particular importance to the applications for warrants. This exercise was begun well ahead of the commencement of the specific investigatory powers, so as to ensure that our expectations of the public authorities were well understood and to give ample time for the agencies to make any necessary changes to their processes in order to ensure compliance with the Act.

I considered that it was in the public interest to resolve as many potential difficulties as possible before commencement of the main elements of the Act. I will report on the effectiveness of this approach in the next annual report.

The IPCO approach

2.9 As already indicated, the two most important early priorities were establishing the IPCO team and the processes that will enable the Commissioners to consider the applications for warrants. These have both been very substantial undertakings but, subject still to the appointment of some key staff, they are now essentially – and, I suggest, successfully – complete. Our focus for the next stage will be on creating the most effective possible inspection regime across the entirety of the many bodies for which we have responsibility, bearing in mind that IPCO is, in one sense, the result of a merger of three very distinct precursor organisations. We have recently started the work that will be necessary to unify our approach to inspections. Indeed, some months ago we instituted inspections across the former operational boundaries to ensure that we apply consistent standards to the authorities we oversee. Inspections of the intelligence agencies have already changed fundamentally. Previously they were inspected by the Intelligence Services Commissioner, accompanied by a member of his staff. Since early 2017, when the IOCC and ISComm offices were brought together under one Head of Office (in effect, the Chief Executive), two inspectors, directed by the relevant Commissioner (my Deputy, Sir John Goldring), have been conducting inspections focussing on six themes:

- S.7 Intelligence Services Act 1994 (ISA) and the Consolidated Guidance
- Property Interference and Intrusive Surveillance;
- Directed Surveillance and Covert Human Intelligence Sources;
- Communications Data and Bulk Communications Data;
- Bulk Personal Data; and
- Interception.

2.10 The Commissioners will regularly attend part or all of these inspections, and oversee the work of the inspectors, and I am firmly of the view that the new model has given us greater flexibility and reach than under the previous approach. We plan to expand the cadre of inspectors assisting with intelligence work. My understanding is that the agencies recognise and accept the benefits of these changes to the inspection regime.

2.11 There is a strong symbiotic connection between the ex post facto inspections we conduct and the Commissioners' judicial review function. It is of note that for countries with broadly equivalent oversight bodies, while some combine the oversight and review function in one body, many have divided them between separate organisations. This latter approach is favoured by many in civil society. My strong view is that having responsibility for both elements makes my overall oversight of the intelligence and law enforcement agencies significantly more effective than would be achieved by two separate bodies. The Commissioners are able to identify areas which merit particular scrutiny on inspection, and the inspectors are well placed to inform the JCs of the issues of relevance to future applications for warrants that were identified on inspections. The Government, as a result of this regime, needs to engage with IPCO on an extensive range of issues which are identified on inspections, to ensure effective compliance before the Commissioners are asked to approve applications. IPCO's ability to analyse the circumstances surrounding and relevant to warrants during inspections means that it is reasonable to include less background material in the applications than is sometimes seen in jurisdictions where the two functions have been separated. For example,

applications in the United States Intelligence and Surveillance Court (FISA) can easily run to 50 or more pages. Applications under the Act will rarely be more than 10. Throughout this extensive period of change, and with significantly less than a full complement, the inspectors have been working extremely hard to deliver reports that are uniformly of an exceptionally high standard. I am grateful for their dedication and commitment.

2.12 Although they have been recruited and appointed, the engagement team is not yet in place (see the section on resources below). Nonetheless, we have done all we can to engage with our external stakeholders, and in particular we have liaised with a number of NGOs and some academics. These discussions with civil society have been notably instructive, and they have contributed to the approach IPCO adopts when scrutinising the Government's activity. For obvious security reasons it will not always be possible for members of civil society to be briefed in full (or, on occasion, at all) on the Government's capabilities and operations, but it is my ambition that IPCO will act as a bridge, ensuring that valid concerns can be highlighted for the officers and analysts conducting intrusive activity.

2.13 We are also working closely with a number of foreign oversight bodies. We want to understand how they handle similar challenges and to explore with them whether there are any areas in which we can properly provide joint oversight. We have extensively shared ideas with a number of external oversight bodies, and I would especially like to thank Canada, the USA, the Netherlands, Germany and France who hosted me or other representatives of IPCO during 2017. In a similar vein, we have arranged meetings at our London office for visiting representatives of external oversight bodies.

2.14 We have appointed the Chair of the Technology Advisory Panel and our Standing Counsel: respectively, Professor Sir Bernard Silverman and Tom Hickman. I consider it critical that the Commissioners and inspectors have comprehensive technical and legal support, in what can be a very challenging, specialised and complex area. Over the next year, Sir Bernard and I may appoint additional panel members to the TAP, which has already provided invaluable assistance to the Commissioners and the inspectors. I pay tribute to Tom Hickman for the varied and high quality advice he has given the organisation, often at very short notice.

2.15 The small and, I strongly suspect, significantly under-resourced legal and policy team has produced a wealth of first-rate reports and advice on a broad range of issues, and I have been struck at the extent to which this industrious body of people has managed to cover so much ground.

2.16 Finally, the secretariat and review teams have been highly efficient during our first year. They have successfully set up our new offices; they have run dozens of recruitment competitions, resulting in hundreds of applicants; and they have supported the entire organisation during this period of development and change, notwithstanding long periods of being significantly under resourced. I cannot sufficiently express my thanks for the excellent assistance I have received.

Resources

2.17 Predicting the right structure and headcount for a new organisation is always likely to be difficult. This has been a particularly vexed question for IPCO given the new responsibilities with which we have been entrusted, in addition to the existing work of our precursor organisations. I am reasonably confident that we have identified right number of Judicial Commissioners (16 including myself). However, only time will tell whether we have accurately predicted the correct number of inspectors and other members of staff who are critical to ensuring IPCO fulfils Parliament's ambitions, as reflected in the IPA. Whilst I appreciate

the current pressure on public finances, I am concerned that we may have insufficiently resourced both the inspectorate and our numerically-small legal and policy team. Once we have a full complement of staff and implementation of the Act is complete, we will then be able to judge whether the original predictions were awry. The Home Office has agreed that our staffing levels need to be kept under careful review and may need adjustment.

2.18 Finally on resources, I respectfully endorse the observation of the last Chief Surveillance Commissioner, Lord Judge, in his 2016 Annual Report that "the pace of [recruitment] is alarmingly slow", and to this I add my deep anxiety as to time taken by the vetting and security clearance process. This is a problem experienced across government but as a result of the notably slow progress – this regularly takes well in excess of nine months – a significant number of posts in the office remained vacant throughout 2017 and this bleak picture has continued to date. Some extremely well-qualified candidates have accepted other positions because the wait became excessive. This has placed a significant and undue burden on the staff currently in post, and I can only thank them for their considerable forbearance.

Areas that might benefit from oversight by IPCO

2.19 Based on our early work, it appears that there may be some inconsistencies in where the double-lock or my oversight responsibilities currently fall. Intrusive surveillance conducted by the intelligence services, the MOD and HM Forces, along with CHIS operations, fall outside the regime of the double lock, albeit they have the potential to be significantly invasive.

2.20 In a similar vein, some areas of Government or local authority activity are either not explicitly expressed to be within my oversight remit or clearly fall outside it. Some of these activities will be overseen by IPCO because of the 'proportionality' consideration when Commissioners grant or refuse applications for warrants, but there is no concomitant express mandate on me to conduct ex post facto oversight. I have set out a few examples of these potential gaps below:

- **The 'Overseas Security and Justice Assistance' (OSJA) process.** This is the mechanism by which public authorities assess the Human Rights and other implications of cooperative relationships with organisations in other countries. This activity seemingly falls, arguably inconsistently, outside of my mandate.

- **Facial recognition.** There has been some recent controversy regarding the use of facial software by police forces. I oversee any conduct that requires surveillance authorisation, but neither Parliament nor the courts have yet established a framework against which to judge this particular activity.

- **Surveillance activity conducted by Local Authorities in Northern Ireland.** Whilst the Regulation of Investigatory Powers Act 2000 provides for an Investigatory Powers Commissioner for Northern Ireland, the post remains vacant and the oversight of Local Authorities is outside of my remit, with the effect that they operate without any external scrutiny.

2.21 It is entirely a matter for the Prime Minister and the government to decide whether it is in the public interest for areas such as these to be placed under the double lock or as coming within IPCO's oversight. And it is for the government to decide on the framework within which any such oversight is to be exercised. I simply highlight the **argument** that there is currently insufficient regulation of these areas and that this could be resolved through their designation as part of IPCO's double-lock and ex post facto oversight responsibilities.

3. Covert Human Intelligence Sources (CHIS)

Description of powers and use

3.1 Individuals act as a covert human intelligence sources (CHIS) if they i) establish or maintain a relationship with another person to obtain information covertly, ii) give access to information to another person, or iii) disclose information covertly which they have obtained using the relationship or they have obtained because the relationship exists. The role of a CHIS also includes undercover work such as using a public authority employee or a person holding an office, rank or position in a law enforcement agency to act as an undercover officer (UC). In practice, CHIS are used to tackle a huge variety of offences and to gather intelligence in both the real and virtual world, from burglary and supplying drugs through to complex investigations into human trafficking, child sexual exploitation and domestic and international terrorism. If a law enforcement agency uses an undercover officer they are called a 'relevant source' and additional oversight controls apply.

3.2 The Regulation of Investigatory Powers Act 2000 (RIPA) Part II governs the use of CHIS by the intelligence agencies, law enforcement agencies (LEAs) and other public authorities in the UK. The Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) governs the use of CHIS by public authorities in Scotland. Outside the UK, s.7 of the Intelligence Services Act 1994 applies, and the activity is often referred to as agent running. The Secretary of State approves all s.7 authorisations. Many public authorities conduct human intelligence source activity online.[1]

3.3 Those public authorities that are entitled to authorise CHIS are detailed in Part 1 of Schedule 1 RIPA.[2] These include police forces, law enforcement agencies such as the NCA, HMRC, the intelligence services, the armed forces, other government departments, regulators such as the Financial Conduct Authority and local authorities.

3.4 The intelligence and law enforcement agencies can use CHIS in fulfilling their statutory functions, including preventing or detecting crime and protecting the interests of national security. Other public authorities have a more limited range of statutory purposes available to them, reflecting their more specific functions.[3]

3.5 Using CHIS powers presents considerable challenges to public authorities. They need to consider carefully (i) the complex welfare and safety issues for the CHIS and his or her family; (ii) the proportionality of the activity to be undertaken; (iii) managing the safety

1 The code of practice advises public authorities to seek RIPA authorisations where available under the act for any overseas operations where the subject is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material being used in evidence before a UK court.
All MOD human intelligence-source running currently takes place outside the UK and does not have a UK connection (as described in the code of conduct). The MOD does not, therefore, require CHIS authorisations under RIPA but they choose to follow the guidance in RIPA when authorising and conducting human intelligence source activity.

2 http://www.legislation.gov.uk/ukpga/2000/23/schedule/1

3 http://www.legislation.gov.uk/uksi/2010/521/pdfs/uksi_20100521_en.pdf

of members of public acting on their behalf; (iv) the reliability of the CHIS and whether corroborating material should be obtained; and (v) any financial payments to the CHIS.

3.6 Using CHIS can be contentious. There has been a significant debate about the propriety of inducing individuals to provide intelligence or evidence in circumstances when many would expect, or hope, that the public would simply volunteer their knowledge of criminal activity. There has also been significant public disquiet at suggested incidents of impropriety by some undercover police officers. The Undercover Policing Inquiry for England and Wales, chaired by a former High Court Judge, Sir John Mitting, will report on undercover police operations conducted by English and Welsh police forces since 1968. IPCO will provide all possible assistance to the Inquiry.

3.7 Her Majesty's Inspectorate of Constabulary in Scotland (HMICS) conducted a Strategic Review of Undercover Policing in Scotland which we assisted. The review did not find any of the disputed practices that are the principal focus of the UCP Inquiry. It did, however, make a number of recommendations aimed at improving Police Scotland's capability, training and governance structures. The Force accepted all the recommendations.[4]

3.8 CHIS participation in criminality may also be seen as controversial. It is considered that to be effective sources of intelligence and to protect their identity, CHIS may need to participate in crime, for example by joining a proscribed organisation. This activity, together with the justifications advanced for it, will be a particular focus of attention for the IPC over the next 12 months.

Statistics on the use of these powers

3.9 The previous annual report of the Chief Surveillance Commissioner reported statistics for the financial year 2016-2017. During the present transition period we have collected statistics for the subsequent three quarters covering 1 April to 31 December 2017. In the analysis that follows, when it is helpful to facilitate comparisons with previous years, we have given an 'annualised' figure.[5]

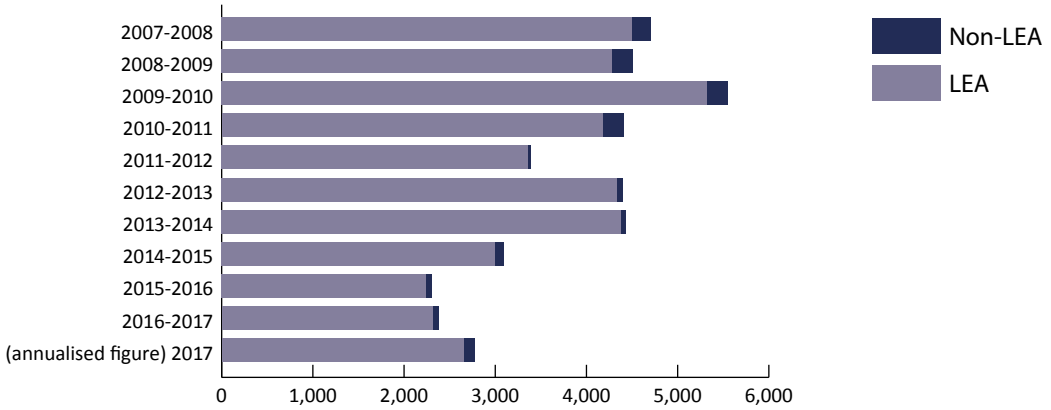
3.10 There were 2,080 CHIS authorisations (excluding relevant sources) by LEAs, local authorities and other public authorities (OPAs, such as government regulators) for the period 1 April to 31 December 2017. On an 'annualised' basis, that represents 2,773 authorisations compared to 2,386[6] for the 2016-2017 period, as reported by the OSC. This may be greater than recent numbers but it remains significantly lower than the 4,000 plus annual CHIS authorisations commonly reported prior to 2014.

4 https://www.hmics.scot/publications/strategic-review-undercover-policing-scotland

5 Individual public authorities provided figures to the OSC for the first quarter of 2017 in the form of a consolidated twelve-month financial year figure (01/04/16–31/03/17). It is impossible to separate these figures from the statistics as previously gathered. Therefore, to give comparable annual totals we have simply multiplied the total for the three quarterly periods 01/04/17–31/12/17 by 133%, to make it – albeit to an extent artificially – equivalent to four quarters. This is, therefore, only indicative of the whole of 2017 and cannot be relied upon as a precise figure.

6 LEAs, local authorities and OPAs

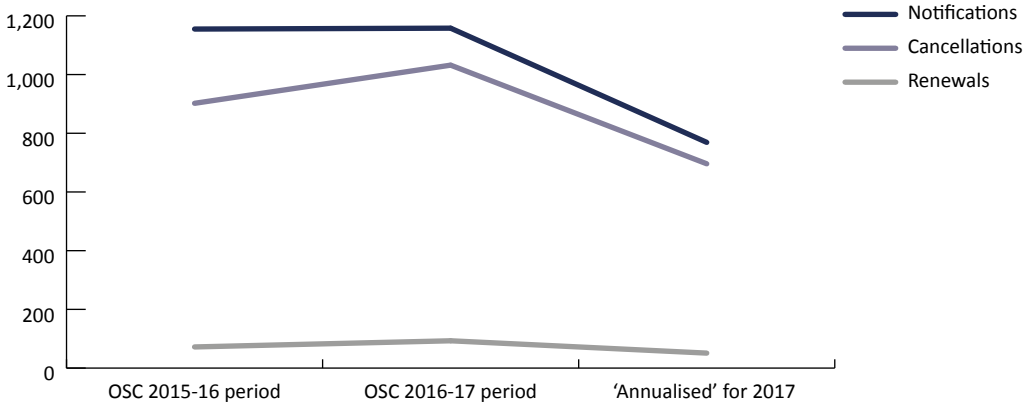
Fig. 1 CHIS Authorisations over the last 10 years (excluding UKIC and relevant sources)



3.11 At the end of 2017, there were 2,281 extant CHIS authorisations, which is very similar to the 2,229 last reported by the OSC (31/03/2017).

3.12 Whilst almost all law enforcement agencies used their CHIS powers during April to December 2017, only 5% of non-law enforcement agencies (excluding intelligence agencies) reported using their CHIS powers, albeit those bodies represented a wide variety of government departments and local authorities.

Fig. 2 Relevant Source notifications, renewals and cancellations



3.13 There has been marked decline in the number of Relevant Source notifications and renewals compared with the two previous 12-month periods reported by the OSC.[7] During the period 01/04/17–31/12/17 there were 577 notifications, 38 renewals and 522 cancellations ('Annualised' 769 notifications, 51 renewals and 696 cancellations). It is too early to comment as to whether this indicates a trend and, if that is the case, the reasons for it.

7 However, as these statistics represent the number of times an individual undercover officer has been authorised for a specific operation, they do not necessarily reflect the number of such operations as one operation may require the deployment of a number of undercover officers.

The Authorisation Process

3.14 Often CHIS relationships start after a referral. This might be, for instance, when someone indicates they have information of possible use to a public authority or when a public authority identifies that an individual may be of assistance. Before deciding whether someone is suitable to be a CHIS – certainly before making an approach – public authorities should consider a number of issues, including the potential value of any likely intelligence weighed against possible vulnerabilities such as mental health concerns, drug use or age.

3.15 A senior manager,[8] for example a superintendent in the police, must authorise a CHIS relationship before this step can be taken. The authorising officer (AO) acts in a quasi judicial role when considering such requests. They must be impartial and, wherever possible, separate from the investigation itself. The AO can seek relevant information or legal advice, but the decision whether or not to grant an authorisation is for them alone. By way of an exception, when the CHIS is a vulnerable individual or juvenile, the request must be authorised at more a senior level.

3.16 The CHIS code of practice provides particular safeguards for legally privileged and other categories of sensitive material, for instance when there is a higher expectation of privacy or confidentiality such as parliamentary, journalistic, medical or spiritual information. For the intelligence agencies, when the CHIS deployment is intended to facilitate obtaining, providing access to or disclosing material which is subject to legal privilege, the authorising officer must request written approval in advance from the Secretary of State. For LEAs and OPAs a higher level of authorisations, such as by a Chief Constable, must be obtained when privileged or confidential information is likely to be acquired.

3.17 Local Authorities in England and Wales can only use CHIS in accordance with The Protection of Freedoms Act 2012 and Statutory Instrument 2012/1500, which require a magistrate to approve the deployment. The proposed activity must be shown to be necessary for the prevention or detection of a crime which carries a minimum sentence of six months' imprisonment, or because it relates to an offence of selling alcohol or tobacco products to minors.

3.18 In Scotland, where RIPSA applies, local authorities are not restricted by The Protection of Freedoms Act 2012 when they use CHIS, and they may authorise this activity on the grounds of prevention or detection of crime or preventing disorder, and in the interests of public safety and public health. In Northern Ireland local authorities also use these powers but IPCO does not have oversight as to how they use them (see the section on findings below).

3.19 A CHIS authorisation is valid for 12 months, except for juvenile CHIS which were valid for one month during the period covered by this report[9] unless renewed. In urgent situations, public authorities can apply for an oral authorisation which is valid for only 72 hours, after which the normal written process must be followed.

3.20 Within the public authority there will be a 'handler' who has day-to-day responsibility for dealing with the source on behalf of the authority and for the source's security and welfare. Another individual within the public authority, known as the 'controller', will have general oversight of the use made of the source. A risk assessment will be produced which covers

8 The specific role or ranks are prescribed in The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010/521.

9 now four months.

how the CHIS engages with the organisation, how their intelligence is used or disseminated, the specific tasking and the way this affects the CHIS's exposure to risk.

3.21 The AO must review a CHIS regularly during the lifetime of an authorisation, to assess whether the authorisation is still justified on the grounds that it remains necessary and proportionate. This review must take account of the risk assessment. Authorisations, therefore, can be renewed when it is necessary and proportionate, or cancelled when no longer necessary.

3.22 The authorisation and use of CHIS is a challenging activity and there is significant responsibility on the authorising body to manage CHIS properly. This begins before the CHIS is recruited and continues well beyond the end of the authorisation. It follows that public authorities need robust management processes and sufficient resources in place, with appropriately trained personnel, to be able effectively to manage CHIS.

3.23 Local Authorities in England and Wales can only use CHIS in accordance with the Protection of Freedoms Act 2012 and Statutory Instrument 2012/1500, which require a magistrate to approve the deployment. The proposed activity must be shown to be necessary for the prevention or detection of a crime which carries a minimum sentence of six months' imprisonment, or because it relates to an offence of selling alcohol or tobacco products to minors.

How IPCO oversees these powers

3.24 By way of overall approach, we inspect CHIS and surveillance activity at a single inspection, during which between one and several inspectors will attend for up to a week, depending on the size of the authority and the extent to which the powers were utilised. For the intelligence agencies and the MOD, we inspected CHIS use at our main inspections in the spring and autumn of 2017. For LEAs we conducted 59 inspections during 2017.

3.25 As a generality, we now aim to inspect each council in England, Wales and Scotland once every three years. We inspected 103 local authorities in 2017.[10] But whenever necessary, we will conduct an interim or follow-up inspection if the local authority's compliance is poor or during a period of change when an earlier visit is likely to have utility. We also inspected 11 Fire and Rescue Services.[11] Eight of these inspections were on site and three were desktop inspections. In addition we inspected 20 other public authorities (e.g. government regulators); these were all on-site inspections.

3.26 We also inspected 11 Fire and Rescue Services.[12] Eight of these inspections were on site and three were desktop inspections. In addition we inspected 20 other public authorities (e.g. government regulators); these were all on-site inspections.

3.27 During on-site inspections of a public authority, IPCO will scrutinise the CHIS documentation in order to assess all the relevant aspects of the process of authorising and running the CHIS. This will inevitably include the recruitment process and we will consider, amongst other things, the number of times the public authority met or contacted a potential CHIS recruit and whether he or she provided information before the authorisation was in place. We review the details of any contact with the CHIS, assessing always whether useful intelligence

10 60 on-site inspections and 43 desktop or remote inspections.

11 which are not within the constitution of a Local Authority.

12 which are not within the constitution of a Local Authority.

was gained. The inspectors will focus on the welfare of the CHIS and his or her security, and whether the risk assessments were properly compiled. Our resources do not enable us to consider all the use of adult CHIS; instead we look at a representative sample of the authorisations during an inspection and a similar sample of undercover authorisations. By contrast, we look at every instance of the (notably infrequent) use of juvenile CHIS.

3.28 In addition, at MI5 and law enforcement agency inspections we focus on how the agency has applied its own guidelines to covert human intelligence sources who participate in criminality. The Prime Minister avowed oversight of this previously secret area of 'directed' oversight on 6 March 2018. Sir John Goldring, the Deputy Investigatory Powers Commissioner and former Intelligence Services Commissioner, has particular responsibility for our inspections of the intelligence agencies and MOD CHIS.

3.29 As already observed above, we visit the majority of local authorities for their inspections. However, we also utilise remote desktop inspections when a local authority has significantly reduced or stopped using their powers in this context and when there are no apparent significant compliance concerns. A desktop inspection will always be followed by an onsite inspection. Inspectors review the authority's policies and procedures; their approach to training; the use that has been made of the relevant intrusive powers; and a sample of the paperwork underpinning the authorisations. The OSC only carried out desktop inspections for district or borough councils in England.[13] We continue to inspect on site any local authority or Fire and Rescue Service (FRS) that has used its directed surveillance or CHIS powers during the preceding period, or, as set out above, when the previous inspection was a desktop inspection.[14]

3.30 For renewals of law enforcement undercover officers, our inspectors examine how the officer has been utilised. This includes the detail of how they are managed, the assessments that were made as to their safety and the procedures that should ensure the public authority's duty of care is properly applied, as well as the reasons for any renewal.

Findings

3.31 Broadly, we were impressed by a high degree of compliance with the statutory framework in this area. Although instances of failure to follow the processes and procedures were identified, these were not in any sense systemic. This can be a key investigative tool for public authorities and it was reassuring to note that whatever the historic problems may have been, they were not evident in the period under review.

3.32 The risk of obtaining confidential information is a particular concern. It must be recorded in the authorisation if a CHIS is to be tasked to obtain material in this category and the applicant should always consider whether this is a likelihood. In general, the intelligence agencies are cautious in their approach when potentially faced with confidential material, providing protections that are arguably, in some cases, unnecessary. Proportionality has been comprehensively addressed in these cases, which have been approved at a suitably senior level.

13 But excluding London Boroughs. In 2018 we extended this practice to Scotland and Wales, for all types of council and to the Fire and Rescue Services ('FRS').

14 In the period 01/04/2017 – 31/12/2017 no FRS reported using their CHIS powers.

The Intelligence Agencies and the MOD

3.33 The intelligence agencies and the MOD, generally speaking, properly authorised CHIS activity during the period covered by this report. In one case that was inspected, albeit the event occurred prior to the period under review, MI5 failed to obtain a RIPA authorisation for a limited amount of activity in the UK (this was part of a larger, mostly overseas-based operation). On a few occasions SIS mistakenly failed to obtain appropriate CHIS authorisations when meeting covert human intelligence sources or conducting other CHIS-related activity in the UK. To prevent similar errors in the future, SIS has implemented mandatory legal and compliance training for all officers (valid for two years) and refresher training for officers returning from overseas. We will monitor this programme closely.

3.34 The intelligence agencies and MOD pay close regard to the welfare of their human intelligence sources, albeit – as with law enforcement – we found instances when rehearsing out-of-date information risked confusing an assessment of present risk.

3.35 At MI5 each case is reviewed by a dedicated operational security officer, who is independent of the case handler and the AO. MI5 uses its Behavioural Science Unit to support those human intelligence sources with particularly challenging welfare issues.

3.36 We were briefed by MI5 on one CHIS case in which role-players were in contact with a 'subject of interest' who was experiencing particularly difficult personal circumstances. The human intelligence and source-running section consulted the MI5 Ethics Counsellor at an early stage in the planning process and the counsellor helped shape the operational plan in order to minimise the emotional impact of the operation. This history was well documented in the relevant authorisations and the high level of intrusion in this case was clearly justified by the threat to national security posed by this individual.

3.37 The MOD recently started using online CHIS and this has been inspected by IPCO. We are content with their approach and we are currently reviewing their recently introduced internal guidance.

3.38 It is particularly evident that the intelligence agencies and the MOD manage CHIS cases with detailed regard for necessity and proportionality: (i) in complex cases; (ii) whenever there were significant concerns around a CHIS's security and welfare; and (iii) in cases involving significant levels of intrusion (e.g. those involving access to confidential material). By way of contrast, these issues were often insufficiently addressed in the more routine applications. This is an area for improvement.

3.39 We also also recommended that GCHQ review its CHIS application and renewal template to ensure they record greater detail in the fields relating to necessity, proportionality and collateral intrusion, and that they provide improved guidance on intrusion and personal information. We recommended that the MOD maintains an up-to-date record of intrusion into the lives of the family members of a CHIS.

3.40 In a similar vein, MI5 needs to improve how it considers collateral intrusion. Assessments can appear formulaic, with the same wording being applied in different contexts. To reach a useful assessment, officers need to have an in-depth knowledge of the CHIS and they should assess the particular ways in which the individual may gather intelligence. Highly relevant in this context are the sources of the CHIS, together with the locations and the context in which he or she works. We recommended that MI5 improves how collateral intrusion is addressed in the authorisation paperwork, and that staff understand the need to set out relevant collateral intrusion information on the CHIS forms, including for renewals.

3.41 The MOD must reflect changing circumstances in renewal documents and not simply repeat the substance of earlier applications. SIS should record review dates, together with a summary of the review, in accordance with the CHIS code of practice.

3.42 Most SIS CHIS activities take place overseas, although in some cases SIS assess that a particular CHIS operation may affect individuals in the UK. SIS documentation did not always explain sufficiently clearly why a CHIS authorisation was needed. We recommended that when there is a likely UK connection (e.g. a human intelligence source or the target of an approach is possibly travelling to the UK or a UK-based individual may engage with the CHIS online), SIS should clearly set this out in the application and any related paperwork. This recommendation is in line with the code of practice.

3.43 We examined one MI5 operation which took place largely overseas without the need for a RIPA authorisation but where there was a small amount of CHIS conduct within the UK before MI5 obtained a RIPA authorisation. Shortly afterwards, MI5 sought a CHIS authorisation to cover further activity within the UK. MI5 must ensure it obtains a timely CHIS authorisation for any UK conduct. We recommended that where an overseas operational plan risks this eventuality, MI5 should seek a RIPA authorisation from the outset to ensure that all the activity is lawfully authorised.

Law Enforcement

3.44 In recent years there has been improvement across law enforcement as to how they manage and authorise CHIS, including the quality of the documentation and the assessment of necessity and proportionality.

3.45 However, there is an evident gap in the knowledge of various senior officers and officials, as well as on the part of some of those involved in day-to-day operations, as to the minimum requirements to manage and safeguard CHIS. Indeed, there have been a number of occasions when it was apparent that the AO had little or no in-depth knowledge of the CHIS they had authorised. It is essential that AOs have adequate knowledge of the CHIS's background, the specific risks they face and any potential difficulties for the organisation.

3.46 The points made above concerning weaknesses within MI5 as regards collateral intrusion apply with equal force to law enforcement; it is to be particularly stressed that undercover authorisations need to be assessed on a regular basis.

3.47 Risk assessments do not always contain sufficient detail to enable the AO to judge whether suitable risk-management measures are in place. However, in cases in which more detail is provided, it can be repetitive and formulaic. Risk assessments should provide a depth of information to enable officers to identify and anticipate risks throughout the lifetime of the authorisation, and thereafter. We recommend using an accredited risk-assessment model. With renewals, we found examples of officers repeating out-of-date information which risked distorting the risk-assessment process. Up-to-date information is essential in this context, and we have recommended that renewal submissions should focus on the most recent period, providing an explanation if there has been no progress.

3.48 It is critical to continue developing national standards for the management of CHIS and to implement a programme of ongoing professional, operational and occupational development for practitioners. Accredited training for AOs needs to be readily available.

3.49 The documentation and standards for the authorisation of relevant sources remain generally high for undercover officers, and the quality has improved as a result of enhanced standardisation. These processes have improved since forces increased oversight for UCs.

3.50 There are three areas of particular concern:

- First, the Senior Investigating Officer should not unduly or improperly influence the routine management of UCs, which should be focussed on the safety of the officer. The SIO ought not to attempt to dictate the tactical deployment of the CHIS.
- Second, it is evident that, on an excessively frequent basis, forces fail to notify IPCO in a timely way, or indeed at all, that there has been a new authorisation for an undercover officer (see statutory instrument 2013/2788).
- Finally, we remain concerned as to how law enforcement interprets the expression 'same operation', which determines whether an application for a renewal should be made to a JC. In many operations, particularly online, an undercover officer will engage with the same or similarly-minded criminals on more than one occasion, albeit the contact may last for only a few weeks. The AO needs to consider when the authorisation is due to expire whether the operation should be continued by way of a renewal or a new authorisation. We plan to scrutinise this aspect of covert activity closely over the coming year.

Juvenile CHIS

3.51 The Regulation of Investigatory Powers (Juveniles) Order 2000 and CHIS code of practice recognise that juveniles are more vulnerable than adults, and makes special provision for those under 18. Juvenile CHIS must be authorised at a more senior level than adult CHIS, and, in 2017, renewed monthly.

3.52 If any juvenile CHIS have been deployed by a LEA, the inspectors will consider the detail of each case.

3.53 Although the circumstances will vary, IPCO inspectors will look at:

- the details of the recruitment of the CHIS, with particular focus on whether the young person has previously been uninvolved in relevant criminality and is being asked to report on criminals with whom they would not normally associate. In reality, this never, or only extremely rarely, occurs;
- the risk assessment and welfare management of the juvenile CHIS, both during the period authorised and for the period after the deployment (depending on the case, these may be extensive or they may be limited to ensuring the CHIS understands to contact the Source Handling Unit if there are any problems);
- the tasking given to the source, focusing particularly on the element of danger and ensuring the young person is not being asked to mix in criminal circles to which they would otherwise not have been exposed; and
- whether the parents have been informed and consulted (in some cases sharing this information with the parents may create a risk to the young person).

3.54 There is detailed focus, therefore, on the duty of care, to ensure that juveniles are not being put into dangerous situations.

3.55 It is very rare that the intelligence agencies seek to recruit and run juvenile CHIS. We were satisfied that MI5 handled cases appropriately with authorisations approved at a senior level and subject to monthly renewal.

3.56 SIS informed us they do not seek to cultivate or recruit juvenile sources. We asked about any training exercises conducted in public spaces, with particular concern as to how they ensure that officers are not approaching or interacting with minors. SIS said officers were expected to make this judgement and to take a cautious approach. We are content that while this does not entirely eliminate the risk, the nature of any approach would be minimally intrusive and SIS is taking appropriate steps to ensure that there is no engagement with minors.

3.57 The MOD and SIS share a similar policy on the risk of encountering juveniles when engaging online. We were satisfied that the MOD will begin a structured review process if a target is identified as a juvenile, albeit it assesses the risk of encountering juveniles to be minimal.

3.58 GCHQ will immediately break off contact if they become aware they are dealing with a juvenile.

3.59 In late 2018 concern arose about the use of juveniles as CHIS following the extension of the authorisation period to four months. The Investigatory Powers Commissioner has undertaken to report in more detail in 2019 about the use of juvenile sources, including by way of providing more detailed statistics. Enquiries so far (although not complete) show that very few juveniles have been used by LEAs as CHIS during the relevant period (at any one time young people acting as CHIS are unlikely to reach double figures) and that all these CHIS were above 15 years old. Furthermore, their involvement is usually of short duration, and they are, with very few exceptions, involved in criminality or youth gangs before they are recruited.

Northern Ireland local authorities

3.60 The IPC does not have oversight of directed surveillance or the use of CHIS by local authorities in Northern Ireland. There is an argument that this anomaly should be rectified.

4. Surveillance

Description of power and its use

4.1 Directed surveillance occurs when there is covert surveillance of an individual in order to obtain private information about them in support of a particular operation or investigation. It applies when the surveillance is not an immediate response to events or circumstances the nature of which means it would not be reasonably practicable for an authorisation under Part II of the 2000 Act (or its RIP(S)A equivalent) to be sought.

4.2 This is an investigatory technique that is available to many public authorities for a variety of statutory purposes, including the protection of national security and public safety, or to prevent and detect crime or to prevent disorder. The technique is frequently used by the law enforcement agencies, the intelligence agencies and local authorities, as well as regulators such as the Financial Conduct Authority.

4.3 There will be a likely instance of directed surveillance if a member of a public authority follows someone on foot or in a vehicle, sets up at a location to record their movements or covertly monitors an individual's social media activity. It is of note that the use of online surveillance is increasing. LEAs often use directed surveillance to identify criminal suspects and it is sometimes a stepping stone to more invasive tactics in serious criminal investigations. Examples of the circumstances when local authorities use directed surveillance include identifying those responsible for environmentally damaging fly-tipping or selling alcohol or tobacco to minors.

4.4 Directed surveillance is to be distinguished from intrusive surveillance. Intrusive surveillance is covert surveillance of any residential premises or private vehicle which is, self-evidently, likely to be notably invasive. Intrusive surveillance can be used for a limited range of purposes. These are principally the interests of national security, the prevention or detection serious crime or the interests of the economic well-being of the UK. Intrusive surveillance is available to only a limited number of public authorities: the intelligence agencies, the police, the MoD, HM Forces, HMRC, NCA, Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), Home Office[15] and the Ministry of Justice and Northern Ireland Office.[16]

4.5 Any surveillance conducted outside the British Islands by the intelligence agencies is not authorised under RIPA unless it is likely that intelligence gained from the surveillance will be used as evidence in a UK court.

15 For departments exercising functions relating to immigration matters and with officers designated as customs officials.

16 The Ministry of Justice and Northern Ireland Office are designated by order to enable intrusive surveillance to be carried out in prisons..

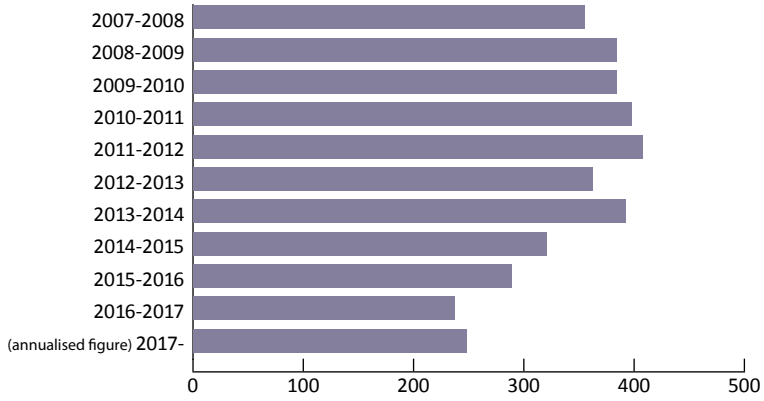
Statistics of use of powers

4.6 Directed surveillance is frequently deployed as an investigative tool by law enforcement agencies but there has otherwise been a marked reduction in its use, particularly by local government and the Fire Service. There may be a number of reasons for this, including statutory change[17] and increased collaboration with local policing teams, but budget constraints are also likely to have played a part. I am concerned that there may come a point in the near future when there will be public anxiety that some of the relevant authorities are failing to make proper use of this important technique to investigate and prosecute crime.

4.7 For the intelligence agencies, most of the surveillance activity we oversee is conducted by MI5 under a combination of specific and thematic directed surveillance authorisations and intrusive surveillance warrants.

4.8 On an annualised basis, 186 intrusive surveillance authorisations were granted for Law Enforcement in the period 1 April to 31 Decem ber 2017[18] This is a similar number (when 'annualised' to 248 authorisations) to the previous 12-month period, but it remains significantly lower than the average of 400 authorisations per year seen regularly before 2014.

Fig. 3 Intrusive Surveillance Authorisations over the last 10 years (excluding UKIC)



17 The Protection of Freedoms Act 2012 limited the levels of criminality for which the powers are available to local authorities in England and Wales, and introduced the need for a magistrate's approval of the activity.

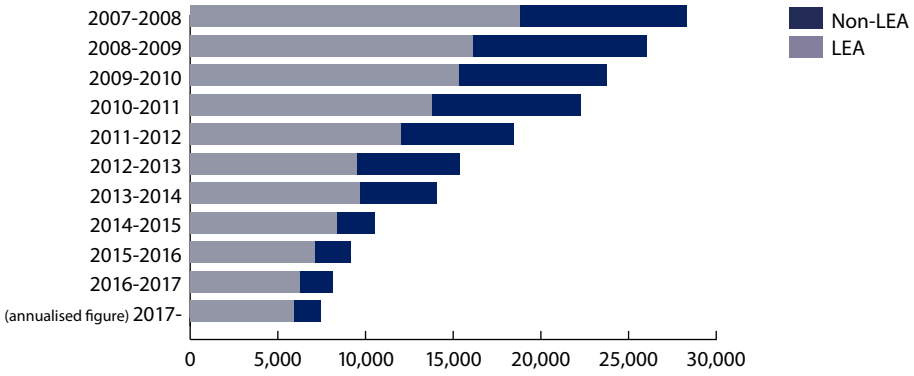
18 See the chapter above on CHIS in which we have explained the approach to collecting statistics for this period.

The Directed Surveillance authorisations granted by the different types of public authorities were as follows:

Public Authority Type	01/04/17–31/12/17	'Annualised figure'	Extant on 31/12/17
Law enforcement agencies	4,492	5,989	822
Local authorities	233	310	15
Fire & Rescue Services [Independently constituted from local authorities]	0	0	0
Other public authorities (e.g. govt regulators)	933	1,244	130

4.9 Based on 'annualised' figures, the number of law enforcement directed surveillance authorisations has fallen to 5,989 compared to the 6,237 authorisations for the 2016-17 financial year (as reported by the OSC). This continues a long term decline in the number of directed surveillance authorisations from the 20,000 per annum ten years ago. There were 822 extant directed surveillance authorisations on 31/12/2017 compared to the 808 on 31/03/2017.

Fig. 4 Directed Surveillance Authorisations over the last 10 years (excluding UKIC)



4.10 The number of Local Authority and Other Public Authority authorisations remains broadly similar to recent years. By a significant margin, the Department for Work & Pensions remains the public body which authorises the most directed surveillance (792 of the 933 OPA authorisations).

4.11 As can be seen from the table overleaf, Fire and Rescue authorities did not use surveillance powers at all during this reporting period. Only 22% of local authorities and 42% of other public authorities granted authorisations for directed surveillance during the reporting period.

4.12 Law Enforcement Agencies used the urgency provisions 700 times during the period 1 April to 31 December 2017 (on an 'annualised' basis, 933 times). This is similar to previous years.

The Authorisation Process

Directed surveillance

4.13 Save for local authorities in England and Wales, a written application for directed surveillance is submitted to an authorising officer within the same public authority, specifying the details of the proposed surveillance, including why it is suggested to be necessary and proportionate to undertake the requested activity. In urgent cases, the applicant may seek oral authorisation, although this must always be followed by a written application.

4.14 As for CHIS, authorising officers act in a quasi-judicial role when considering these requests. They must be impartial and, where possible, they should be separate from the investigation.[19] Although they can seek more details and legal advice, the decision whether or not to grant an authorisation is entirely theirs. Authorising officers must be of superintendent, senior military or senior manager level (for law enforcement agencies and government departments).[20] Please see Chapter 3 on CHIS for additional detail.

4.15 For local authorities in England & Wales, an application must be approved by a magistrate.[21]

4.16 Initial authorisations for directed surveillance are valid for three months, as set out in the code of practice, and must be recorded by the public authority on its central record and updated when renewed or cancelled. The code of practice stipulates exactly what information must be recorded and retained for oversight purposes. All authorisations must be reviewed regularly and cancelled as soon as they are no longer necessary.

Intrusive surveillance authorisations

4.17 Intrusive surveillance applications are authorised at a higher level than for directed surveillance. For the intelligence agencies, the MOD and HM Forces, the Ministry of Justice and the Northern Ireland Office, a Secretary of State considers the application. For the police, the NCA, HMRC, CMA, IOPC and Home Office this role is undertaken by a senior authorising officer or a designated deputy.

4.18 The authorisation process for intrusive surveillance authorisations is otherwise similar to directed surveillance except that for the police, the NCA, HMRC, CMA IOPC and Home Office authorisations must be approved by a JC before they take effect. There is an exception to this for urgent cases.

Combined authorisations

4.19 During the period relevant to this report, the intelligence agencies have applied separately for intrusive and directed surveillance authorisations even when they have been carrying out the surveillance by the same 'means', for example, tracking a vehicle using a route logger

19 If an AO is not independent, the 2014 code of practice which governed the period under review in this report required that this was highlighted in the centrally retrievable record of authorisations and the Commissioner or inspector should be invited to view it at the next inspection.

20 For the intelligence agencies authorisation is undertaken at a 'middle management' or above level.

21 No urgency provisions are available for local authorities.

and audio listening device. The MOD relies on joint authorisations. Under the IPA 2016, the intelligence agencies will be able to apply for joint authorisations for directed and intrusive surveillance when the collection includes equipment interference.[22]

How IPCO oversees these powers

4.20 IPCO oversees all surveillance activity conducted by the law enforcement and intelligence agencies, the MOD and other public authorities, in addition to the local authorities in England, Wales and Scotland (see Chapter 1). We are concerned that there is a lack of oversight in this regard for local authorities in Northern Ireland which means these powers are exercised without any external scrutiny.

4.21 Most inspections are carried out at the public authority's premises. The inspectors will scrutinise the policies and procedures that have been utilised to ensure compliance. IPCO considers any training and how the surveillance equipment is managed, and the inspectors will review a sample of the authorisation paperwork. The inspectors speak with senior managers, authorising officers and the operational teams. They look in detail at the operations, what was planned and what happened in order to test why the surveillance was required, whether it was appropriate, if it was successful, what intelligence was gained and how it was handled.

4.22 Inspections can last between one and five days, depending on the extent and complexity of how the various powers have been utilised. As reported in the previous chapter (CHIS), in 2017 we conducted 59 surveillance and CHIS inspections at law enforcement agencies, 134 at local authorities[23] and 21 at other public authorities (e.g. government regulators). Surveillance authorisations were also considered in detail during our primary bi-annual inspections at each intelligence agency during 2017 (led by Sir John Goldring).

4.23 Every local authority in England, Wales and Scotland is inspected once every three years, or more frequently if their compliance record is poor or if there is some other good reason for an interim visit. This is either at the premises of the authority or by way of a desktop inspection, when an inspector will remotely review the authorisations and the materials relevant to compliance. As already highlighted, many local authorities are using their directed surveillance powers less frequently than a decade ago; as a result, remote inspections will be utilised to a greater extent than hitherto, particularly for those authorities that have not used these powers since the last inspection.

4.24 However, there will always be an inspection, by either method, of each local authority – irrespective of whether or how often they use their powers – to confirm (amongst other things) that they are not carrying out surveillance inadvertently. In 2017 we also undertook desktop inspections of Fire and Rescue authorities who have effectively ceased to use their powers. It is for the government to review whether access to these powers is still required.

Findings

4.25 Following our inspection of a range of warrants and authorisations, we are confident that intrusive surveillance is being conducted satisfactorily. The following discrete points, however, are worthy of mention.

22 Full details of which warrants and authorisations may be combined, and the wider range of public authorities for which this is permissible is contained in Schedule 8 of the Investigatory Powers Act 2016.

23 Including 46 'desktop inspections'.

Intelligence agencies and MOD:

Complex surveillance authorisations

4.26 MI5 conduct a range of complex surveillance activities under each separate authorisation. We have questioned whether the full range of that activity is adequately reflected within the surveillance authorities, including the renewal documents, and we suggested MI5 should review its approach to the directed surveillance records to ensure that the necessity, proportionality and intrusion considerations are clearly set out for all the relevant activity. We will scrutinise this with particular care over the next 12 months.

Directed surveillance errors

4.27 We were concerned by a comparatively high number of errors at MI5 under this heading, and we criticised their failure to recognise the adverse issues in this area which we identified, and which appear to stem from a persistent focus on the authorisation process rather than a review of internal practice. In some cases these errors originated from a lack of appropriate internal controls in key areas. We have pressed MI5 to resolve this deficiency and to facilitate a wider review of their directed surveillance activity, along with the adequacy of the current internal controls. We are confident, however, that they have reported all the identified errors where the lack of internal controls has led to a breach of an individual's right to privacy.

SIS and GCHQ

4.28 SIS and GCHQ undertake relatively little surveillance in the UK because of their international focus. We are confident that all the UK-based surveillance by both agencies is adequately captured, but we concluded that GCHQ did not always set out the scale of the planned surveillance sufficiently and therefore the likely level of intrusion was sometimes unclear. This is an area for improvement.

MOD

4.29 We expressed a concern that the MOD conducted directed surveillance under intrusive surveillance authorisations, which would be contrary to s.28 RIPA. However, the MOD indicated that this practice applied only to overseas surveillance and no directed surveillance had been conducted in the UK without a specific directed surveillance authorisation. It is of general note in this context that there is a mistaken belief that directed surveillance is simply a lesser, rather than a different, type of surveillance. It is reassuring that the MOD will ensure that all combined directed and intrusive surveillance authorisations state clearly that both types of surveillance will be conducted.

Product handling arrangements

4.30 In his 2016 report, Sir Mark Waller raised the importance of setting out clearly in an application how any unwanted product would be handled. We noted that surveillance casework at the MOD did not provide details as to how unnecessary information was to be treated. It is essential that the authorisation is clear in this regard, particularly when there is risk of a high level of intrusion. Appropriate handling arrangements are a key method of managing and mitigating intrusion. It follows that the authorising officer should have a clear understanding of how the product will be handled, whether or not it is of intelligence value. Again, this is an area that calls for improvement.

Complex and technical operations

4.31 The intelligence agencies and the MOD have adopted a thoughtful and sensible approach to surveillance principles during the process of developing new techniques. We inspected a range of authorisations for non-traditional surveillance, including by complex technical means. In most cases, authorising officers have taken care to describe the likely extent of intrusion from the operation but in some highly technical operations it can be difficult to explain simply the true nature and scope of the operation. The MOD has adopted the practice of annexing project proposals to the surveillance application form. We recommended that the intelligence agencies adopt this approach, and ensure they apply a clear policy on any technical terms and descriptions that are set out in these annexes.

Renewal paperwork

4.32 We inspected a range of directed surveillance renewal authorisation documents for the intelligence agencies and we recommended that more detail was provided about any action that had been taken during the original period of authorisation. Renewal documents must reflect the content and value of the surveillance activity. MI5 keep a record of surveillance activities under surveillance authorisations. These are centrally retrievable but they are not set out in a single format. The renewal document, furthermore, does not always provide a full reflection of the surveillance activity captured in these records. We have recommended that renewals would benefit from the inclusion of specific examples of activity and intelligence.

4.33 We found that MI5 and the MOD often simplify renewal forms by focusing on primary methods of surveillance and they fail to refer to all of the actions that have been authorised. For both directed and intrusive surveillance, the focus is often on a single or primary target, and does not reflect the totality of the likely intrusion. For example, in one case at the MOD an agent was used to facilitate an intrusive surveillance operation but the agent, not the targets, were the subject of the intrusion considerations. We recommended that the totality of surveillance activity is considered on authorisation and renewal paperwork.

GCHQ authorising officer considerations

4.34 During our first inspection of the year at GCHQ, it was suggested that the authorising officer should record their considerations to demonstrate that they have taken into account the necessity and proportionality of the proposed surveillance. In a follow-up review, we noted that this recommendation had been implemented: the authorising officers are providing a succinct summary of the relevant considerations, and their approach to any unusual factors relevant to the case.

Local Authorities:

4.35 Our inspectors did not identify any significant change in compliance compared to previous years when inspected by the OSC.

Seriousness of crime threshold

4.36 We identified a small number of cases in England and Wales for which the offence and the available sentence were not sufficiently described. These cases should not have been approved and we have encouraged councils to ensure the documents are clear on this point.

Online surveillance

4.37 Local authority guidance on surveillance does not always address how investigators should use social media or where they may need an authorisation. The 2018 revised Home Office code of practice for surveillance contains helpful advice local authorities can incorporate into their policy documents and training.

4.38 Our inspectors were particularly impressed by Durham County Council, whose senior responsible officer commissioned a helpful audit across the organisation on the 'Use of social media in Covert Investigations', to evaluate and report on whether their system is adequate and appropriate for this purpose. We commend this approach.

Compliance challenge for local authorities who infrequently use their powers

4.39 In general, the compliance problems that were identified rarely amount to more than a failure to review or cancel authorisations, or instances when the authorisation was poorly articulated.

4.40 However, we conducted an extraordinary inspection of one local authority in relation to surveillance that had been authorised to obtain evidence for family court proceedings. The council appointed a private investigator to identify whether the parents were associating with each other. The judge in the case did not criticise the appointment of the private investigator but was concerned that the council had not obtained an authorisation under RIPA to conduct this surveillance. It became apparent that the relevant council officers were unsure of the correct procedures and had not been trained in the surveillance application process. They were unaware of both the council's RIPA guidance and the identities of the Senior Responsible Officer and RIPA Co-ordinator. The officers sought assistance from the legal team but the advice they received failed to address the RIPA implications of this activity. As a result, the officers attempted to gain authorisation for the activity without proper consideration of the relevant legislation. This could have had a serious impact on the lawfulness of undoubtedly necessary investigative work, in the context of important court proceedings. We asked the council urgently to review their internal training and awareness policies to ensure this did not happen again. It goes without saying that ignorance of the legislative requirements and the lack of properly formulated policy and procedural arrangements will constitute serious failings on the part of an authority.

4.41 Instances of a serious lack of knowledge amongst operational officers, albeit rare, are not confined to council officers as a recent IPT ruling in relation to unauthorised surveillance by the British Transport Police has demonstrated.[24] Appropriating training and supervision is required in all public authorities who have surveillance powers available to them.

4.42 We are encouraged to see that many local authorities have established table top exercises, regular training regimes and senior staff walkabouts to raise awareness. Merseyside Fire & Rescue Service, North Ayrshire Council, Rotherham Metropolitan Borough Council, Torridge District Council and Durham County Council, have been proactive in this area. We are confident these tactics will provide additional safeguards against inadvertent unlawful activity in the future.

24 Gary Davis vs British Transport Police https://www.ipt-uk.com/docs/Davies%20G%20Determination%20and%20Remedies.pdf

Law enforcement:

4.43 The general approach of law enforcement agencies, as reflected in the authorisations individually inspected, strongly indicate that forces are appropriately evaluating the value of material that is available online and what, if anything, it will add to an investigation. During the inspections, there was reassuring evidence that the authorities routinely consider the public's right to privacy in this context. The management oversight arrangements and associated policies generally indicate that appropriate safeguards are in place to ensure online surveillance activities are proportionate. It was equally apparent that forces are mindful of the speed at which intrusion can escalate during an online surveillance operation.

Non-RIPA Surveillance by Law enforcement and Local authorities

4.44 On occasion, public authorities conduct 'non-RIPA' surveillance because an authorisation, whether directed or intrusive, is unavailable under the Act. This could include, for example when the police, by consent, seek to deploy a camera within the house of a vulnerable person in order to investigate allegations of doorstep 'scams'. Authorities need to be careful in these circumstances, to ensure that the activity is appropriately overseen. This will often include implementing a non-statutory authorisation process that runs in parallel to any RIPA approvals.[25] We will review the adequacy of these arrangements throughout 2018. The IPC does not seek in any way to discourage 'non-RIPA' surveillance but instead public authorities should usually follow a RIPA-style approach in these circumstances.

25 The Investigatory Powers Tribunal provided clear guidance (IPT/11/129/CHIS; IPT/11/133/CHIS; and IPT/12/72/CHIS) that where no authorisation is capable of being granted in such circumstances public authorities should closely mirror the procedures that would have been used if an authorisation could have been obtained.

5. Property Interference (including equipment interference)

Description of powers and use

5.1 Property interference is any action which interferes with private property. This includes trespass onto private land to carry out surveillance by, for example, taking photographs; covert entry into vehicles or buildings to conduct searches or deploy surveillance equipment; or obtaining information covertly from telephone or computer equipment (often referred to as hacking).

5.2 Property interference is an investigatory power available to the intelligence agencies, the police, the services police,[26] HM Revenue and Customs (HMRC), National Crime Agency (NCA), Competition and Markets Authority (CMA),[27] Independent Office for Police Conduct (IOPC), Police Investigations and Review Commissioner, or Home Office.[28]

Intelligence agencies

5.3 The intelligence agencies can carry out property interference in the UK under s.5 Intelligence Services Act 1994 (ISA) warrants. SIS and GCHQ use s.7 ISA warrants to authorise property interference on equipment based outside the British Islands. These warrants authorise MI5, SIS or GCHQ to access, enter into, and interfere with property, including electronic equipment. These warrants can also authorise interference with wireless telegraphy. Any action must be necessary for the purposes of assisting the agency concerned in carrying out its functions.

5.4 Under s.42(2) of RIPA, a single warrant or authorisation can combine intrusive surveillance warrant and a property interference activity. This might cover, for example, entering a vehicle to install an audio monitoring device, and monitoring that audio device. At present, property interference undertaken by an intelligence agency under s.5 ISA is not subject to commissioner approval. The Investigatory Powers Act 2016 introduces the double lock only where the interference includes equipment interference (see below).

Law enforcement and others

5.5 In the UK, law enforcement agencies such as the police, NCA and HMRC use powers under Part III of the Police Act 1997 to enter, or interfere with, property and to interfere with wireless telegraphy when it is necessary for the statutory purpose of preventing or detecting serious crime. The larger metropolitan police forces and law enforcement agencies use these powers extensively, in contrast to the CMA.

---

26 The Royal Navy Police, Royal Military Police and Royal Air Force Police.

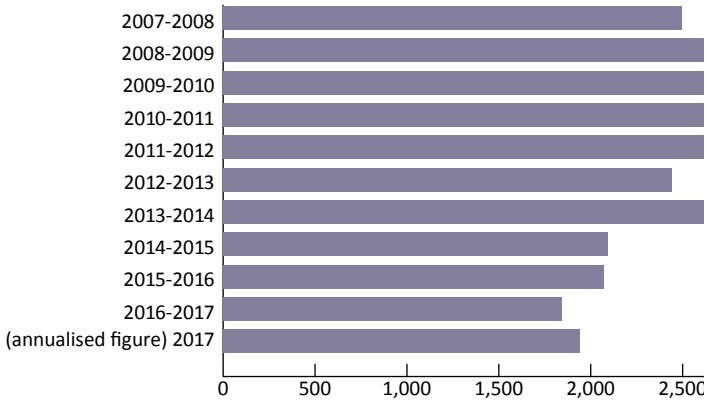
27 The power is only available to the CMA for the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (the cartel offence).

28 For departments exercising functions relating to immigration matters, and officers designated as customs officials.

Statistics of use of powers

5.6 1,453 authorisations for property interference under Part III of the Police Act 1997 were granted during the nine months from 1 April to 31 December 2017. Annualised this is 1937 warrants, which is broadly similar to the 1,842 reported by the OSC for the 2016-17 annual report period. Over the past ten years, the number of authorisations has fluctuated between two and three thousand authorisations per annum.

Fig. 5 1997 Police Act Property Interference Authorisations over the last 10 years



5.7 During this reporting period no property interference authorisations were quashed by a Surveillance Commissioner or JC.

5.8 We currently report the number of Intelligence Services Act warrants to the Prime Minister in a confidential annex to this report.

The authorisation process

5.9 The process for authorising property interference is different for law enforcement and the intelligence agencies.

Law enforcement agencies and others

5.10 An applicant must submit a written request to the authorising officer who is a member of the same public authority, unless a relevant collaboration agreement exists. In urgent circumstances the applicant may make an oral application which must be followed up in writing at the earliest opportunity.

5.11 As with other applications for investigatory powers, the application must provide a detailed description of the activity and its consequences. This should include, for example, a description of the property subject to the interference, the identity of those who possess it, where the interference will take place, the nature of the interference, the offence under consideration and why the intrusion is justified, along with any collateral intrusion.

5.12 Like intrusive surveillance, property interference must be authorised at a higher level than directed surveillance, for example, by a Chief Constable.[29] Written authorisations last for three months and urgent oral applications for only 72 hours.

5.13 All decisions to authorise, renew or to cancel must be notified to a JC. When the proposed authorisation relates to property that is a dwelling, hotel bedroom or office or to information subject to legal professional privilege, confidential personal information such as medical records or spiritual counselling, the communications of MPs, or confidential Journalistic material, it must first be approved by a JC before interference can take place.

Intelligence agencies

5.14 A member of the intelligence agencies can apply for a warrant from the Secretary of State. Applications must contain the same detail as law enforcement applications and they last for six months. There is no requirement for the intelligence agencies to notify a Commissioner, nor do these warrants need to be approved by a JC where they relate to sensitive locations or confidential information.

How IPCO oversees these powers

5.15 IPCO oversees all property interference warrants and authorisations retrospectively. As explained above, for law enforcement authorisations, a JC is notified of the authorisation and, in certain circumstances, must approve the activity before it can commence.

Retrospective oversight

5.16 We inspected property interference by police forces and other law enforcement agencies as part of their annual CHIS and surveillance inspection. In 2017 we conducted 59 inspections of law enforcement agencies in this regard. At the intelligence agencies we inspected property interference during the two primary inspections at each agency in 2017.

5.17 The Warrant Granting Departments (WGDs) at the Foreign Office, Home Office and Northern Ireland Office (NIO) were inspected to assess the gatekeeper role they perform. This included an assessment of their use of the urgency processes, together with the briefing notes from senior officials to the Secretaries of State.

5.18 As with other powers, within each organisation the inspectors scrutinised a random cross-section of documents, policies and procedures and they interviewed senior managers, operational and technical staff.

5.19 IPCO seeks to identify any irregularities or examples of poor compliance, most particularly to prevent them becoming systemic. The number of inspectors and the time they spend inspecting a public authority varies depending on the use by the authority of its powers, the complexity of the cases it handles and any compliance concerns.

5.20 It is to be noted in passing that in 2017 we particularly focussed on whether public authorities had properly considered the potentially significant commercial and technological impact of operations which may reveal security weaknesses in widely used systems, thereby creating opportunities for unwarranted interference (colloquially referred to as hacking).

29 Unless urgent, when in this example an Assistant Chief Constable can authorise.

Findings

Law enforcement

5.21 The inspections revealed a generally high standard of compliance with the legislation, the codes of practice and the guidance that was historically provided by the Office of Surveillance Commissioners. These particular powers have been in place and inspected for approaching 20 years and the necessity and proportionality requirements are, generally speaking, well understood. Few formal recommendations for the police or the other law enforcement agencies were made in this context. In the main, these related to relatively minor areas such as the need to provide a better explanation of the parameters of some of the authorisations, along with the nature of activity to be undertaken, avoiding an unnecessarily complex and technically obscure description of the equipment.

5.22 In updated guidance provided to practitioners in 2016 by the OSC, emphasis was placed on the need to ensure there was a clear intelligence requirement to extend interference more widely, as well as on the importance of engaging the Authorising Officer at an appropriate stage to consider the necessity, proportionality and collateral interference of any additional tactic. This guidance led to improvements in the detail provided in property interference authorisations inspected in the following period.

Intelligence agencies

MI5 overall assessment

5.23 Because of their domestic focus, the majority of the s.5 authorisations inspected related to MI5. The applications and renewals are completed to a high standard; this is in part due to the close scrutiny they receive from the Warrant Granting Department.

5.24 There are, nonetheless, areas that would benefit from improvement. We identified an instance where the NIO should have kept a more detailed record of the oral briefing given to the Secretary of State whilst requesting a warrant under urgent conditions. The Home Office's written briefing notes, written by a senior official as a supplement to the authorisation casework, should always accurately set out the key facts to enable a review of them as freestanding documents. MI5 should avoid using boilerplate text in applications, concentrating more clearly than at present on the circumstances of the individual case. The limits of the agency's understanding of a new target must be accurately described in each application, avoiding standardised wording that can obscure the precise limits of their knowledge.

SIS and GCHQ overall assessment

5.25 Although SIS & GCHQ completed s.5 applications to a good standard, the broader applications by GCHQ should set out more clearly than at present the anticipated scale of the activity and the likely intrusion.

Legally privileged material[30]

5.26 The requesting agency must consider the likelihood of acquiring legally privileged material (LPP), always analysing each individual action for which authorisation is sought. Some applications cover more than one action. If, for instance, a vehicle tracking device and an audio recording device are installed, only the latter creates the risk of capturing material covered by LPP. Particularly with complex authorisations involving a range of actions, there needs to be reassurance that this has been individually addressed, albeit the conclusions can be expressed by way of a composite statement. We stress we have no concerns that LPP is being improperly obtained.

Parties acting on GCHQ's behalf

5.27 We identified a small number of examples of named individuals or entities acting on behalf of GCHQ. These relationships need to be considered carefully, paying attention to the access contractors have to GCHQ systems and the legal relationship between GCHQ and any primary contractors and their sub-contractors.

5.28 We plan to scrutinise the use of contractors more closely in 2018.

Multiple deployments[31]

5.29 Property interference can be a single event or repeated during the period covered by the authorisation. A vehicle location tracking device or beacon is likely to be continuous, whilst a technical operation conducted at a range of locations to identify a communications device will self evidently be of limited duration.

5.30 In a small number of instances, the applications by MI5 and SIS were unclear as to whether the activity was to be a single event or repeated instances. It is critical that this is accurately described because repeat deployments cannot take place if the submission indicates only one occurrence.

5.31 The plans for the operation, including the likelihood of repeat deployments, should be clearly set out in the application. The number and the dates of the deployments should be recorded in cancellations.

Investigatory Powers Act changes

5.32 Under the IPA 2016, public authorities will need to obtain an equipment interference warrant when they are interfering with any equipment for the purpose of obtaining communications, equipment data or other information. This will prevent the use of other powers to obtain stored communications and information from equipment where the interference is in the UK and would otherwise constitute an offence under the Computer Misuse Act 1990. Interference with equipment that is not for the purpose of acquiring communications or equipment data, or other information, will still constitute 'property interference' and will still be capable of authorisation under section 5 or 7 of ISA 1994 (UKIC) or Part 3 Of the PA 1997 (LEAs).

30 MI5

31 MI5 and SIS

5.33 A warrant for equipment interference, whether signed by a Secretary of State or a law enforcement Chief Officer, has to be approved by a Judicial Commissioner before it can be issued. In urgent cases when the activity can be undertaken without the prior approval of a JC, the public authority must seek judicial approval within five working days.

5.34 Following the commencement of the IPA, property interference by the intelligence agencies will continue to be authorised by s.5 ISA; equipment interference for the purpose of obtaining information (including communications and equipment data) by part 5 of IPA; and equipment interference with the intention of altering an electronic device in certain circumstances by s.5 ISA.

5.35 Property interference which does not amount to equipment interference (as defined by IPA) – for example covertly entering premises to install a recording device – will continue to require an authorisation under the Police Act 1997 or a s.5 ISA warrant.

5.36 Schedule 8 to the IPA provides for combined warrants. These create the option for grouping warrants and authorisations for the same investigation/operation together so that the issuing authority and the JC can consider the full range of actions that may be undertaken in relation to the investigation. A combined warrant can include both an interception and equipment interference warrant.[32] It is not mandatory for such warrants to be combined, but this has the benefit of making the Secretary of State and the JC aware of the totality of the action sought to be undertaken when considering whether it is necessary and proportionate. It is anticipated that there will be a substantial number of applications for combined warrants, and our experience to date matches this prediction.

32 Schedule 8 of the Investigatory Powers Act 2016 provides full details of which warrants and authorisations may be combined.

6. Investigation of Protected Information

Description of powers and use

6.1 Part III of RIPA enables public authorities (such as members of the law enforcement and intelligence agencies, HMRC and the NCA) to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information in an intelligible form or to acquire the means by which protected electronic information may be accessed or put in an intelligible form. This could include, for example, requiring a criminal suspect to provide access to their device(s) by providing the password to their phone. The statutory intention behind the measures in Part III is to ensure that the ability of public authorities to protect the public and the effectiveness of their other statutory powers are not undermined by the use of technology to protect electronic information. Failure to comply with a disclosure requirement or a secrecy requirement is a criminal offence. The specific provisions are:

- power to require disclosure of protected information in an intelligible form (section 49);
- power to require disclosure of the means to access protected information (section 50(3));
- power to require disclosure of the means of putting protected information into an intelligible form (section 50(3)); and
- power to attach a secrecy provision to any disclosure requirement (section 54).

6.2 Protected information has a variety of sources. This includes material obtained i) under a judicial search warrant or a production order (for example, under the Police and Criminal Evidence Act 1984); ii) as a result of a statutory power to seize, detain, inspect, search for property or to interfere with documents or other property; iii) as a result of a statutory power to intercept communications; and iv) as a result of the exercise of certain powers under RIPA. It also includes material disclosed to a public authority voluntarily or which has come into the authority's possession by virtue of its statutory powers.

6.3 A disclosure notice can only be served by a person with an appropriate permission, if he or she reasonably believes that it is necessary to do so on one or more of the following grounds: i) in the interests of national security, ii) to prevent or to detect serious crime, iii) in the interests of the economic well-being of the UK, or iv) because it is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty. The imposition of the requirement must be proportionate to the proposed outcome, and circumstances must mean that is not reasonably practicable to access the information without giving the notice. Any conduct that is excessive as regards the interference and the aim of the investigation or operation, or is in any way arbitrary, will not be proportionate.

6.4 Written permission can be sought from a circuit judge or a district judge (Magistrates' Court), (England and Wales), a sheriff (Scotland) or a county court judge (Northern Ireland). In addition, permission may arise from certain warrants issued by the Secretary of State or authorisations in respect of property under Part III Police Act 1997, if the Secretary of State or authorising officer has included permission to give a disclosure notice.

6.5 The Part III RIPA Code of Practice (revised and published in August 2018) sets out the safeguards in relation to this power. Significantly, no public authority may serve any notice under section 49 of RIPA or, when the authority considers it necessary, seek to obtain appropriate permission without the prior written advice of NTAC. This applies both in relation to an individual case or a category of cases. Advice should not be sought from a public body other than NTAC unless the Secretary of State has agreed that it is appropriate for that public body to provide advice about the exercise of functions conferred by Part III. The role of NTAC or another appropriate public body is to provide assurance to the Investigatory Powers Commissioner that the scope for inappropriate use of the powers is mitigated

6.6 As set out in the IPA, the exercise of powers and duties under Part III of RIPA is kept under review by the IPC. Every public authority must maintain a central record of: (i) all applications for permission to give notices (ii) advice given by NTAC or another public body; (iii) the grant of permission; (iv) the giving of all notices; and (v) compliance with each notice. These records must be available for inspection by a JC and retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions.

Statistics

6.7 In 2017, 108 applications were received by NTAC, of which two were declined. The rest were granted.

6.8 No s.49 notices were issued in relation to interception warrants during 2017.

How IPCO oversees the powers and Findings

6.9 S.49 notices (along with the associated documentation) are examined as part of our surveillance and CHIS inspections of public authorities. As the volumes of notices are typically low, most – if not all – will be examined at an inspection visit.

6.10 Typically the notices relate to post-arrest examination of devices (e.g. mobile telephones) seized by the police when a password is sought from a suspect. This is frequently seen in investigations into the supply of illicit drugs or child sexual exploitation. The applications for these notices are normally straightforward and, overall, we have found them to be justified and compliant with the required procedures. This undoubtedly reflects the need to obtain judicial approval and to seek guidance from NTAC.

7. Interception

Definition and process

7.1 IPA targeted interception warrants and bulk interception warrants replace warrants under s.8(1) and (4) RIPA. Whilst this chapter relates to interception undertaken during 2017 under RIPA (IPA interception warrantry had not commenced), for ease of reference we use the IPA terminology of 'targeted' and 'bulk' in this chapter.

7.2 Interception occurs when the content of a communication is collected during transmission by someone who is not the intended recipient or sender. Examples of content include exchanges during a telephone conversation or the text of an email or letter.

7.3 A limited number of public authorities were allowed to carry out interception under s.8(1) and (4) RIPA. The RIPA interception code of practice (CoP) gave detailed guidance on the use of these powers. Interception warrants cover broad aspects of the interception of communications. This includes acquiring the content of the communication and obtaining related communications data and communications which are not identified in the warrant but which, for technical reasons, are inevitably intercepted as part of the process of intercepting the targeted communications.

7.4 A Secretary of State can issue a warrant in response to an application from the Director General MI5, the Chief of SIS, the Director of GCHQ, the Director General of the NCA (on behalf of the NCA or police forces for serious crime), the Metropolitan Police Commissioner (for counter terrorism), the Chief Constable of the Police Service of Northern Ireland (PSNI), the Chief Constable of Police Scotland, HMRC Commissioners and the Chief of Defence Intelligence.

7.5 This means that four Secretaries of State and one Scottish Minister consider most requests for interception warrants. They are the Home Secretary, the Foreign Secretary, the Secretary of State for Northern Ireland, the Cabinet Secretary for Justice for Scotland, and the Defence Secretary.

7.6 The interception must be necessary for one or more of the following:

- in the interests of national security;
- to prevent or detect serious crime;
- safeguarding the economic well-being of the United Kingdom; or
- in circumstances equivalent to those in which the Secretary of State would issue a serious crime warrant for implementing an international mutual assistance agreement.

7.7 To issue an interception warrant for any other purpose would be unlawful, and it is part of our oversight function to ensure that all warrants are issued only when necessary for these statutory purposes. The Secretary of State may not issue an interception warrant unless he or she believes that the conduct authorised by the warrant is proportionate to what is sought to be achieved.

7.8 Targeted warrants must name or describe one person as the interception subject, or a single set of premises as the location to which the interception relates.[33] In contrast, a bulk warrant does not have to name or describe a person as the subject of the interception or a single set of premises as the target of the interception. Bulk interception warrants are only for the interception of 'external' communications (communications sent or received outside the British Islands). The warrant can include intercepting communications which are not external if this step is necessary in order to intercept the external communications to which the warrant relates. Put generally, targeted warrants are essentially an investigatory tool for use once a subject for interception is identified, while bulk warrants are primarily an intelligence gathering capability.

7.9 The intercepting agency has to take a number of steps to ensure it intercepts the minimum amount of material in order to obtain the information covered by the warrant. This includes using its knowledge of the way in which international communications are routed and conducting regular surveys of the relevant communications links in order to identify the communications carriers that are most likely to hold relevant material. The agency must carry out interception in ways that limit collection of non-external communications to the minimum.

7.10 Bulk warrants do not necessarily seek to limit the quantity of external communications which are to be intercepted.[34] Provided the bulk interception requirements in the legislation are met, the interception of all communications transmitted via a particular route or cable, or carried by a particular Communication Service Provider (CSP), can properly be lawfully authorised. However, under RIPA, the Secretary of State provides a certificate which describes at least a part of the material that is to be intercepted, and he or she certifies that examining this material is necessary for one or more of the statutory purposes. Examining material for any other purpose would be unlawful.

7.11 There is a limit to how much we can say in a public document about the interception of communications because of the statutory secrecy provisions contained in RIPA (and replicated in the IPA). These provisions place a duty on anyone involved in interception to keep secret certain aspects of the interception process including, for example, the existence and contents of a warrant, the steps taken to enforce a warrant, and everything in the intercepted material or any related communications data.

7.12 The restrictions on what we are able to discuss in this report self-evidently do not limit how we oversee the use of these powers. All those involved in intercepting communications are required to disclose to the IPC all the information he needs to carry out his oversight functions and we have full and unrestricted access to all of the information and material we require.

33 F1 RIPA 8 (1) refs.

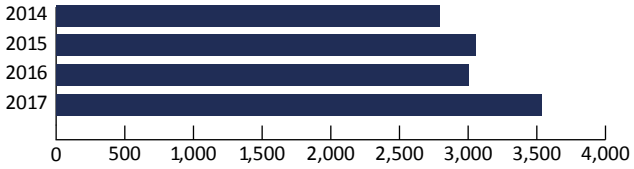
34 Para 6.2 Interception of Communications Code of Practice 2016.

Statistics of use of powers

Total Numbers

7.13 The figure below shows the number of new interception warrants issued in each of the years 2015–2017 for the nine interception agencies. There were a total of 3535 warrants issued during 2017, an increase of just over 17.5% compared with 2016.

Fig. 6 Number of new interception warrants issued



7.14 On 31 December 2017 there were 1,974 warrants in force, a 23.2% increase on the number extant at the end of 2016. 21 of these warrants were issued under the bulk provisions. A proportion were first authorised before the start of 2017 but it remains the case that most interception warrants do not run for longer than six months.

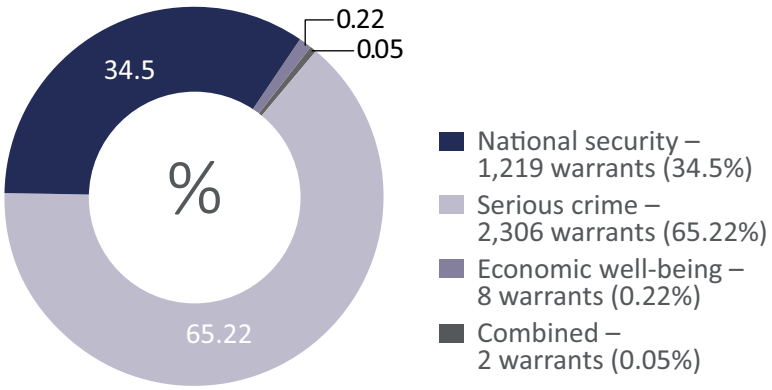
7.15 Only a small number of interception warrants are rejected because there is an exceptionally high level of scrutiny of each application as it goes through the stages of the authorisation process, before it is sent to a Secretary of State (under the IPA, these warrants, once authorised by the Secretary of State, will then be sent to a Judicial Commissioner to be reviewed). A number of appropriately qualified individuals review each application within the interception agency, and applications must be supported at a senior level before beng submitted to the relevant warrant granting department (WGD). The WGD then scrutinises the warrant in detail before it is submitted to a Secretary of State.

7.16 During 2017 there were 116 occasions when a senior official or Secretary of State sought clarification or additional information from the applicant before authorising.

By statutory purpose

7.17 Figure 7 details the breakdown by way of the different statutory purposes of the 3,535 interception warrants issued in 2017.

Fig. 7 Proportion of 2017 warrants by statutory purpose



7.18 The vast majority of the serious crime warrants fall into one of five categories: unlawful supply of controlled drugs, firearms, financial crime (such as money laundering), armed robbery and human trafficking.

Urgent approvals

7.19 The Secretary of State approved 341 urgent warrants in 2017. These all related to exceptional cases where, for example, there was an imminent threat to life within the following 24 hours; an imminent threat to national security or a unique opportunity to obtain intelligence of vital importance to national security; or the imminent importation or handover of a substantial quantity of drugs (within the following 24 hours). Almost all of these urgently approved warrants were issued on behalf of either MI5 or the National Crime Agency.

The authorisation process

Submission and application content

7.20 Each application for an interception warrant contains a detailed explanation of why the agency is seeking the warrant and why the proposed activity is necessary and proportionate.

7.21 The code of practice requires that a targeted RIPA warrant describes (i) the background to the operation; (ii) the person or building which is the subject of the application and how they feature in the operation; (iii) the communications to be intercepted, including details of the CSPs, and an assessment of the feasibility of the interception operation (where this is relevant); (iv) what is being authorised, including what steps are necessary in order to carry out the activity authorised under the warrant; (v) any related communications data likely to be intercepted; (vi) why the conduct is proportionate to what is sought to be achieved; (vii) any collateral intrusion and why that intrusion is justified in the circumstances; (viii) whether the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between a Member of Parliament and another person on constituency business; (ix) the supporting justification when an application is urgent; and (x) an assurance that all material intercepted will be handled in accordance with the safeguards required by the legislation.

7.22 Targeted warrants contain one or more schedules, with details designed to inform the relevant CSPs or others providing assistance what communications they are required to intercept.

7.23 Bulk RIPA warrant applications are very similar except that they do not need to specify a person or premises, but they must detail the certificate that will regulate the examination of intercepted material and provide an assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and that the application meets the conditions of the legislation.

7.24 The intercepting agency submits applications for interception warrants to the relevant WGD for the relevant Secretary of State. These departments are made up of senior officials and staff responsible for scrutinising the warrant applications and presenting them to the Secretary of State with any relevant advice or recommendations.

Issuing

7.25 Interception warrants have to be considered personally by a Secretary of State, including in urgent cases, and he or she will sign the warrant.[35] An urgent warrant is valid for five days unless it is renewed by the Secretary of State.

7.26 The Secretary of State will consider whether a warrant is necessary for one of the permitted statutory purposes and proportionate to what is sought to be achieved by the activity described in it. Consideration will be given to the likely level of intrusion and whether the information sought could reasonably be obtained by less intrusive means.

Renewals

7.27 Interception warrants are valid for six months where the statutory purpose is national security or economic well-being, or three months where the statutory purpose is serious crime.[36] Unless they are renewed, the warrants will cease to have effect at the end of that period. The Secretary of State may personally renew an interception warrant before the end of its period of validity only if he or she believes it continues to be necessary for a statutory purpose. Applications for renewals must justify the necessity for renewal and provide an assessment of the intelligence value thus far of the interception. Renewals take effect from the date on which the Secretary of State signs the renewal instrument.

Cancellations

7.28 The Secretary of State must cancel an interception warrant if it is no longer necessary for the authorised purpose. In practice this means the interception agencies keep their warrants under continuous review and apply to cancel any warrant when it is no longer necessary. The senior official in the WGD cancels warrants on the Secretary of State's behalf.

Safeguards

7.29 Strict safeguards ensure the minimum necessary disclosure and/or copying of intercepted material for the purpose authorised. Every copy of intercepted material or related communications data is destroyed as soon as there are no longer grounds for retaining it for any of the authorised purposes.

Safeguards relating to the examination of bulk material

7.30 The code of practice imposes additional safeguards for bulk warrants. The material should only be examined to the extent that is necessary for a statutory purpose and it should not relate to an individual who is known to be in the British Islands.

7.31 It follows that a bulk warrant does not generally permit the selection of communications of someone in the British Islands for examination. But the legislation permits the examination of material acquired under a bulk warrant relating to the communications of a person in the British Islands if the Secretary of State has certified that it is necessary for a statutory purpose for a specific period (not more than six months for national security and three months for serious crime or economic well-being). Since any such certification has to relate to an individual, it is broadly equivalent to a targeted warrant. This type of material may

35 In urgent cases, where the Secretary of State is not present, warrants can be signed by a senior official on the verbal authority of the Secretary of State.

36 All interception warrants under IPA will be valid for six months.

be examined for a very short period to avoid losing essential intelligence on the written authorisation of a senior official, when the person was believed to be abroad but it has latterly been discovered that he or she had entered the British Islands.

7.32 Before an intelligence analyst is able to read, look at or listen to material obtained under a bulk warrant, he or she must justify why access to the material is required, explaining how the examination is linked to one of the statutory purposes, why it is a valid intelligence requirement and why such access is proportionate.

7.33 The procedure relies mainly on the analyst's professional judgement, and his or her training and oversight, and there is no further internal pre-authorisation or authentication process for the selection of any material. GCHQ's Internal Compliance Team carries out retrospective random audit checks of the justifications for selection and the IT Security Team carries out technical audits to identify and investigate any possible unauthorised use.

7.34 There are a number of other security and administrative safeguards in place at GCHQ which have general relevance. These include the security policy framework and staff vetting; ongoing instruction and training for all staff on the legal and other requirements of operating within the legislation (with particular emphasis on Human Rights Act requirements); and the development and operation of computer systems designed to search for, and check on, instances of potentially non-compliant use of GCHQ's systems and premises. All staff must pass a periodic online test to demonstrate their understanding of the relevant legal and other requirements.

7.35 Our inspections and audits show that, in so far as we are able to judge, the individuals concerned carry out the selection procedure carefully and conscientiously. GCHQ has historically reported the results of the retrospective audits and safeguard breaches to IOCCO (please see the errors and breaches section). The retrospective audits are a strong safeguard and serve to act as a deterrent against improper use.

Retention

7.36 Every interception agency has its own policy as to how long intercepted material and related communications data can be retained before it is destroyed. All content is reviewed and deleted after a very short period unless action is taken to retain the content for longer because this step is necessary. The retention periods for selected content differ between the interception agencies but range from between 30 days to one year. The retention periods for any related communications data also differ, ranging from six months to two years.

How IPCO oversees these powers

7.37 IPCO will inspect the intercepting agency and the WGDs, and the interception inspections are structured in order to ensure the key areas covered in the legislation and the CoP are scrutinised. We inspected all nine intercepting agencies and the four WGDs in 2017, examining 997 warrants for the relevant period. This equates to over 50% of the warrants in force at the end of the year and 28% of the new warrants issued in 2017.

Interception agency inspections

7.38 At a typical interception agency inspection we (i) review any action points or recommendations from the previous inspection and assess the progress made in implementing them; (ii) evaluate the systems in place for intercepting communications to ensure they are sufficient for the purposes of the legislation and that all relevant records are kept; (iii) examine selected interception applications to assess whether they were necessary and whether they fulfil the proportionality requirements; (iv) interview case officers, analysts and linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring the material were proportionate; (v) examine any urgent oral approvals to check the process was justified and used appropriately; (vi) review those cases where communications subject to legal privilege or other confidential information (e.g. journalistic or medical) have been intercepted and retained, and cases where a lawyer is the subject of an investigation; (vii) review the adequacy of the safeguards; (viii) investigate the procedures for the retention, storage and destruction of intercepted material and related communications data; and (ix) review the reported errors, including checking that the measures put in place to prevent errors recurring are effective.

WGD inspections

7.39 There are broad similarities in our focus when inspecting the four main WGDs. We examine the integrity of the authorisation process and the extent of the challenge the Secretaries of State and their senior officials apply to warrant requests. The role of the WGD is to provide a source of independent advice to the senior official and the Secretary of State, and it performs valuable pre-authorisation scrutiny of warrant applications and renewals, particularly as regards necessity and proportionality.

7.40 We inspect WGDs after the interception agencies for which they are responsible. This gives us the chance to discuss findings and recommendations from the interception agencies' inspections with the relevant WGD.

Inspection methodology

7.41 During our inspections of WGDs and the intercepting agencies we focus on the systems and processes, which is usually a three stage process. We request a list of all the applications for warrants since the last inspection. From this list, we select a sample that covers a wide spectrum of different crime types and a range of threats to national security. We additionally focus on applications of particular interest or sensitivity. Examples include applications which have (i) resulted in an unusual degree of collateral intrusion, (ii) been extant for a long period (so we can assess the continued necessity for interception), (iii) been approved orally under the urgency procedure, or (iv) resulted in the interception of legal or other confidential communications.

7.42 Having examined the paperwork, we identify those warrants, operations or stages of the process where we need further information or clarification. The inspectors will interview the relevant operational, legal or technical staff.

7.43 We examine the warrant documentation electronically whenever we have access to the authorisation systems at the interception agencies. If possible, the inspectors conduct or direct query-based searches against the intercepted material and the reporting to test for compliance. This identifies trends and patterns from the applications. The queries are designed to elicit, amongst other things, whether (i) the intercepted material has been used or analysed; (ii) the product has been utilised for the intended purpose; (iii) the intrusion has been conducted consistently and, if not, why the operational team did not seek to cancel the

authorisation; (iv) there are effective retention, storage and destruction arrangements; (v) any errors or breaches resulted from the activity; (vi) the intercepted material was examined in a timely way; and (vii) keyword searches identify sensitive material that has been incorrectly handled (e.g. solicitor or lawyer).

7.44 These searches enable IPCO to review whether the Secretary of State was provided with an accurate picture.

7.45 Over the last 12 months, there have been a number of cases in which we have recommended that a warrant was modified, required changes to be made to the operational practice in order to safeguard privacy, directed that additional information is provided to the Secretary of State either immediately or at the next renewal, or recommended cancellation.

Inspections reports

7.46 After each inspection, a comprehensive report is provided to the head of the intercepting agency, setting out the inspectors' findings and recommendations. Copies of the report are sent to the relevant Secretary of State and the WGD. With the WGD inspections, the report is provided to the relevant senior official and is copied to the Secretary of State.

7.47 The reports include an assessment of (i) whether the recommendations from the previous inspection have been achieved; (ii) the number and type of interception documents selected for inspection, including a list of the warrants; (iii) the warrants selected for further examination; (iv) the errors or breaches reported during the inspection period; (v) the retention, storage and destruction procedures; (vi) any policy or operational issues which the agency or warrant granting departments raised during the inspection; (vii) how any material subject to legal professional privilege, or other confidential material, has been handled; and (viii) overall, whether there has been compliance with the legislation. Recommendations may be made that are aimed at improving compliance and performance, in which case the agency or department is required to respond within two months, detailing the progress that has been made.

7.48 The reports also contain operational detail which cannot be disclosed because of the statutory secrecy provisions contained in RIPA (and replicated in the IPA).

Findings

7.49 Put generally, interception is being conducted lawfully, in compliance with RIPA and the relevant code of practice.

7.50 We made a total of 26 recommendations in our inspection reports; 24 of these related to the interception agencies and two to the WGDs. These recommendations broadly fell under the following categories:

a) **Necessity, proportionality and collateral intrusion.** Some of these recommendations concerned the need for greater clarity and detail in the application concerning any potential collateral intrusion that might occur as a result of the interception activity and how this would be managed. For example, to the extent that it is known whether a phone line or internet connection is used by a number of people, when one or more of whom is a target but the others are not of intelligence interest. The remainder of the recommendations centred on the linked need for a more consistent approach when assessing collateral intrusion, ensuring that this was appropriately re-assessed when a warrant was being renewed.

b) **Legal professional privilege material or other confidential material.** There are special arrangements and safeguards contained in the CoP covering material of this nature. Some of the recommendations in the reports addressed the need to ensure that the renewal submissions describe when material of this kind had been intercepted, and explain how it had been handled. Although in most instances LPP or confidential material is immediately destroyed as not being of intelligence interest, a small number of recommendations were directed at ensuring there was a justifiable intelligence case for retaining material of this nature, and directing that it was appropriately protected and the content was only shared to the minimum extent necessary.

c) **Cancellation and suspension of interception.** The majority of the recommendations fell within this category. For the 997 warrants analysed, there were a few examples of warrants that had not been cancelled in a reasonable period of time (for example, following the target's arrest and remand in custody, or when warrants relating intercepted devices should have been cancelled or suspended because a target had ceased using a particular mobile phone).

8. Targeted Communications Data

Definition and process

8.1 Communications data is conveniently described as 'the who, where, when, and how' of a communication but critically it does not include the 'content'. It identifies, therefore, how, when and where people or machines communicate with each other, but excludes what is said during a communication, or any data within the body of the communication, such as text, or audio and video files.

8.2 RIPA defines communications data as being traffic data, service use data or subscriber information (see s.21 (4)).

8.3 Traffic data is data that is (or was) contained in, or attached to, a communication for the purpose of transmitting the communication. This can include, for instance, (i) incoming call records; (ii) information identifying the location of a device used to make or receive a communication, or the sender or recipient of a communication; (iii) information about the server, domain or website a device has accessed; and (iv) any information on the outside of a postal item or online tracking of communications including postal items.

8.4 Service use information is material about the services provided to customers of postal or telecommunications service providers. It is routinely supplied to subscribers of the service. It includes (i) itemised telephone call records; (ii) records of connections to internet services; (iii) information about the amount of internet data downloaded or uploaded; and (iv) registered or recorded postal delivery and collection information.

8.5 Subscriber information is information the CSPs hold concerning the people who use their communication services. This may include (i) details about the person who subscribes to a telephone number or email account; (ii) the payment method and details of payments; and (iii) details of the device an account holder uses, such as serial numbers.

Who can use the power

8.6 Over 500 public authorities, including 52 police forces and other law enforcement agencies, the intelligence agencies, 429 local authorities and other public bodies (including fire and ambulance services and regulators such as the CMA and ICO) are authorised to acquire communications data under the powers set out in Chapter 2 of Part I RIPA.

8.7 Each of these public authorities is able to acquire communications data for one or more statutory purposes. These purposes include (i) the interests of national security; (ii) preventing or detecting crime, or preventing disorder; (iii) public safety; (iv) public health; (v) collecting tax; (vi) in emergencies, preventing death or injury; (vii) investigating miscarriages of justices; (viii) regulating financial markets; and (ix) identifying dead or vulnerable people, and their next of kin.

8.8 Not all of the statutory purposes are available to all the public authorities (see Statutory Instrument No. 480 of 2010). For example, it is only the Commissioners of HMRC who may acquire data to exercise the functions relating to the assessment and collection of taxes or duties, and acquiring data to assist investigations into alleged miscarriages of justice is restricted to the Criminal Cases Review Commissions in England and Wales, and Scotland.

8.9 Typically public authorities will acquire data directly from the large CSPs, but with the required authorisation they can equally acquire it from smaller businesses or entities such as hotels, restaurants, libraries and airport lounges, to the extent that they provide their customers or users with communication services.

Use of the powers

8.10 Communications data is used for a wide range of enquiries, to identify for instance who was using a particular communications device, where the users were located, with whom they were in contact or the time and duration of the communications.

8.11 It is useful in this context to provide some examples:

Law enforcement

- A police child-sexual-exploitation team responded to a primary school's report that a ten year old pupil had sent indecent photographs of herself on a social media application to a person purporting to represent a modelling agency. Investigators acquired items of internet data to identify the address from which the bogus social media account had been set up. The data enabled the investigators to identify particular premises where the police arrested the offender and seized his telephones and computers. A forensic examination of these devices identified other bogus social media accounts from which the offender had contacted over 100 children. He was subsequently charged with online grooming and the possession and distribution of sexual images of children.
- A law enforcement agency investigated the human trafficking of non-EEA nationals from the UK to other EU member states. Police officers intercepted a trailer which was being used to transport foreign nationals to Dover. Data that was acquired relating to the driver's telephone led to the identification of others who were involved with organised trafficking offences and the locations which were key to the criminal enterprise.

Use by regulators

- The Financial Conduct Authority investigated a 'boiler room scam' whereby fraudsters deceived victims into investing in shares by intentionally inflating and overstating the potential of the proposed investments. The criminal proceeds for these offences were just under £5 million. The 'boiler room' employed 25-30 staff to 'cold-call' prospective investors. Data from 63 RIPA approved applications corroborated the victims' accounts. Internet Protocol (IP) data acquired from the server hosting the fraudsters' websites identified the offices from which telephones and computers were seized and at which the offenders were arrested. Eight defendants were sentenced to a total of 34 years in prison.

Use by local authorities

- A fraudulent trader called at the home of an elderly lady and coerced her into paying inflated charges for unnecessary maintenance work. The local authority's trading standards department acquired subscriber information which related to the telephone number on a leaflet which the suspect had left with the victim. The subscriber information enabled the investigators to attribute the telephone number to the suspect, thereby undermining his defence that he worked on behalf of someone else. He was convicted of offences under the Fraud Act 2006.

Retention

8.12 During 2017 the Secretary of State's power to give a retention notice to a public telecommunications operator to require it to retain relevant communications data was not within the oversight remit of the Investigatory Powers Commissioner's remit, or that of his predecessors.[37]

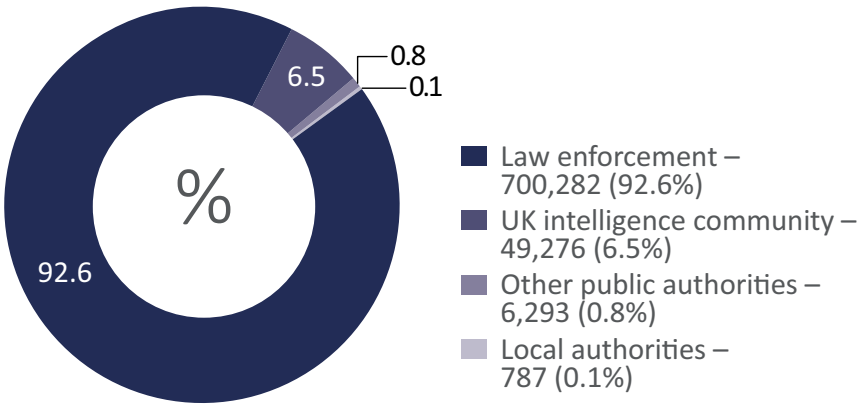
8.13 The requirement for a Judicial Commissioner to approve a Secretary of State's decision to give a retention notice under Part 4 IPA has only recently come into effect in 2018 and will be commented upon more fully in the next annual report.

Statistics

8.14 Each relevant public authority is required to maintain records of their use of the power to acquire communications data and those records must be made available to IPCO inspectors. The public authorities, additionally, must provide their records to the IPC annually. These returns have formed the basis of the statistical breakdown in this section.

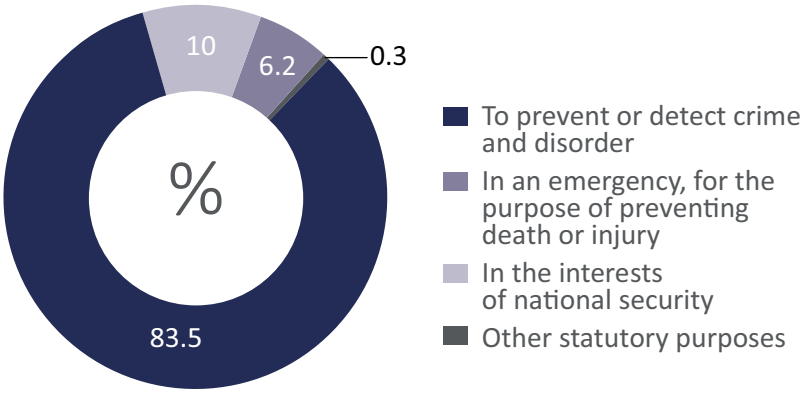
8.15 757,977 items of data were acquired by public authorities in 2017, a similar number acquired in 2016 (754,559 items) and 2015 (761,702 items). Figures 8 – 9 show that the vast majority of data was acquired by law enforcement, for the purpose of preventing and detecting crime, particularly drugs, sexual and violent offences.

Fig. 8 Items of data by public authority type



37 The former Interception of Communications Commissioner Sir Anthony May highlighted in his 2015 half yearly report (https://www.ipco.org.uk/docs/iocco/2015%20Half-yearly%20report%20(web%20version).pdf) the Data Retention and Investigatory Powers Act (DRIPA) did not provide for oversight of the Secretary of State's power to give retention notices.

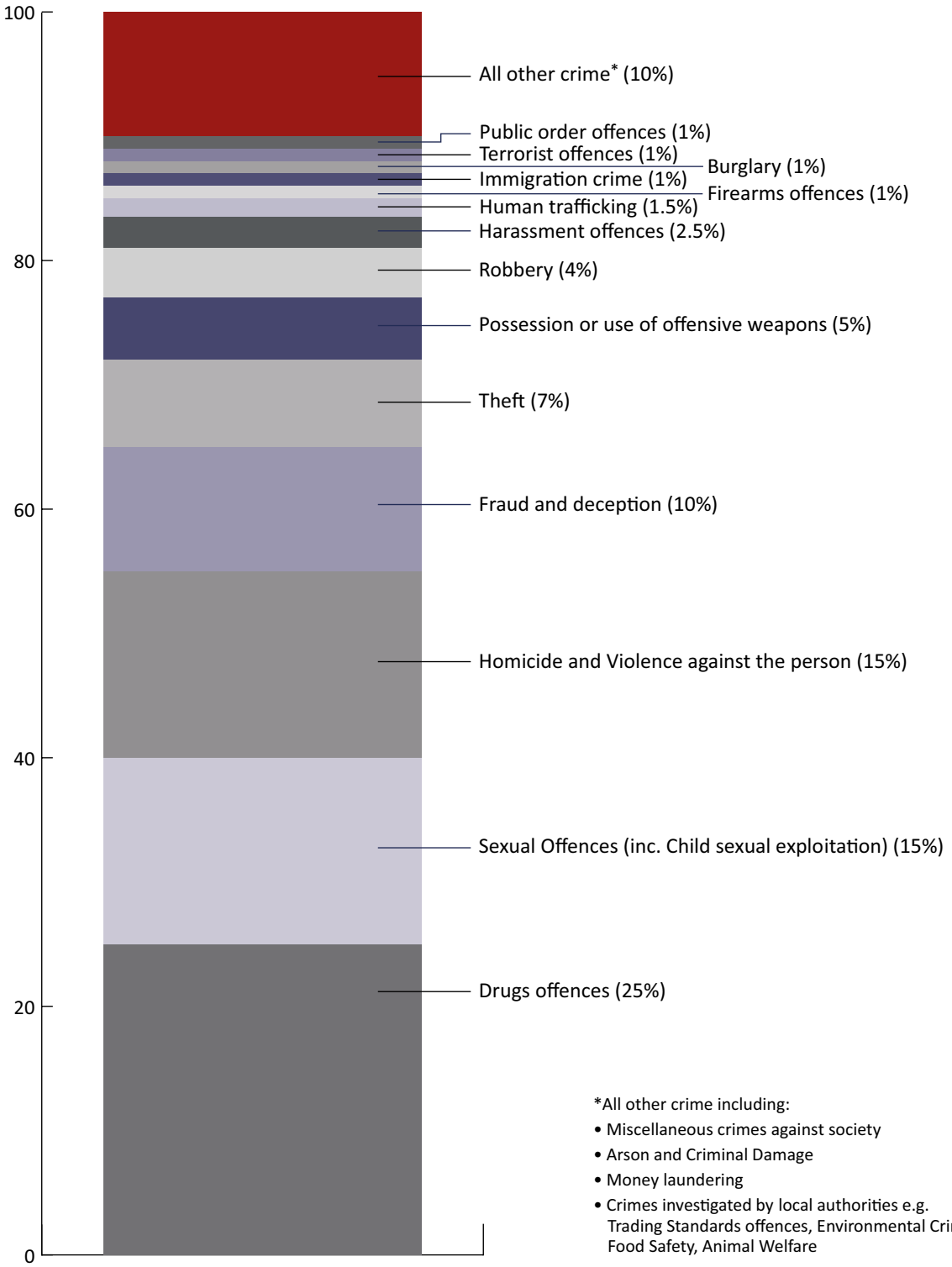
Fig. 9 Items of data by statutory purpose



The following statutory purposes were collectively less than 0.3%

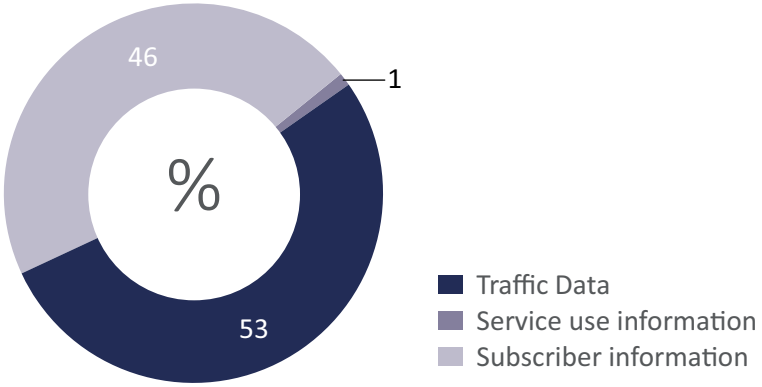
- In the interests of the economic well-being of the UK;
- In the interests of public safety;
- For the purpose of protecting public health;
- For the purpose of assessing or collecting tax, duty or levy;
- To assist investigations into alleged miscarriages of justice;
- To assist in identifying a person who has died other than as a result of a crime or a person who is unable to identify himself;
- In relation to a person who has died or is unable to identify himself, for the purpose of identifying the next of kin or obtaining information about the reason for their death or condition; or
- For purposes relating to the regulation of financial services and markets or to financial stability.

Fig. 10 Items of data acquired for preventing/detecting crime by crime type[38]



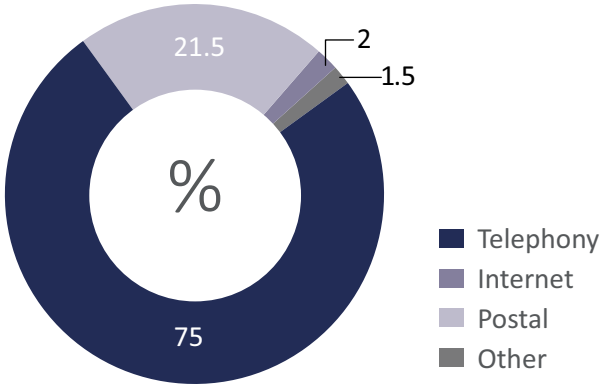
38 Public Authorities acquired communications data under a total of 79 different reported crime categories.

Fig. 11 Communications data items acquired (by category)[39]



8.16 In terms of the type of data being acquired, Figures 11 and 12 show, generally speaking, an even split between the acquisition of traffic and subscriber information, and that the majority (75%) related to telephony. This is broadly similar to that reported in previous years by IOCCO, although the proportion of items relating to the internet is steadily increasing.

Fig. 12 Communications data items acquired (by communication method)[40]

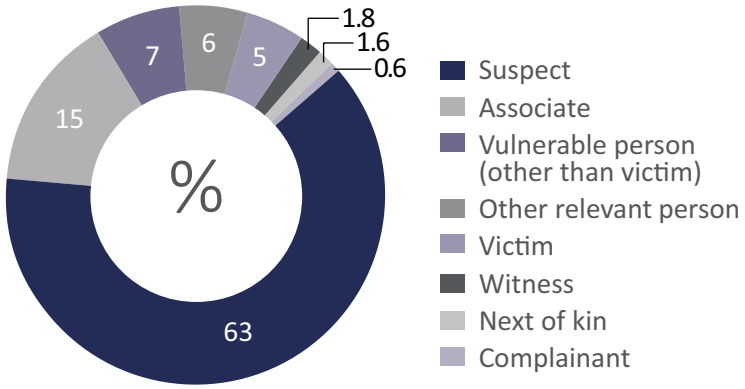


8.17 Figure 13 shows that, similar to previous years, the data acquired largely relates to suspects, their associates or vulnerable persons (typically where police are trying to locate them for their safety).

39 This is not based on a full sample of the 757,977 items acquired.

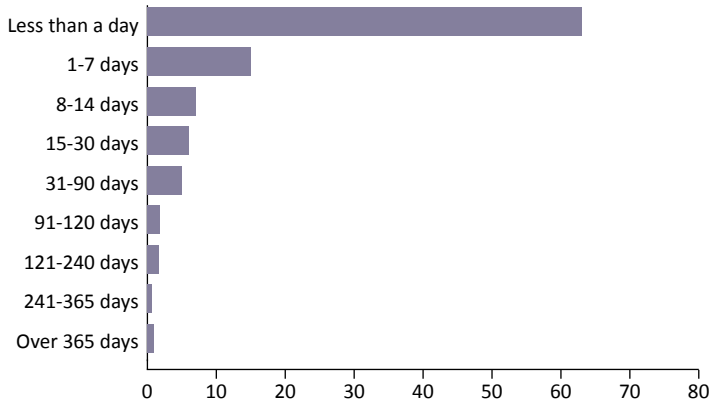
40 This is not based on a full sample of the 757,977 items acquired.

Fig. 13 Items of data by subject's relevance to the investigation[41]



8.18 Figures 14 and 15 show, respectively, the age of the item of data when it was acquired and, in relation to traffic and service use data, the period of data acquired. This is relevant to the question of how long data should be retained by CSPs. It can be seen that almost half of the data acquired is less than a month old. In terms of traffic data and service use data, public authorities are most commonly requesting periods of data under 90 days.

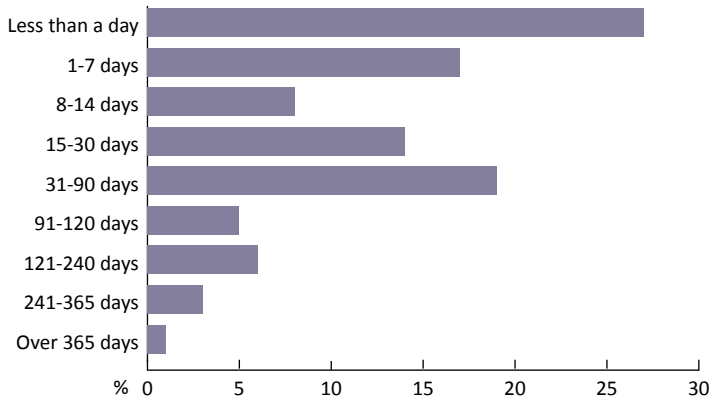
Fig. 14 Items of data by age of item at the point of acquisition[42]



41 This is not based on a full sample of the 757,977 items acquired.

42 This is not based on a full sample of the 757,977 items acquired.

Fig. 15 By period of traffic data / service use items requested[43]



8.19 33% of submitted applications were returned to the applicant by the SPoC[44] and a very small proportion (0.83%) were declined by the SPoC. Of those applications submitted to a Designated Person[45] for consideration 1.71% were declined by the DP.

Returns, rejections and declinations of applications during 2017

Percentage of applications returned to the applicant by the SPoC for development	33%
Percentage of applications returned by the DP for development	5%
Percentage of applications declined by the SPoC	0.83%
Percentage of Applications rejected by the DP	1.71%

The authorisation process

8.20 Applications for communications data are typically made by those conducting investigations or operations for a public authority which has the power to acquire communications data. The applicant submits the application to a Single Point of Contact (SPoC); the SPoC carefully checks the application to ensure that it is reasonably practical to obtain the data sought and that it is lawful under RIPA and free from errors; once satisfied, the SPoC submits the application to a designated person (DP) who decides whether to authorise the application.

8.21 All applications must include details about the targeted communications data, specifying any relevant dates or time periods, the identity of the individual with whom the data is concerned, its relevance to the enquiry, the statutory purpose underpinning the application and an explanation of the necessity and proportionality of the proposed acquisition.

43 This is not based on a full sample of the 757,977 items acquired.

44 The single point of contact (SPoC) is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and the CSPs. Despite the name, in practice many organisations will have multiple SPoCs, working together. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC authentication identifier. SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. Details of all accredited individuals are available to CSPs for authentication purposes – Para 3.19 Acquisition and Disclosure of Communications Data Code of Practice 2015.

45 The designated person (DP) is a person holding a prescribed office in a relevant public authority. It is the designated person's responsibility to consider the application and record their considerations at the time (or as soon as is reasonably practicable) in writing or electronically. If the designated person believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice given Para 3.7 Acquisition and Disclosure of Communications Data Code of Practice 2015.

8.22 If the application is authorised, a notice will be issued to a CSP to disclose the requested data. In order to facilitate the secure and swift disclosure of communications data, many CSPs have systems in place for the SPoCs to access the authorised communications data directly, while maintaining the security of the information and an audit trail.

8.23 An authorisation or notice to acquire communications data must comply with the requirements of RIPA 2000. They are valid for a maximum period of one month and can be renewed by the same procedure under which they were originally authorised. If it is no longer necessary or proportionate to acquire the communications data, the authorisation/ notice must be cancelled.

8.24 Once the SPoC acquires the data he or she ensures it complies with the authorisation or notice and thereafter provides the data to the applicant.

The National Anti-Fraud Network (NAFN) – Local authorities

8.25 The Protections of Freedoms Act 2012 introduced an additional safeguard for the 429 local authorities in England and Wales, Scotland and Northern Ireland which have the power to acquire communications data. Under this safeguard, authorisations granted or notices served do not have effect until such time as a relevant judicial authority has approved the authorisation or notice, or any renewal.

8.26 To standardise the process by which applications are made, all local authorities are required to channel their submissions to acquire communications data through the SPoC at NAFN. NAFN's role is to ensure that the requests are legally compliant.

Urgent oral applications

8.27 Authorisations and notices must be given in writing although, in urgent circumstances, an application and its authorisation can be handled orally. Such circumstances include:

- where there is an immediate threat to life such that a life might be endangered if the application was made in writing;
- an urgent operational requirement where data acquired within 48 hours would assist with the prevention and detection of serious crime, and operational opportunities might be lost if the application was made in writing; or
- a time-critical threat to national security.

Examples of the use of urgent oral applications

8.28 As above, it is helpful to provide some examples of when such applications might be used:

- An urgent operational requirement would include situations when children were at immediate risk of being abused or otherwise significantly harmed. A typical example of this would be when a young girl has entered into an online relationship with a person purporting to be a boy of her age and leaves home to meet this individual, perhaps at a pre-arranged time and location. If it is suspected that the girl's contact is an adult who intends sexually to exploit her, the police could acquire communications data, using the urgent oral procedures, to identify any relevant online or telephone contact. This could include possible information as to the location of the child and the suspected adult.

- An urgent operational requirement would include attempts to locate and arrest those suspected of committing serious offences, such as importing illicit drugs. The investigators would need to demonstrate how the communications data would assist with the prevention and detection and that, without the use of the urgent oral procedures, operational opportunities to arrest the suspects and seize the drugs would be lost.

- A time-critical threat to national security could arise during the immediate aftermath of a terrorist attack, when law enforcement investigators seek to confirm whether an arrested terrorist suspect acted with others who may continue to pose a threat to the public. The urgent oral process typically will be invoked to acquire call and location data without delay.

8.29 The urgent oral process can only be used whilst the urgent situation subsists. Once the case for urgency has ended, the written process must be used for subsequent applications.

Additional protections – certain professions

8.30 As already highlighted, communications data acquired and disclosed under RIPA does not include content. Nonetheless, the DP must consider 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.

8.31 The 2015 Acquisition and Disclosure of Communications Code of Practice (paras 3.72-3.77) requires applicants to give special consideration to requests for communications data 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.

8.32 Public authorities must record the number of such applications and report to the IPC annually. In 2017, public authorities advised that they had made a total of 755 applications to acquire data which related to persons who held sensitive professions. It is fair to say that a significant proportion of those applications would have been categorised incorrectly as a consequence of clerical error or the applicant's misunderstanding about the subject's profession.

8.33 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 communications data requests were made in an attempt to attribute phone numbers or emails addresses to perpetrators.

8.34 Given the public interest in a free press, save when there is an immediate threat to life, applicants cannot use the provisions of RIPA to acquire data which is intended or is likely to identify journalistic sources. Instead, law enforcement agencies must now apply to a court for a production order. IPCO inspectors found no instances in 2017 of RIPA being used improperly to identify journalistic sources.

How IPCO oversees these powers

8.35 The acquisition of communications data is overseen across the annual IPCO programme of inspections. The larger users of communications data, such as police forces, are inspected at least annually. Smaller users are inspected less frequently, but at least once every two years. Typically, an inspection takes between one and four days to complete and involves from one to four inspectors depending on the size of the authority and the volume of data requested.

8.36 There were 61 inspections in this context during 2017. Two were at the intelligence agencies, 44 at law enforcement agencies, 14 at other public authorities and there was one inspection of NAFN (for local authorities).

8.37 IPCO also has a role in overseeing errors committed by public authorities in acquiring communications data (see the Errors and Breaches Chapter)

Inspection methodology

8.38 Prior to an inspection, the inspectors review the errors which have been reported to the IPC over the course of the relevant period and consider the materials the public authorities are required to make available no later than two weeks before the inspection.

8.39 The inspections involve a review of (i) a representative sample of the requests for data; (ii) the actions of the SPoC, including advice offered to the applicant and the DP; (iii) the recorded considerations of the DP, which should include a necessity and proportionality assessment; (iv) the use made of the acquired data; and (v) other relevant matters, such as whether there is a central record of documentation and the effectiveness of any recording and reporting of errors resulting from the acquisition or disclosure of the data.

8.40 Many of the larger public authorities manage the process of acquiring, disclosing and retaining data on a secure, auditable 'workflow' database. An interrogation of these workflow systems through query-based searches enables the inspectors to analyse large volumes of applications.

Inspection reports

8.41 The inspectors' findings are reflected in a template report which is provided to the authority. The report focuses principally on compliance with the legislation and the code of practice, and whether data is being acquired lawfully for a statutory purpose which the organisation is entitled to use.

8.42 Any findings of non-compliance are likely to result in recommendations. These are colour-coded depending on the level of non-compliance:

- Red recommendations address areas of immediate concern, including serious breaches or incidents of non-compliance with RIPA or the CoP;
- Amber recommendations focus on non-compliance of lesser seriousness, but which could nonetheless lead to breaches; and
- Green recommendations highlight where efficiencies and effectiveness could be improved.

8.43 Following receipt of the report, the SRO must respond to the recommendations, outlining whether they are accepted and detailing any proposed remedial action.

Findings

8.44 During the course of the year, all the public authorities inspected demonstrated an acceptable level of compliance but the SROs have been encouraged to consider the detailed recommendations with care, and to implement the inspectors' advice.

8.45 In 2016, 55 authorities received 235 recommendations (10 Red, 144 Amber and 81 Green). The 235 recommendations resulted from 68 inspections, an average of 3.45 recommendations per public authority.

8.46 In 2017, 39 authorities received 104 recommendations (7 Red, 68 Amber and 29 Green). The 104 recommendations resulted from 61 inspections, an average of 1.7 recommendations per public authority.

8.47 The recommendations can be placed in broad categories, although the seriousness of each individual recommendation within a category may vary. Some recommendations address more than one issue and may therefore have been included in more than one category:

- Applicants or DPs failed adequately to address the question of necessity (21);
- Applicants or DPs failed adequately to address the question of proportionality (29);
- Applicants or DPs failed to address the likelihood of collateral intrusion (29);
- Unreliable or inaccurate recording of errors (8);
- Erroneously acquired data was not destroyed (1);
- Insufficient consideration of sensitive professions (19);
- Improvements were required to the records for urgent oral applications (12);
- DPs' reasons were not sufficiently tailored to the application ('boiler plate' reasons) (4);
- DPs did not review applications promptly or their reasons failed to address the requirements of the code of practice (5);
- DPs failed to justify the grading of priority applications (4);
- The independence of DPs was called into question (10). As a consequence of recurring matters relating to a lack of DP independence, the Commissioner asked two Chief Constables to explain their non-compliance. In both instances, structural and personnel changes were satisfactorily implemented as a result.

9. Bulk Communications Data

Description of powers and use

9.1 Bulk Communications Data (BCD) is a large quantity of communications data acquired from communications service providers (CSPs), the vast majority of which is unlikely to be of any intelligence interest. It is also sometimes known as 'bulk acquisition'.

Legislation

9.2 Previously the Secretary of State issued directions to CSPs, under s.94 of the Telecommunications Act 1984, which enabled the intelligence agencies, specifically MI5 and GCHQ, to obtain communications data in bulk. The power was first used at scale in the UK in 2001 after the attacks in New York on 11 September.

9.3 The IPA repeals the s.94 powers (insofar as they relate the bulk acquisition of communications data) and replaces them with bulk acquisition warrants. Chapter 2 Part 6 IPA enables the Secretary of State to issue a bulk acquisition warrant once it has been approved by a Judicial Commissioner. However, for 2017 the relevant provisions of the IPA had not come into force and we were only concerned in this Report with the s.94 powers. Although there is no code of practice governing the use of s.94 powers, the government published handling arrangements in 2015.[46]

9.4 IPCO took responsibility for overseeing the s.94 Directions in September 2017.

Utility

9.5 The government published a paper entitled the 'Operational Case for Bulk Powers' in order to inform the public about the use of these provisions.[47]

9.6 In brief, the paper suggests that bulk communications data enables the intelligence agencies to identify the links and frequency of contact between subjects of interest and their associates, and to uncover networks, in order to narrow down likely targets more quickly than otherwise would be the case. Identifying these links can help indicate whether other investigatory powers, such as interception, are likely to be of use. This also allows the intelligence agencies to search for traces of activity by previously unknown suspects who surface in the course of an investigation, thereby revealing other potential threats that need to be investigated.

46 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

47 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

9.7 In the 'Operational Case for Bulk Powers', the government gives a number of examples which describe how the powers have been of assistance in, for instance, countering terrorist activity when combined with complex analysis. These examples include preventing bombings, kidnaps and mass casualty attacks on aviation, and it is explained how they assisted in catching perpetrators after an attack. It is contended that if the intelligence agencies had had to rely on acquiring targeted communications data these operations would have had different – and worse – outcomes.

9.8 In his review of bulk powers[48] Lord Anderson concluded that:

"Bulk acquisition has been demonstrated to be crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation. The case studies provide examples in which bulk acquisition has contributed significantly to the disruption of terrorist operations and, though that disruption, almost certainly the saving of lives.'

Bulk acquisition is valuable as a basis for action in the face of imminent threat, though its principal utility lies in swift target identification and development.

The SIAs' [Security & Intelligence Agencies] ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means.

Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition."

Statistics of use of powers

9.9 There were 15 extant s.94 Directions in 2017 which related to MI5 and GCHQ.

9.10 MI5 made 20,503 applications in 2017 to access communications data obtained pursuant to s.94 directions. These applications related to 98,798 items of communications data.[49]

9.11 In 2017, 9.4% of GCHQ's end product reports included material acquired under s.94.[50]

The authorisation process

9.12 Authorisation is a four part process. Some of the steps may happen simultaneously:

- the agency identifies and describes the bulk communications data it considers it needs to meet its operational objectives;
- the agency identifies the relevant public electronic communications network/s (PECN)[51] and consults with them to assess whether acquiring specific communications data in bulk

48 Report of the Bulk Powers Review, August 2016 – https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

49 In 2016, MI5 made 19,995 applications to access bulk communications data. These applications related to 97,382 items of communications data.

50 In 2016, 7.5% of GCHQ's end product reports included material acquired under section 94.

51 A public electronic communications network (PECN) is defined in section 151 of the Communications Act (2003) as: 'an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.' This excludes those who provide services or networks that are not available to members of the public (typically, private networks and other bespoke services). PECNs tend to be bodies which would be referred to as CSPs under RIPA, the IPA and in other parts of this report. For simplicity we refer to them as CSPs in this chapter.

from them is reasonably practical and the extent to which the data required is inextricably linked with other data;

- the agency assesses whether the data can be made available by means of a s.94 direction (this process will involve further liaison with the CSP); and
- the agency determines whether the bulk acquisition of communications data is appropriate under a s.94 direction and, if it is, prepares a detailed submission for the Secretary of State (Home Secretary or Foreign Secretary).

The submission

9.13 The submission is sent to the Secretary of State by the head of MI5 or GCHQ. They provide information which will enable the Secretary of State to decide whether (i) acquiring and retaining the relevant BCD is necessary in the interests of national security or international relations; (ii) whether the acquisition, retention and selection would be proportionate to what is sought to be achieved; (iii) whether there is a less intrusive method of obtaining the information or achieving the national security objective; and (iv) the level of collateral intrusion that will be caused by acquiring and exercising the BCD warrant the agency is requesting.

9.14 The submission will rehearse any national security or international relations arguments as to why the Secretary of State cannot lay the Direction before both Houses of Parliament in accordance with section 94(4) of the Telecommunications Act.

9.15 If the Secretary of State agrees the Direction, it is served on the relevant CSP. Before the CSP provides any data to the agency, they make arrangements to ensure that the data is shared securely.

9.16 Both MI5 and GCHQ have kept a central record of the s.94 directions given by the Home Secretary or Foreign Secretary. This central record includes (i) the date the direction was given; (ii) the name of the Secretary of State giving the direction; (iii) the CSP to which the direction relates and the date the direction was served on the CSP; and (iv) a description of the activity the CSP is required to carry out.

How IPCO oversees these powers

9.17 The Prime Minster wrote to the then Interception of Communications Commissioner (IoCC) in January 2015 to ask him to extend his oversight to include directions given by a Secretary of State under s.94. The Prime Minister acknowledged that the IoCC had previously provided limited non-statutory oversight of how MI5 used one particular set of directions and now wished to extend that oversight.

9.18 In October 2015 the IoCC started his first review of the directions issued under s.94 with a view to (i) identifying the extent to which the intelligence agencies used these directions; (ii) assessing what a comprehensive oversight and audit function of s.94 directions would look like; and (iii) assessing whether the systems and procedures in place for s.94 directions were sufficient to comply with the legislation and any relevant policies.

9.19 On 4 November 2015, the Home Secretary publicly avowed the powers to acquire bulk communications data in a statement to the House of Commons concerning the then draft Investigatory Powers Bill.[52]

9.20 IPCO has overseen acquisition of bulk communications data under the s.94 regime through on-site inspections. We undertook five BCD inspections in 2017.

9.21 During our inspections in both MI5 and GCHQ we have examined all extant s.94 directions and the supporting documentation.

9.22 Our inspections focus on:

- the application procedures relating to s.94 directions, including how the agency dealt with necessity and proportionality;
- the administrative process for the operation of the directions;
- the procedures for reviewing, modifying and cancelling s.94 directions; and
- the activity carried out pursuant to the directions.

9.23 We also examine the procedures in place to access the data. The inspectors interview those in charge of intelligence operations, senior managers authorising access, analysts in operational teams and those who manage and carry out audits of the access.

Findings

Quality of submissions, directions to CSPs and reviews

9.24 During our inspections in both MI5 and GCHQ, we concluded:

- the submissions to the Secretary of State from MI5 and GCHQ, respectively, were highly detailed, made explicit why the acquisition, retention, access to and analysis of BCD was required in the interests of national security, and set out the intelligence requirements they were seeking to address;
- the submissions included extensive detail as to how the BCD would address operational requirements, the expected value of the intelligence derived from it and why there was no viable alternative to the proposed acquisition of BCD. The two intelligence agencies also provided examples from recent operations where using BCD had been critical;
- the supporting documentation and each s.94 direction itself made explicit that the relevant Secretary of State was giving the direction in person, and each was signed;
- the s.94 directions specified the communications data which was the subject of the direction by using terminology familiar to the CSPs;
- the directions signed by the Home Secretary and Foreign Secretary and served on the CSP made explicit that MI5 and GCHQ would carry out a review of the direction every six months and share these reviews with the relevant Secretary of State;
- the six monthly reviews for the 2017 period of all the extant s.94 directions were comprehensive and contained:

52 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf

- a summary of the data that had been retained, and how the BCD was to be handled and analysed;
- an assessment of the value and operational advantages that access to this data would provide for the relevant operations and investigations;
- the operational justification and legal basis for continued retention and use;
- the process for members of staff within the agency to access the BCD;
- an assessment of the collateral intrusion by the intelligence agency in possession of, and having access to, the BCD;
- an update on the ongoing IPT case; (see later reference in this Chapter)
- confirmation of ongoing liaison with the CSP which was the subject of the s.94 direction; and
- consideration of the issues and consequences of alternative forms of acquisition and the potential contingencies involved.

Access to the bulk communications data retained by the agency

9.25 The last IOCCO annual report described that distinct processes have developed in MI5 and GCHQ to access bulk communications data, both of which include consideration of the principles of necessity and proportionality as set out below. The different procedures mean it is not possible to provide comparable statistical information about access to, and use of, bulk communications data.

9.26 GCHQ treats all operational data gathered from a variety of different sources in the same way. Where there is an operational requirement to access operational data which will include bulk communications data, an analyst must justify why the access and examination of the data are necessary and proportionate. This is a three-stage process which covers (i) why the search is necessary for one of the authorised purposes, for example, in the interests of national security; (ii) an internal cross-reference number which equates to the specific intelligence requirement and priority for the search; and iii) the necessity and proportionality justification for accessing the data.

9.27 During inspections into the selection of bulk communications data for examination by analysts at GCHQ, our inspectors review the breadth and depth of the internal procedures and audit a number of individual requests made by analysts. They have been satisfied that, in the individual requests examined, the analysts had justified properly why it was necessary and proportionate to access the communications data.

9.28 Previous IOCCO reports[53] commented on the process at GCHQ for selecting and examining intercepted material and related communications data.[54] The process for selecting and examining bulk communications data is essentially the same. We draw, therefore, the same conclusion as in previous years, namely that although the selection procedure is carried out carefully and conscientiously, the process relies mainly on the professional judgment of analysts, their training and management oversight.

53 See for example Paragraphs 6.37 to 6.40 of the March 2015 Report.

54 See section 20 of the Regulation of Investigatory Powers Act 2000 for definitions of 'intercepted material' and 'related communications data' http://www.legislation.gov.uk/ukpga/2000/23/section/20.

9.29 GCHQ carries out robust retrospective audit checks. The senior managers we interviewed as part of the inspection process explained and demonstrated in some detail how the audit processes work and the function of GCHQ's Internal Compliance Team who carry out random ex-post facto audit checks of the analysts' justifications for the selection of bulk communications data. In addition, GCHQ's IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use. This year it was recommended that GCHQ initiates work to update its systems to enable our inspectors to carry out a more thorough audit similar to that facilitated at MI5 and which we describe below.

9.30 MI5 has a policy and procedure for accessing the bulk communications data, acquired and retained by the agency as a consequence of s.94 directions, which substantially mirrors that set out in Chapter 2 Part 1 RIPA and the code of practice for the Acquisition and Disclosure of Communications Data.[55]

9.31 The investigator/analyst sets out in an application why it is necessary and proportionate to access the data. A designated person (DP) of appropriate seniority in the organisation considers whether to give authority for access to the data MI5 retains.

9.32 During inspections, our inspectors have access to the system used by investigators and analysts at MI5 to apply to access the bulk communications data and we undertake random sampling and run query-based searches on the system. For example, inspectors might use the system to show us every application which included the word 'journalist'. This means that our inspectors can (i) evaluate the analysts and investigators' necessity and proportionality considerations; (ii) examine particular operations; and (iii) identify requests for more sensitive data sets or those requiring data over longer time periods.

9.33 Overall we concluded that the MI5 applications we examined were submitted to a notably high standard, and particularly they satisfied the principles of necessity and proportionality.

9.34 In the latter part of 2017 we undertook work in addition to the scheduled inspections, in order to review the systems used to acquire, retain and manage access to BCD by MI5 and GCHQ. These included the following topics:

- security governance arrangements;
- information security frameworks and policies;
- training and security awareness;
- physical security;
- access management for users (e.g. analysts);
- network access controls;
- system monitoring;
- the deletion of data from the systems; and
- logging, monitoring and audit trails.

9.35 This additional work will continue through 2018 and we will publish our findings in a report to the Prime Minister.

55 See Chapter 3 – The General Rules on the Granting of Authorisations and Notices https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

IPT Case 15/110/CH

9.36 During 2017 our inspectors assisted the Investigatory Powers Tribunal (IPT) with a request made about case IPT/15/110/CH in relation to the acquisition and use by the intelligence agencies of BCD (pursuant to s.94 directions) and the bulk personal data regime. The issue before the IPT was the lawfulness of the BCD and BPD regimes in domestic and European law. The existence of bulk personal data was first publicly avowed in March 2015 and bulk communications data in November 2015.[56]

9.37 The IPT, in carrying out its functions, is empowered to request the IPC to provide all such assistance, including giving an opinion on a matter before the tribunal, as the IPT requires. The IPT requested assistance in verifying the results of numerous searches the claimants had requested the agencies undertake as part of the 'discovery process', in order to determine what data was held in relation to specific entities (for example, communication addresses and travel information). This investigative work took our inspectors many days to complete and resulted in a detailed report that was submitted to the IPT.

9.38 The IPT provided its final judgment in July 2018,[57] finding that:

- many of directions made prior to October 2016 by the Foreign Secretary to Communications Service Providers to provide BCD to GCHQ were not in accordance with law;
- (by a majority) the regime in respect of sharing of BCD/BPD with foreign agencies complied with Article 8 of the ECHR;
- the regime in respect of sharing BCD/BPD with industry partners complied with Article 8 ECHR; and
- the steps taken by way of collection , retention and use of BCD or BPD by the authorities complied with the requirements of proportionality pursuant to Article 8 ECHR and EU law.

9.39 Addressing the adequacy of the oversight of this power, the tribunal recognised that Sir Stanley Burnton (IoCC) had identified many of the same issues as regards GCHQ's submissions and authorisations by the Foreign Secretary as the tribunal, and 'did not conclude there was any inadequacy of supervision by reference to the (IOCCO) July 2017 Review'.

9.40 Two specific questions concerning the oversight of access to, and sharing of BCD (and Bulk Personal Datasets) were addressed:

"As to the Commissioner's knowledge of the number of internal contractors with access, the tribunal determined "the absence of such precise knowledge does not in our judgment detract from the adequacy of their oversight, which in this regard was in place and, so far as checking conduct by contractors as well as employees, was plainly exercised."

56 There remains an outstanding reference to the CJEU in this case, on whether security and intelligence agencies use of the powers to acquire BCD is in scope of EU law and, if so, would the requirements outlined by the CJEU in the Watson case apply to the BCD regime.

57 https://www.ipt-uk.com/judgments.asp

- on the linked issue of knowledge of sharing with industry partners, the tribunal observed 'What is however significant is that the Commissioners did not know about sharing with industry partners by GCHQ... but it plainly forms a minimal part of the operation of BPD/BCD, and an even more miniscule part of the work of the Agencies subject to the Commissioners' oversight. This is a failing in the operation of oversight and in the duty of GCHQ to bring it to the Commissioners' attention. However, given the totality of the work done both by the Commissioners and by the Agencies, we do not conclude that this amounts to or illustrates a systemic failure.'

10. Bulk Personal Datasets

Description of powers and use

10.1 A bulk personal dataset(BPD) is a collection of data that includes information which identifies a large number of people, for instance by their names or addresses. Most will not be of interest to the intelligence agencies. These datasets may include, for example, the electoral roll or the telephone directory.

10.2 Historically (including the 2017 period to which this report relates), there was no statutory framework as to how the intelligence agencies retain and use bulk datasets. This meant that they each have developed discrete internal processes for the retention and use, as well as the internal review, of BPD.

10.3 The intelligence agencies use BPDs in a variety of ways to research individuals of interest. BPDs hold a considerable quantity of information that enables an agency to build a profile of someone in whom they are interested without using more intrusive methods. The intelligence agencies suggest that examining these datasets helps limit the intrusion into a target's privacy, whilst accepting that self-evidently there is intrusion into the privacy of members of the public who are not targets and whose data is captured in the BPD, but will not necessarily be selected for examination. However, database search results are structured so that the officer does not view the details of other individuals if their data is not relevant to the particular search. It is suggested this greatly limits any collateral intrusion because it very significantly reduces the extent to which analysts will ever need to look at the personal details or identities of general members of the public.

10.4 Lord Anderson's review[58] contains numerous examples of BPDs and how they have been used by the intelligence agencies, including:

- Law enforcement and intelligence agencies: datasets containing operationally focused information;
- Travel: datasets containing information which provides details of travel activity;
- Communications: datasets enabling the identification of individuals from communications data, e.g. a telephone directory;
- Finance: datasets allowing the identification of finance-related activity;
- Population: datasets providing population data or other information which could be used to help the task of identification, e.g. passport details; and
- Commercial: datasets providing details of corporations / individuals involved in commercial activities.

58 Report of the Bulk Powers Review, August 2016 – https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

10.5 Part 7 IPA, which came into effect in August 2018, provides for an intelligence agency to retain a bulk personal dataset if (i) the agency obtains a set of information that includes personal data relating to a number of individuals; (ii) the nature of the dataset is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in exercising its functions; and (iii) after any initial examination of the contents to determine whether it is a BPD that is necessary and proportionate for them to retain, the agency retains the dataset for the purpose of the exercise of its functions, and the set is held, or is to be held, electronically for analysis in the exercise of those functions.

10.6 Under the IPA, any agency holding any BPD must set out a clear case for its retention, or retention and examination and ensure protective safeguards are in place to prevent any misuse. Datasets which contain a substantial proportion of sensitive personal data, as defined by the Data Protection Act (1998), require additional safeguards. The intelligence agencies must not hold BPDs for longer than is necessary for the proper exercise of their functions, under any circumstances.

10.7 The IPA allows the intelligence agencies to apply to retain, or retain and examine, bulk personal datasets under either a 'specific' or 'class' warrant. These warrants will be authorised by the Secretary of State and they require approval by a JC. A class warrants will describe the class of BPDs to which it relates. Datasets that include health records, or a substantial proportion of sensitive personal data, cannot be retained, or retained and examined, under a class warrant, and the agency would have to apply for a specific warrant.

Statistics of use of powers

10.8 We are prevented from giving statistical information about the intelligence agencies' use of BPDs in a public document because of the secrecy provisions. The IPC intends to keep the suggested need for this restriction on publication under review, and in due course this may form the basis of recommendations to the Prime Minister. The Confidential Annex to this report gives details about the number of BPDs held and how frequently they have been accessed.

The authorisation process

10.9 As set out above, the intelligence agencies have developed their own internal procedures for retention, examination, deletion and internal review.

How IPCO oversees these powers

10.10 In November 2014 the Prime Minister gave direction to the Intelligence Services Commissioner (ISCom) to oversee the intelligence agencies' acquisition, retention, use, disclosure and deletion of BPDs. New provisions under the IPA supplement this direction. The JCs additionally perform a double-lock function for new applications to retain, or retain and examine. BPDs and IPCO will include their use of BPDs in the regular inspections of the intelligence agencies.

10.11 In 2017, Sir John Goldring led the inspections of BPD at GCHQ, MI5 and SIS (nine inspections). These were structured as set out below.

10.12 We conducted an initial inspection at each agency in the spring, as part of a general inspection. Over the summer we undertook specific inspections of BPD sharing. In December, we held focused inspections of BPD holdings at each agency. This exercise comprised a random audit of BPD holdings and a review of the data handling processes

and policies, as well as specific consideration of more complex datasets. Independent of this, the intelligence agencies provided a series of detailed briefings on their plans to develop the BPD regime in order to achieve compliance with the IPA.

10.13 In practice at inspections we (i) look at the authorisation paperwork, which differs at each agency; (ii) speak to the operational leads who use and 'sponsor' the data; (iii) review the minutes from the data retention panel meetings; and (iv) speak to the analysts who run tasks and searches on the data.

10.14 We identified three areas of particular note concerning the policies and procedures for using and disclosing BPDs.

10.15 First, we were concerned that GCHQ was not clearly identifying all the BPDs held. We probed this at the December inspection and briefing sessions.

10.16 Second, we reviewed how the intelligence agencies identify and record sensitive personal data. Section 202(b) of the IPA stipulates that an agency may not retain a bulk personal dataset under a class authorisation if a substantial proportion of it consists of sensitive personal data. This means that whenever the dataset contains a substantial proportion of sensitive personal data, it must be authorised individually under a specific warrant. We have been briefed by the intelligence agencies as to how they will ensure that any sensitive personal data is appropriately identified and the risks assessed carefully. We will review this process with particular care during our 2018 inspections.

10.17 Third, building on specific 'sharing' inspections, we plan to conduct a detailed review of how the intelligence agencies work with parties acting on their behalf. This potentially includes contractors, industry partners and academics to understand the role these individuals play and any access they are afforded to sensitive data.

Findings

Assessment of record-keeping

10.18 We are content that GCHQ is working to capture all its bulk data holdings, and will in due course provide more clarity on the nature of the complex BPDs, and how they are handled, at future inspections. It is worth noting that GCHQ does not operate distinct safeguards for BPDs. It handles BPD using the same techniques as for other sensitive information they hold. It is vital that there is an accurate understanding of the BPDs that are held by the intelligence agencies and that appropriate warrants issued under the IPA are in place to retain and access the information.

10.19 Previous Intelligence Services Commissioners have been satisfied with the records kept on BPDs. However, we have made a number of recommendations to improve the clarity of the records. During the inspections, the documentation is not viewed in isolation and the staff briefings and interviews have led us to conclude that this sensitive data is being held and used appropriately. Nonetheless, the documentation should be a reliable, free-standing source of information in order to demonstrate that the relevant issues have been properly considered as regards the retention, investigation and handling of this data. There are improvements to be made in this area.

10.20 Our recommendations aim to standardise the record-keeping, so that the authorisation paperwork is uniformly clear on what is being retained and its potential use. We have suggested that the documentation sets out the restrictions on access. The intelligence

agencies must ensure that any sensitive casework is explained in full and that it is adequately protected. Sensitive information should be assessed in accordance with a clear and consistent policy. Finally, records should be clear on where a dataset is to be retained, and that the data within it will be deleted after a defined length of time, to be replaced by more up-to-data material. These recommendations do not reflect systematic failings but instead result from a need for a consistent approach. It is recognised that the present paperwork does not necessarily reflect the extent of the present storage and access arrangements and we are aware of the work being undertaken to implement our recommendations.

10.21 We have also made recommendations in relation to the review process. Each agency has an independent panel which systematically reviews the justification for all BPDs. This process typically relies on a case for retaining the data that is drafted and presented by the 'data sponsor', supported by an analysis of the statistics concerning the use of the specific dataset. We have recommended that the intelligence agencies revise their approach to capturing and documenting 'value', providing specific examples of use, to ensure that this is clear and consistent on review. We have recommended that they take and keep fuller minutes of the decisions of the independent panels, including the reasons for approving or rejecting the request to retain the data. This process should be used to review the access restrictions on any BPD the intelligence agencies hold, and to help determine whether they need to retain the entire dataset. They should record the reason for deleting any data. This process will, in future, feed into any applications to renew the retention, or retention and examination of a BPD under the JC double-lock procedure.

Assessment of necessity and proportionality

10.22 The intelligence agencies have demonstrated that BPDs are important in enabling them to perform their statutory functions. We are persuaded of the necessity and proportionality for retaining BPDs in general, and particularly in respect of those cases we reviewed in 2017. However, we were not fully satisfied with the adequacy of records kept in relation to BPDs, especially as to retention and use.

10.23 From our discussions with analysts and authorising officers, we were afforded evidence that they gave a high level of consideration to necessity and proportionality in relation to the use and retention of this data. We made a number of recommendations in this area and throughout 2017 observed these being implemented either in general working practices or by way of the design work for the IPA regime. The intelligence agencies' engagement was impressive; SIS, which holds the highest number of datasets, was notable in this respect.

10.24 One key area to consider on BPDs is how to the intelligence agencies articulate their approach to collateral intrusion of privacy. The systems each agency uses are designed to limit intrusion and they have live audit processes to ensure officers are accessing data appropriately. However, we were not content with the manner in which they articulate these intrusion considerations. In particular, we were not persuaded that GCHQ officers had demonstrated an adequate understanding of the intrusive nature of their work. It is necessary that officers set out their understanding of the impact that retaining and using BPDs has on the right to privacy, even when all appropriate steps are taken at an operational level to limit intrusion to that which is strictly necessary for the particular task.

10.25 The articulation of intrusion at the three intelligence agencies is based on somewhat differing interpretations of the impact on individuals' privacy of this activity. We have recommended that the intelligence agencies adopt a common structure, based on the following considerations:

- the intrusion into the privacy of members of the public as a result of holding the dataset within the agency's systems, prior to access to the data. This depends on the nature of the data, the public expectation of privacy, and duration for which the data is held, amongst other factors; and

- the intrusion resulting from access to the data by agency staff, which may include collateral intrusion for those who are not subjects of interest. For example, a search for a specific individual may also return details for people with similar names or addresses.

Ingestion delays

10.26 Ingestion is the process by which a BPD is processed so as to make it available for analysis. In his 2015 and 2016 reports, Sir Mark Waller noted his disquiet at the delay in ingesting data the intelligence agencies had acquired into the analytical systems. It is reassuring to note that the 2017 inspections did not echo these concerns, largely because the intelligence agencies have made changes to their ingestion processes on the basis of Sir Mark's recommendations. It is worth remarking in passing that the IPA introduces BPD warrants for any data retention or use, but not its acquisition. Under ss.220-4 IPA, before obtaining a warrant an agency may carry out a preliminary examination of the dataset to establish whether it is a BPD, and whether it is of a nature that the agency wishes to retain, or retain and examine. This initial examination period is up to three months if the information was created in the UK, and up to six months if it was created outside the UK. This means the agency can begin to ingest the data while obtaining an authorisation to retain and examine the set, but it will not be possible to examine it for intelligence operations or investigations until the relevant warrant is in place. However, data ingestion remains technically complicated and we will review both compliance with the IPA deadlines and any ingestion delays for warranted datasets.

IPT Case 15/110/CH – Adequacy of ISComm oversight

10.27 BPDs have been the subject of significant public interest since they were publicly avowed in March 2015, and were the subject of a case brought before the Investigatory Powers Tribunal (IPT), along with the acquisition of communications data in bulk. At a hearing in September 2017, the IPT considered evidence in relation to a challenge against the lawfulness of sharing BPDs with foreign governments or industry partners. We co-operated fully with the IPT on this case, providing both classified and unclassified evidence in relation to oversight.

10.28 In its judgment[59] and specifically with regards to the complaint that ISComm did not have a team of inspectors considering this area and failed to obtain independent technical advice, the IPT set out:

"There is no doubt that he (Sir Mark Waller) did carry out supervision, with diligence and regularity, and it can be seen by simply reading his reports how detailed he was in his consideration, and how many detailed and technical points he explored with the Agencies.

His aim, as he explained it to Parliament, was to make sure that he had personal oversight, which was not delegated to others, and it is plain that he frequently required and received regular explanations. Another Commissioner might have taken a different view as to the appropriateness of technical assistance, but the perceptive nature of his comments in his reports, and the fact that he often required changes and improvements, show that he had, and was able to have, a hands-on approach."

10.29 The IPT judged that while the new regime might be better, that does not mean the old regime was inadequate:

"In our judgment the fact that the new supervision regime now has the benefit of a team of experts, as a result of the statutory provision under the new Act, may be an improvement, though it is not yet tested, but it does not, in our judgment, evidence prior inadequacy."

59 https://www.ipt-uk.com/judgments.asp

11. Intelligence Services Act 1994 – Section 7 Authorisations

Description of powers and use

11.1 Section 7 of the Intelligence Services Act 1994 (ISA) refers to activity that SIS and GCHQ carry out outside the British Islands. Under s.7, the Secretary of State may authorise SIS or GCHQ to undertake a specific act or a range of activities, such as those to support covert activities overseas. It is important to understand that the authorisation removes any liability under the criminal or civil law of the United Kingdom for what is done. The agency needs to demonstrate that the activity is necessary for the discharge of one or more of its functions. The Government sets the requirements and priorities for GCHQ and SIS centrally.

11.2 The activities that can be authorised under s.7 are broad. They may be highly intrusive or they may result in no interference with privacy. Where the activity is intrusive, the agency requesting authorisation must make this clear to the Secretary of State in its application and implement an internal senior-level scrutiny process to demonstrate clearly how they have considered necessity and proportionality.

11.3 GCHQ and SIS often act under class authorisations, which cover a type of activity rather than a specific operation. Depending on the scope of the authorisation, an internal approval process may be implemented which seeks to ensure that the necessity and proportionality of each operation is considered and documented.

The authorisation process

11.4 When applying for an authorisation, each agency must demonstrate to the Secretary of State (in this context the Foreign Secretary), how the suggested activities meet government priorities in line with the agency's statutory functions, and why they are necessary, proper and reasonable. In addition to ensuring the intelligence agencies act only within the authorisation from the Secretary of State, the authorisation under s.7 removes personal liability under UK law where an officer has been acting in good faith within the parameters of the authorisation.

How IPCO oversees these powers

11.5 Sir John Goldring, the deputy IPC, leads this area of oversight. IPCO conducted two inspections of GCHQ and SIS, in the spring and autumn of 2017, along with two of SIS's overseas stations in early 2017. We carried out separate inspections of the FCO as regards its work with SIS and GCHQ during the summer of 2017.

11.6 In recent years, the Intelligence Services Commissioner has worked to gain a comprehensive understanding of the activities carried out under s.7. Building on this valuable work, we have focused our inspections on the authorisation and review processes, and particularly whether the Foreign Secretary was provided with a proper understanding of the activity that would be sanctioned by the authorisation.

11.7 We interview a wide range of relevant members of staff, including (i) internal authorising officers, (ii) the staff at stations who use or implement the authorisations and (iii) in-house staff at GCHQ. We look at the authorisations and approvals, and any related paperwork. We also speak to the lawyers. The authorisations at the FCO are similarly reviewed (in 2017 we looked at these during the second half of the year).

Findings

11.8 The internal and external review processes have been the subject of impressive continued improvement. However, GCHQ and SIS should establish a clearer and more complete record of all the actions conducted under s.7 authorisations. A particular concern is that the internal approvals do not always document adequately the potential intrusion into privacy.

11.9 The intelligence agencies seek to authorise their dealings with foreign intelligence services under s.7. We are content that work conducted under these authorisations is managed satisfactorily to ensure compliance with UK and international law. This area is carefully scrutinised, and the assurances provided to the intelligence agencies are supported by the close working relationships of the staff at a high and working level. We were impressed by the level of care and dedication SIS showed to supporting and mentoring foreign services. This is a significant area of work, which improves compliance and respect for human rights in a number of countries, and in a way which extends beyond areas of cooperation with the UK.

11.10 Ministerial oversight of the use by the intelligence agencies of covert powers is an important part of the FCO's role. We reviewed the processes they utilise to inform the Foreign Secretary of the relevant activity under s.7 authorisations. If the request is in broad terms, it is particularly crucial that the Secretary of State has a clear understanding of the range of activity that is contemplated. For the renewal process, the FCO provides a summary of the operations conducted but does not provide a full register of the activity carried out. The FCO receives monthly summaries from GCHQ and SIS of this activity, although these are not entirely consistent between the intelligence agencies. GCHQ, for instance, highlights all new, reviewed and deleted approvals under class authorisations, whilst SIS summarise all the submissions and warrants signed by the Foreign Secretary. SIS provides three or six monthly updates on specific operations, as requested by the FCO, and GCHQ sends a record of any legally privileged material that has been obtained during the course of relevant operations. FCO directors conduct an annual Strategic Risk Assessment with GCHQ and SIS operational directors and mission leads, addressing how operations are delivering on key mission areas. An SIS officer is seconded to the FCO, to ensure the reports are considered by the correct officials and to report back on any issues that arise, to ensure they are properly addressed.

11.11 We were not satisfied that the FCO has demonstrated a sufficient challenge to the submissions from SIS or GCHQ in this context, in particular when there is a lack of operational details or intrusion considerations. We accept that the FCO is involved in the early stages of an application for authorisation under s.7, and that this will lead to challenge at a senior level in the FCO before the submission is sent to the Secretary of State. This has the result that the FCO and the Secretary of State may have a greater level of knowledge of the operation – including the risks and safeguards – than is caught by the formal documentation. In our view, careful scrutiny by the FCO is a critical stage in this important process, particularly for

complex and sensitive operations and we are liaising with the FCO to improve oversight by, and on behalf of, the Secretary of State. This will be a focus of the inspections in 2018, when we intend to scrutinise the mechanics of ministerial oversight, and the adequacy of the information that is provided for this purpose.

Assisting parties

11.12 When GCHQ and SIS apply for a s.7 authorisation, they may intend that they are to be assisted by third parties whom they trust. Increased collaboration between UK intelligence agencies, in particular with counter terrorism, means that UK military personnel or MI5 officers are increasingly acting in support of other UK agencies, for example where they have a technical specialism. We have identified a number of cases where these partner agencies are named as assisting parties in the authorisation but the detail of their activity has not been articulated in the submission. The Secretary of State should be aware not only of the activity he is authorising but also who will carry it out. Submissions must identify which organisations or individuals it is proposed should assist the applicant agency, how they will provide that assistance and why this step is necessary.

Legally privileged material

11.13 GCHQ relies on class authorisations for a significant proportion of its covert activity. GCHQ suggested that the scope of these authorisations, which cover a varied set of activities against different targets internationally, makes it difficult to capture the likelihood of obtaining LPP material. We are not presently satisfied that this approach provides sufficient safeguards for LPP and we have recommended that operations which are assessed as being likely to result in a significant proportion of LPP material should not be conducted under these broad authorisations. We asked GCHQ to draft a separate application in relation to a particular operation where this risk was evident. This was reviewed at the following inspection. We will keep this practice under review, as we consider it is necessary to set out the likelihood of obtaining LPP material in the application and renewal documents.

Supplementary documentation and internal approvals

11.14 In general, we are satisfied with the approvals processes utililsed by the intelligence agencies. There are different types of authorisations, such as class authorisations and framework authorisations. What is planned and the likely intrusion is set out in detail, albeit it is critical that there is a clear link between the proposed actions and the individual authorisations.

11.15 We inspected the relevant internal paperwork at each agency. Althought the twin issues of necessity and proportionality are addressed satisfactorily, on occasion the risk of intrusion is not adequately explained. Furthermore, inappropriate language is sometimes used, and there were examples of internal documents being described incorrectly as ‘authorising’ an action which is being carried out under s.7. In a similar vein, in some cases the internal record sets out additional details and safeguards, and provides more information on the target of the operation. IPCO’s advice has been clear, namely that these records can only clarify activity authorised under s.7 and they cannot amend the terms of the authorisation or include additional actions. There must be no confusion in this regard.

11.16 We inspected some authorisations where the intelligence agencies had annexed information as part of the submission. On occasion, the intelligence agencies have later updated the annex to reflect operational requirements and target refinement. However, ISA does not provide for modifications to s.7. It follows that the status of these supplementary documents must be made clear.

CHIS standards

11.17 Sir Mark Wailer recommended that SIS improves its record keeping as to how the principles of the RIPA code of practice are applied to overseas agent running (CHIS). We requested and received several briefings about SIS's overseas CHIS activities, which have provided some initial insight as to how these operations are conducted. It is clear that the key issues in this context are considered, such as necessity and proportionality, intrusion into privacy, the sensitivites around LPP material, the use of vulnerable individuals or juveniles, and CHIS security and their general welfare. There are certain core documents (the Key Decision Record, the Record of Contact and the Operational Plan) in which these matters are set out, as well as in the s.7 submission. We intend to make this area a particular focus of attention in 2018.

Working with liaison partners

11.18 We reviewed the intelligence agencies' approach to working with other bodies and it is of particular note in this regard that SIS liaise and work jointly with the intelligence services of other countries. This liaison is conducted with care, and a premium is placed on local knowledge and experience, along with the need to react to local events such as political changes. It is clear that SIS suspend joint work of this kind whenever officers lose confidence in the safeguards that underpin the engagement and we particularly noted instances when SIS has temporarily suspended cooperation to safeguard an operation or a CHIS. The Secretary of State is appropriately appraised of these developments through Ministerial submissions or letters. However, we observed one occasion when GCHQ shared intelligence with a foreign partner on the understanding that SIS had a good working relationship with them and that a s.7 authorisation was in place. In fact, to the contrary, SIS had temporarily suspended both the engagement and the authorisation, pending assurance as to important matters. While there is no suggestion that GCHQ acted unlawfully, intelligence was passed without up-to-date awareness of the reliability of the other body. We have emphasised that SIS must ensure that they promptly share developments of this kind.

Unwanted material

11.19 During the course of their operations, the intelligence agencies are likely to obtain some material that does not meet a present or anticipated intelligence requirement. For example, this could include social material or information relating to a target's occupation. Operational requirements develop through the course of an authorisation, which can make it difficult to predict at the outset any material that will not be of intelligence value. When planning the operation, the officer must consider this issue carefully as part of the necessity judgement in relation to the intelligence that is being sought. In some cases, information may unexpectedly prove to have value as the operation develops. The agency will need to decide whether to retain all the data, or to delete a portion, in accordance with the data retention policies. Either approach may be proportionate, depending on the circumstances.

11.20 Each agency has clear policies for handing intelligence that has not been assessed to be of intelligence value. These policies set out the material they can retain and how, as well as the length of time for which, it is retained. Because of the complexity of the exercise, these policies are overlaid by the critical individual assessment of the value of the intelligence obtained in each case. We suggested that, whenever possible, submissions should include an outline of the nature of the intelligence that is likely to be obtained, the extent to which valueless material will be gathered and an explanation as to how it will be handled. It is necessary for the Secretary of State, particularly with the more wide-ranging authorisations, to be given a full understanding of the position.

12. Consolidated Guidance

Definition and process

12.1 The Consolidated Guidance sets out the principles governing the interviewing of detainees overseas, together with the passing and receipt of intelligence relating to them. The Guidance seeks to ensure that decisions in this context are consistent with UK and international law. Principally, the Guidance reflects concerns about the use of torture, and cruel, inhuman and degrading treatment (CIDT), as well as the general standards of arrest, detention and treatment.

12.2 The Consolidated Guidance covers an area, therefore, in which both the detainee and individual officers face wholly different risks: the detainee of unacceptable treatment and the officers of legal liability for any unlawful treatment of the former. By way of a stark example, if an officer is involved in a case in which the detainee is tortured, he or she could face civil or criminal proceedings for what occurred. The Guidance expresses the view that if officers act in accordance with its provisions, they have good reason to be confident that they will not be at risk of personal liability.

12.3 The Guidance applies most particularly if the officer knows or believes torture or CIDT will take place, or if he or she judges there is a serious risk of torture or CIDT. In the first instance (knowledge or belief), the officer must remain uninvolved, and the relevant Ministers need to be informed. In the second instance (there is a serious risk of torture or CIDT), the officer must not be involved unless the risk can be mitigated below the threshold of serious risk. If the risk cannot be mitigated in this way, the relevant Ministers must be informed and provided with all the relevant information. The Ministers will then consider all of the circumstances and decide whether or not to proceed. If the risk is lower than a serious risk of torture or CIDT, the officer can proceed, keeping the situation under review.

12.4 In reality, intelligence and military personnel apply the Guidance cautiously. The Guidance is sometimes invoked when an individual could plausibly be detained on the basis of intelligence passed to another country. By way of example, if an officer asks an intelligence agency of a foreign state for information about a citizen of that state, or wishes to inform the foreign intelligence agency of a possible threat from someone inside that country, then the Consolidated Guidance may be considered irrespective of whether there is a request or a plan to detain that particular individual. Indeed, in some cases inspected by IPCO, it was apparent there was no credible expectation that the individual would be detained, or that the information could support such a move. Indeed, on occasion, the Guidance was applied when the relevant individual was not located in the relevant foreign country at the time of the exchange of intelligence. In other cases, the communication has related to an individual who is being detained abroad in any event or is due to be arrested in accordance with the legislation of that country.

12.5 The intelligence agencies and MOD consider sharing intelligence with a wide range of other countries, irrespective of the closeness of the pre-existing relationship, or even the known human rights record of the other country. Because of the potential wide application of this process, there is a complicated system for recording decisions made under the Consolidated Guidance. However, common sense dictates that the extent of the record depends on the facts of the case. If the other country has an exemplary record for respecting human rights, it will not be necessary to log all the instances of intelligence sharing, and this particularly applies if intelligence is shared regularly with countries that we trust.

12.6 'Assurances' are a key element when decisions are made as to whether to share information with other countries. These are an undertaking by a senior official in a foreign government or intelligence service, either oral or written, as to the restrictions that will be placed on the use of the intelligence and how the individual will be treated. These statements of intent are crucial to the UK's ability to liaise effectively with other countries in this context and they are considered alongside any undertakings the country has made internationally, for example as a signatory of the United Nations Convention Against Torture (UNCAT). The agencies do not rely on assurances in isolation and they form part of a wider judgement as to the level of risk to someone who may be, or has been, detained.

12.7 The three intelligence agencies and MOD apply the Guidance in slightly different ways. Each has developed internal policies to ensure its staff consider the Guidance appropriately and that they maintain a record of decisions. GCHQ usually focuses on the Guidance as part of the approval process when passing intelligence to another country. MOD, by contrast, most often utilises the Guidance when seeking a particular individual's detention. We typically focus our oversight at the MOD on areas where the UK military are working closely with foreign partners. As regards the USA, the close nature of our relationship and the work both countries have undertaken in recent years to safeguard human rights in this context have given the MOD – rightly, in our view – a high level of confidence in the joint assessments about the risk of torture or CIDT.

12.8 SIS and MI5 generally apply the Guidance in similar ways. MI5 work with a range of other countries and have longstanding relationships with many of them. The particularly unpredictable nature of counter-terrorism work, however, means that MI5 and SIS sometimes face the challenge of working with countries that may have a poor or uncertain record of compliance with human rights obligations. This inevitably calls for a more thorough assessment. Similarly, SIS has a broad international focus, and works with a range of other countries. SIS, in particular, will often have a good understanding of the risk in the country in question, which will contribute to the decision as to whether to proceed.

How IPCO oversees these powers

12.9 In November 2014, the Prime Minister directed the Intelligence Services Commissioner to oversee the application by the intelligence agencies and the MOD (including the Armed Forces) of the 'Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees'. In August 2017, the Prime Minister issued a direction that the Investigatory Powers Commissioner should continue this oversight following the abolition of the office of the Intelligence Services Commissioner.

12.10 It is important to have in mind that the Consolidated Guidance applies whenever a member of the armed forces, the staff of the MOD, or a member of the intelligence agencies: i) interviews a detainee who is in the custody of a foreign state; ii) requests

a foreign state to seek information from a detainee in the custody of that country; iii) passes information to a security or intelligence service of a foreign state in relation to a detainee held by that country; iv) receives unsolicited information from a foreign state which relates to a detainee; or v) solicits the detention of an individual by a foreign state.

12.11 Sir John Goldring, accompanied by two inspectors, leads this area of oversight. In early 2017, we inspected the application of the Consolidated Guidance at each agency and the MOD as part of our wider inspection schedule. In December 2017, we conducted a one-day inspection at each agency focusing only on this issue.

12.12 During our inspections, we test whether officers were fully aware of the requirements of the Guidance and the limits of any authorisations under which the intelligence agencies are working. We review the logs completed by officers of their assessments, along with the overarching assessments by senior officers which cover routine sharing of intelligence by staff, and the mechanisms which ensure that these assessments are continually reviewed in case the risk changes.

Findings

Inappropriate application of guidance

12.13 During our December inspections we identified three cases where we were concerned that SIS, MI5, GCHQ or the Foreign and Commonwealth Office had not applied the Guidance appropriately, in situations where there was a serious risk of torture and/or CIDT. We reviewed the casework and internal records (including emails about each case); we interviewed the officers involved; and we held a series of discussions with legal advisors from each agency and the FCO. After this scrutiny, we were satisfied that in each case the Guidance had been properly applied.

12.14 These three cases were the exceptions that prove the rule that in nearly every case there is a clear and adequate written record of the approach that has been taken by the relevant officer. This assessment is based on a review of the paperwork and interviews with individuals involved in a range of cases, including senior officers, caseworkers and legal advisors. The documents considered include the official record kept by the officer, the submissions to Ministers, and a range of other internal documentation including emails, operational logs, and the communications sent to other agencies or bodies. We are satisfied that the intelligence agencies and MOD are applying the Guidance with considerable care. Ministerial oversight by the Foreign and Defence Secretaries is strong and officials at the Foreign and Commonwealth Office closely scrutinise every case and provide them with clear advice on the level of risk.

Records

12.15 The records kept by MI5 and SIS particularly demonstrate a clear consideration by their officers of the principles of the guidance, in a range of difficult circumstances. GCHQ maintains a log of Consolidated Guidance casework, but we have queried whether the record of each case is clearly and sufficiently recorded.

12.16 There is clear room for improving the records relating to the lawfulness of detention and due process by the MOD, and to a lesser extent the other agencies. We will expect this to have improved by the next inspection.

12.17 Each organisation has a bespoke mechanism for assessing, escalating and recording risk, which we accept are appropriate in the context of their work, command structures and internal records. However, Sir Mark Waller suggested that the intelligence agencies should co-ordinate their underlying assessments more closely, and centralise their review and referral processes. In accordance with Sir Mark's recommendations, the intelligence agencies have worked to align assessments in relation to the risk of torture and CIDT to ensure that officers in each organisation are working on the basis of the same approach. This process will encourage officers to gain a more comprehensive understanding of the risks, based on a combination of local knowledge, precedent and any reported concerns. SIS has taken the lead in this area and we have suggested that the MOD should participate.

12.18 It is to be stressed that, in some cases, the agency will have established a number of safeguards and mitigations with the foreign country, which can lead to confidence that the risk is lower than serious even if the state has a poor human rights record. This enables the UK to work abroad, in undoubtedly challenging circumstances, in order to meet vital intelligence requirements. The record must set out the safeguards and mitigations explicitly, together with an assessment of their credibility and an assessment of the risk once they are in place. Frequently, the agency informs the Minister of the steps they plan to take even though the Guidance does not strictly require them to do so. The standard of these records has notably improved in the recent past, in particular for cases that fall below the threshold for a Ministerial submission.

12.19 We have made several recommendations which are intended to encourage the agencies to adopt a more thorough and consistent approach to record keeping than at present. The record should be full and clear, and it should be a freestanding document. In complex cases, a summary of the assessments should be included. Individual liaison services should be given separate consideration. It should be explicit if the Guidance is relevant in more than one way, for example if an agency is requesting historic intelligence relating to a former detainee, and live intelligence relating to a current detainee. The record must explain (i) how historic risk constitutes a relevant consideration; (ii) whether the individual in question is located in a particular country; (iii) whether the individual can be traced on the basis of information that has been shared; and (iv) what, if any, expectations there are for action by the foreign liaison service. The descriptions of the safeguards, whenever they are entered, must reflect substantive knowledge of the relevant circumstances, and the agencies must reflect carefully as to how these details are provided.

12.20 The agency working directly with the foreign country, most commonly SIS, will keep a written record of any assurances that have been given. This makes it easier for any officer acting under the Guidance to make a clear judgement on the risk of mistreatment if intelligence is passed, or if a request is made in relation to a detainee. The agencies understand the importance of establishing confidence in any assurances, written or oral, on a case-by-case basis before conducting any additional activity that engages the Guidance. In 2018, IPCO will focus on whether the confidence placed in these assurances is appropriate.

12.21 We have otherwise made a number of recommendations to each agency which are intended to improve the clarity and consistency of their records.

Breaches

12.22 The Guidance does not define, or require reporting of, a breach of the policy. MI5 and GCHQ have chosen to inform IPCO of perceived failures in applying the Guidance. The cases they highlighted involved inadvertent departures from internal policy rather than a failure to apply the core principles of the Guidance, and these errors did not result in any substantive harm. There does, however, need to be a consistent approach by all four organisations in this area.

Due process

12.23 The Consolidated Guidance indicates some of the factors that personnel should bear in mind when considering the adequacy of the standards of arrest and detention, including whether (i) the arrest was lawful under local law, (ii) the individual has been given the reason for the arrest, and (iii) the opportunities to challenge the lawfulness of the detention. Officers should consider whether the detainee would be denied access to his or her family or to legal representation, and whether he or she was informed as to whether, and when, there will be an appearance before a judge, and whether he or she will receive a fair trial. The lawfulness of the circumstances of detention is to be measured against local and international law. It is of note that the MOD forms fail to refer expressly to the lawfulness of the detention and access to due process, and as a consequence this has been addressed somewhat inconsistently within the agency. However, when questioned, the officers involved in these cases demonstrated an appropriate level of understanding of the legal and judicial systems in the relevant country. In consequence, we do not apprehend there has been a risk of due process, but it remains important that these matters are properly recorded.

Consistency

12.24 SIS has implemented changes to the way in which it deals with assurances when working with foreign countries. It has requested all of its overseas stations to complete and update its risk assessments, and SIS plans to make these available to the other intelligence agencies and to use them to inform assessments of risk at a local level.

12.25 In 2017, MI5 and SIS conducted a trial of a new system that is intended to improve consistency and efficiency. Hitherto, if MI5 planned to pass intelligence to a foreign liaison service via an SIS station, the agencies would complete separate risk assessments. Given SIS has the better knowledge of the other country, under this new approach MI5 pass intelligence to the station, having assessed that it was necessary and proportionate to do so, and SIS then makes the final assessment of the risks involved. We inspected the results of the trial in December 2017 and it has been successful to date. We will continue to review this practice in 2018.

The MOD and Afghanistan

12.26 The MOD has also streamlined its process for briefing the risk of CIDT to Ministers in relation to Afghanistan. The MOD has a high level of knowledge of the relevant circumstances in Afghanistan and this gives justified confidence when judging if there are mitigations on which reliance can properly be placed. The MOD utilises a single submission to the Minister, supplemented by monthly updates, addressing the circumstances in each case.

13. Prisons

13.1 Within this annual report the use of investigatory powers by prisons is considered separately to all other public authorities because of the unique environment within which widely available investigatory powers are utilised (i.e. surveillance & CHIS), and the particular provisions that provide for other powers e.g. interception under the prisons rules.

Description of powers and use

13.2 The prison authorities are entitled to intercept the communications of prisoners, conduct surveillance and use covert human intelligence sources (CHIS). More recent legislation also allows the Prison Service to tackle the use of illicit mobile phones within prisons by interfering with mobile telephone signals or requiring the disconnection of particular telephones from the network.[60]

Interception

13.3 Prisoners communicate with the outside world by telephone calls, letters or (in some establishments) emails. Telephone calls are controlled by a pin-phone system (each prisoner has an individual telephone account which they access with a pin-number) and their letters and emails are scrutinised manually to try to ensure no prohibited material is either sent or received through the postal system.

13.4 In most prisons telephones are only available in booths in communal areas, although an increasing number are providing devices in cells. Prisoners submit telephone numbers to be called which are checked by the prison authorities. Prisoners are asked to nominate any numbers that are to be used for legally privileged calls or other confidential reasons because the confidentiality of prisoners' communications with their legal advisors, Members of Parliament or bodies such as the Samaritans or the Prison and Probation Ombudsman are protected. Prisoners cannot generally receive incoming phone calls.

13.5 In England and Wales, the interception of prisoners' communications (telephone calls and mail) is governed by the Prison Rules 1999 (as amended), which are made under the Prison Act 1952. Any interception that takes place must be necessary and proportionate for one or more of a number of statutory purposes including national security, preventing or detecting crime, public safety, the security and good order or discipline of the prison, the protection of health and morals and the protection of the rights and freedoms of any person. Additional rules govern how the prison authorities record, retain or disclose intercepted material. Similar rules and ministerial directions provide for the interception of communications in Northern Ireland and Scotland.

60 Serious Crime Act 2015 and the Prison Telecom Restriction Orders & Prisons (interference with wireless telegraphy) Act 2012.

13.6 By way of example, prison officers and staff will read a prisoner's mail or intercept his or her telephone calls to gather intelligence and to prevent the prisoner from (i) bringing illicit drugs and other items into the prison, (ii) interfering with witnesses, (iii) grooming or harassing victims, or (iv) committing other criminal offences. The prison may disclose the content of the interception to law enforcement officers.

13.7 In England and Wales, the Prison Service Instructions (PSIs), the National Security Framework and the Public Protection Manual provide detailed guidance on how interception should be carried out.

Surveillance and CHIS

13.8 The Regulation of Investigatory Powers Act 2000 (RIPA) provides the legislative basis for Her Majesty's Prison and Probation Service (HMPPS England & Wales), and the Prison Service for Northern Ireland, to carry out directed surveillance and to use CHIS to prevent and detect crime and to protect public safety. The Scottish Prison Service is similarly authorised under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)

13.9 The prison authorities use surveillance and CHIS powers to combat the supply and internal distribution of illicit goods such as controlled drugs and mobile phones, including in cases where staff corruption is suspected. Security is a critical issue, for instance for those prisoners who pose an escape risk or if intelligence indicates there may be some other material risk. A percentage of telephone calls and letters are randomly monitored.

Statistics

13.10 The decision to authorise the interception of a prisoner's communications is made by a Governor within an individual prison. The authority and its associated documents are stored in the establishment with any intelligence recorded in the prisoner's personal files. IPCO inspections capture the number of live authorities at individual prisons, on the day of inspection, but statistics for interception of prisoners' communications are not collected centrally and reported annually. The numbers of surveillance and CHIS authorisations by the prison service are reported within the non-LEA total figures provided in the earlier chapters.[61]

The Authorisation process

Interception

13.11 The prison authorities have a responsibility to inform inmates that their communications may be intercepted. They do so by issuing a 'communications compact', a document which explains the interception process, the statutory purposes for which a Governor can authorise interception and the availability of confidential calls.

13.12 In England and Wales, Prison Rule 35A gives a prison Governor the authority to intercept any communications by a prisoner or a class of prisoners, if this step is necessary and proportionate. Prison Rule 81 allows Governors to delegate their powers to other officers. In practice, the responsibility to consider and authorise requests to intercept prisoners' communications is delegated to the Head of Offender Management or the Head of Prison Security.

61 Figures 1 and 4

13.13 An Interception Risk Assessment needs to be completed whenever there is a request to intercept a prisoner's communications. This document should explain the threat, the proposed course of action, the assessment of necessity and proportionality, the duration of the proposed monitoring and any other matters taken into consideration by the Authorising Officer.

Surveillance and CHIS

13.14 The process for authorising surveillance and CHIS is essentially the same as for law enforcement agencies. An operational manager, commonly the deputy governor of a prison, acts as the authorising officer.

How IPCO oversees these powers

13.15 During 2017, prior to and following the establishment of IPCO, there were separate inspection regimes for the oversight of the interception of communications, on the one hand, and the use of directed surveillance and CHIS on the other. In future, oversight will be conducted by way of unified inspections covering all the intrusive powers in a single audit.

Interception

13.16 Oversight of the interception of communications in prisons within England, Wales and Northern Ireland (but not Scotland) was previously the responsibility of the Interception of Communications Commissioner (IOCC). The current prison inspections are based on the Prison Rules and PSIs.

13.17 At inspections we aim to ensure that:

- the prison authorities inform prisoners that their communications are liable to be intercepted;
- inmates are aware that confidential communications – always depending on the individual or the organisation in question – will not ordinarily be monitored;
- the correct authorisations and risk assessments are completed;
- interception is conducted lawfully;
- the approach to interception is consistent and ; and
- appropriate measures are in place for the retention, storage and destruction of any material that is gathered.

13.18 In 2017, we carried out 33 inspections of the prison estate, a reduction of between 50% and 60% as compared with previous years. This is primarily because our inspectors have spent more time than anticipated on the work required to set up IPCO.

13.19 Usually one of our inspectors will inspect a prison over a single day. The former IOCCO inspection regime aimed to inspect each of the 128 prisons in England and Wales once every two years. Our inspectors visit the various parts of the prison that are linked to interception, for example the security offices, the accommodation wings, the administration hubs and the offender management units, in order to examine the records and to test whether the relevant staff have the level of knowledge that is necessary to apply the correct procedures and to ensure that the interception is necessary and proportionate.

13.20 Statutory oversight of the use by prisons of powers to prevent or restrict use of communications devices by prisoners and interference with wireless telegraphy was introduced by s.229(3) of the IPA. During 2018 IPCO has been developing oversight of these powers which will be reported on more fully in the next annual report.

Surveillance and CHIS

13.21 During 2017, there were separate inspections of the Prison Services of Scotland, Northern Ireland and England and Wales with regard to their use of surveillance and CHIS powers under RIPA and RIP(S)A.

13.22 Each received a single annual inspection, extending over a number of days, during which there would be a visit to the central body and inspections at a number of prisons.

Findings

Prison interception

13.23 From our 33 inspections in 2017 we made a total of 149 recommendations, an average of 4.5 for each prison. Each of these recommendations were accompanied by a 'traffic light' rating which has historically been used by IOCCO. **22%** of the recommendations were red, **65%** amber and **13%** green. A Governor should take immediate action on red recommendations in order to resolve what will have been a serious area of non compliance. The prison authorities are required to write to the Commissioner, reporting in a timely way on the prison's progress in implementing the each of the recommendations

13.24 Additionally, we give prisons an overall grading which reflects the standard of the approach overall to interception, along with the establishment's progress in implementing previous recommendations. For 2017:

- **51.5%** received a good grade
- **30.5%** were satisfactory
- **18%** were poor.

13.25 In July 2016, HMPPS issued an updated PSI, 'The Interception of Communications in Prisons and Security Measures', which included a number of improvements to the way prisons manage interception. As IOCCO's report for 2016 noted, implementing these changes has not been an easy process, with the result that inspection scores were weaker than hitherto and the inspectors made more recommendations than normal. Despite the enduring difficulties, we are content with the response to last year's recommendations. HMPPS is supporting the relevant Governors to ensure that they complete the outstanding recommendations and improve standards.

13.26 The Interception Risk Assessments, on a notable number of occasions, failed sufficiently to set out the necessity and proportionality considerations to a standard that would enable the Governor to make a lawful decision as to whether to authorise interception. This was observed with particular frequency with regard to prisoners who pose a risk to the public, such as those convicted of violent assaults, harassment or sexual offences. In total 30% of the prisons inspected failed to complete the application documentation to a suitable standard. Our inspectors highlighted instances of deficient paperwork, a general failure to include sufficient detail of the factors relevant to the particular case, an apparent disregard of any Human Rights issues that were engaged and an insufficient record of the matters the Authorising Officer had taken into consideration.

13.27 It is of note that these failings have been reflected in previous IOCCO annual reports.

13.28 In addition, 35% of the prisons inspected failed to carry out suitable reviews of the authorisations. This was particularly the case when there were low numbers of monitors or monitor supervisors.

13.29 It is critical that the prison authorities make a sufficient recording of every intercepted call to meet the requirements of the case, and that they are listened to in a timely way. Additionally, summaries must be forwarded to the appropriate member of staff. Self-evident risks will arise if this does not happen.

13.30 To improve standards of interception and to ensure that risks are managed correctly, the 2016 instruction recommended the creation of a Daily Management log. This electronic document is designed to summarise daily the intelligence gathered on each prisoner who is subject to interception. Although a number of prisons have instituted these electronic logs, the process of implementation remains markedly incomplete. We will look for improvements in this context in 2018.

Surveillance and CHIS

Her Majesty's Prison and Probation Service

13.31 HMPPS, previously entitled the National Offender Management Service, was established on 1 April 2017 and brings together HM Prison Service and the National Probation Service.

13.32 Deploying covert tactics in prisons is an inherently difficult and risky undertaking. Frequently this is necessary step because other tactics are not viable and it is in the public interest to utilise this tactic to prevent and detect crime.

13.33 HMPPS is working on legislative, technological and operational solutions to the undoubted difficulties that accompany the prevalent use of illicit items in the prison estate. Covert tactics are a part of the approach to these problems.

13.34 Lord Judge, the last Chief Surveillance Commissioner, was concerned as to how the National Offender Management Service used and managed the available covert powers, as reflected in his 2016 and 2017 annual reports. Lord Judge and the present IPC have discussed the more acute issues with Mr Michael Spurr, the Chief Executive, and members of his strategic management team. The OSC identified a lead inspector to work with the prison service in order to help improve compliance. This has been a successful innovation which we have continued since the creation of IPCO.

13.35 HMPPS has made considerable efforts to address the recommendations outstanding from last year and has implemented eight of the ten recommendations. As already highlighted, intelligence plays a vital part in ensuring good order and discipline within prisons, and it generally assists in the prevention and detection of crime. There are undoubted attempts to run organised crime enterprises from inside prisons, and terrorists and extremists frequently attempt to influence others. To that end, HMPPS has established an Intelligence Strategy, underpinned by the 'Agency Intelligence Model', which is similar in all respects to that used by law enforcement. There has also been significant investment in training and IT.

13.36 A new regional model has been piloted and is due to be deployed over the next 12 months. Initially, it will manage how prisons use CHIS. In due course, it will be used to manage applications for directed surveillance, which should facilitate improved standards and compliance. Authorisations for the use of CHIS by HMPPS have increased since the introduction of the Yorkshire Regional pilot, which adds weight to the utility of the regional model.

13.37 The number of directed surveillance operations in HMPPS has fallen significantly. This could be for a number of reasons, including the increased use of overt CCTV,[62] tactics such as closed visits, and a lack of resources.

Northern Ireland Prison Service

13.38 Northern Ireland Prison Service (NIPS) comes within the Department of Justice and operates three establishments, one of which manages young offenders and female prisoners. There are approximately 1,400 prisoners, which include separated prisoners who have been sentenced for terrorism offences. The Service has consistently made slight use of the RIPA provisions, resorting to more overt tactics. This year's inspection report highlighted the need for a more comprehensive training programme.

Scottish Prison Service

13.39 An agency of the Scottish Government, the Scottish Prison Service (SPS) operates 15 establishments holding some 7,400 prisoners. This includes women and young offenders. Authorisations under RIP(S)A over the past reporting year have been limited. SPS continues to develop its systems and processes for managing covert activity with a number of options under discussion. Steps have been taken to address previous recommendations such that only one minor matter awaits resolution. SPS benefits from a strong cooperative relationship with Police Scotland; this enables a significant exchange of intelligence and experience, to the benefit of both organisations.

62 see Prison Rule 50A which was added to Prison rules through the statutory instrument 2000/2641 and states:
50A.—(1) Without prejudice to his other powers to supervise the prison, prisoners and other persons in the prison, whether by use of an overt closed circuit television system or otherwise, the governor may make arrangements for any prisoner to be placed under constant observation by means of an overt closed circuit television system while the prisoner is in a cell or other place in the prison if he considers that—
(a)such supervision is necessary for—
(i)the health and safety of the prisoner or any other person;
(ii)the prevention, detection, investigation or prosecution of crime; or
(iii)securing or maintaining prison security or good order and discipline in the prison; and
(b)it is proportionate to what is sought to be achieved.
HMPPS have added significant guidance and training around rule 50.

14. Errors and Breaches

14.1 Errors and breaches – the terms are interchangeable for these purposes – refer to circumstances in which the statutory or other regulatory provisions have been overlooked or contravened.

14.2 Errors can have significant consequences for the rights of individuals who are adversely affected (including vis-a-vis their privacy and family life). It is critical that they are identified, because, amongst other things, this can help identify systemic problems along with individual failings. A key objective for IPCO is to prevent recurrence (e. g. further unjustified intrusion or the continuation of an unjustified operation) and the reporting process provides an opportunity for those affected to seek redress at the Investigatory Powers Tribunal.

14.3 It is essential that members of staff within the relevant authorities report errors as soon as they become apparent. Transparency and openness underpin our ability to deliver oversight in this area. In addition, IPCO investigates an authority's compliance during our inspections, identifying unreported errors and monitoring compliance with any remedial action which was agreed or mandated for past incidents.

Investigatory Powers Act changes

14.4 The IPA defines a 'relevant error' [section 231(9)] as an error:

(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and

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

14.5 The IPC has specific duties to inform affected parties of a serious error[63] when this step is in the public interest. There were similar provisions in relation to errors of a 'serious nature' in the Acquisition and Disclosure of Communications Data Code of Practice 2015 which was in force during the period under consideration. During 2017 the IPC notified 8 individuals of a serious error.

14.6 The Home Office had not published the relevant revised codes of practice by the end of 2017, and this report addresses errors in the context of earlier iterations of the codes. Moreover, as already indicated, for most of the year oversight was conducted by IPCO's predecessor organisations. This report reflects that split in responsibility, not least because we do not have the advantage of a single set of data covering the entire year.

63 see s.231 IPA

Oversight of the powers covered by the Office of Surveillance Commissioners (Non-intelligence agency surveillance and CHIS)

14.7 The OSC was, until the end of August 2017, responsible for oversight of certain covert activities by public authorities (with the exception of the intelligence services) that could carry out the following activities: directed surveillance, intrusive surveillance, property interference, covert human intelligence sources (CHIS) including undercover activity, and encryption (Parts II and III of RIPA, Sections 6 and 7 of RIP(S)A, and Part 3 of the Police Act 1997). The OSC's remit covered the United Kingdom and the Sovereign Base Area of Cyprus (in the latter instance, in accordance with a Regulation of Investigatory Powers Ordinance).

14.8 There was no formal definition of error provided by the OSC, but the Chief Surveillance Commissioner expected to be provided with a report by any public authority when it realised, or suspected, that it had been 'in breach' of the statutory requirements, or had failed to comply with the procedures established by the OSC in order to fulfil its prior approval role. The following section of the OSC's Procedures & Guidance document advised how this was to be managed:

"All covert activity that is not properly authorised should be reported as soon as it is recognised. Activity which should properly be authorised but which isn't should be reported to the Chief Surveillance Commissioner, in writing, as soon as the error is recognised. An initial email alerting the OSC should be followed by a report detailing the circumstances and remedial action submitted by the Chief Officer or Senior Responsible Officer. This does not apply to covert activity which is deliberately not authorised because an Authorising Officer considers that it does not meet the legislative criteria, but allows it to continue. It does include activity which should have been authorised but wasn't or which was conducted outwith the directions provided by an Authorising Officer. All activity which should have been authorised but was not should be recorded and reported to the Inspector(s) at the commencement of an inspection to confirm that any direction provided by the Chief Surveillance Commissioner has been followed."

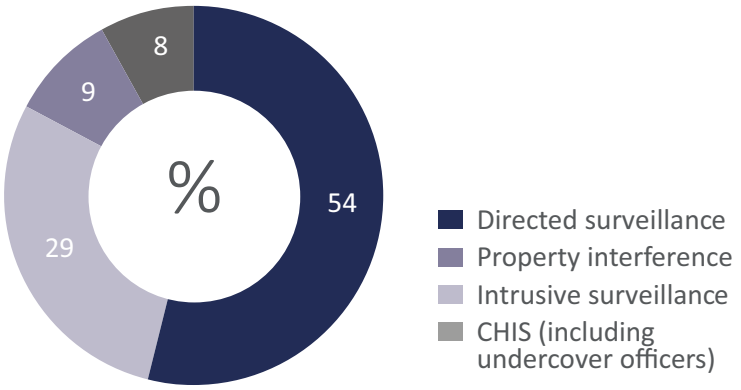
14.9 In the main, public authorities have responsibly reported breaches at an early stage, very often by way of a brief email with the promise of a detailed letter and report to follow. There is sometimes a noticeable gap before those latter documents arrive but the delay is usually the result of the internal investigation into the circumstances and the time needed to formulate proposals for remedial action.

14.10 It has been clear for many years that authorities take errors or breaches seriously, and they are almost invariably met with a robust and thorough response. There is a strong culture of reliable 'self-reporting'.

14.11 83 breaches under this heading were reported to the OSC and IPCO during 2017 in relation to surveillance, property interference and CHIS. This is a slight reduction from 2016-17.

These are broken down as follows:

Fig. 16 Total breaches reported under Part 3 of Police Act 1997 and Part 2 of RIPA or RIP(S)A during 2017



14.12 The breaches, as reflected by these figures, vary in their seriousness. It is of particular note that the number of errors for covert activities remains reassuringly small. As the Chief Surveillance Commissioner has previously observed, some of the incidents are very minor in nature, on occasion scarcely meriting inclusion. That said, it is reassuring that the various organisations adopt a stance of over-reporting rather than under-reporting.

14.13 The following are examples of breaches reported to the OSC and IPCO during 2017:

- An authorisation was granted by a Senior Authorising Officer for the deployment of an audio recording device inside the vehicle of an individual of interest. This required an authorisation for property interference under Part 3 of the Police Act 1997 (installing the device and thereby interfering with the vehicle) and for intrusive surveillance under Part II of RIPA (downloading, recording and listening to conversations recorded by the device). The property interference authorisation was active from the moment of signature, but the authorisation for intrusive surveillance was not effective until approval had been obtained from a Surveillance Commissioner (under the OSC's regime). Due to human error, the technical surveillance team was advised that both activities could be commenced before the Surveillance Commissioner had made a decision. As soon as the error was appreciated, the recording was stopped and an urgent authorisation was obtained to enable the intrusive surveillance to restart. A full internal review was undertaken by the police force to avoid repetition and the results were shared with IPCO.
- A number of Facebook records were accessed by investigators as part of a murder enquiry, in order to investigate the communications between the suspects. The records were accessed over a protracted period of time. Whilst an authorisation for directed surveillance, with one-sided consent, had been obtained in relation to some of the suspects, this was exceeded as the investigation developed to encompass others. Once this was identified, the police force implemented a number of remedial steps. These included additional training, specific advice for the relevant officers, and changes to the practice for making requests of this kind. The breach was reported to the CPS and the material was not used during the subsequent proceedings.

- Breaches are most frequently the result of a simple human mistake. The examples are numerous and include installing equipment or starting the surveillance before the authorisation is in place or continuing the activity or leaving the equipment in situ after the authorisation has been cancelled. The steps taken by the authority in these circumstances generally – indeed, almost invariably – are reassuring: the error is reported and any material obtained as a result of unauthorised activity is handled with appropriate care, including its destruction.

14.14 It will be apparent from the analysis above that many errors are readily avoidable if greater attention is paid to the detail of the relevant circumstances. By way of example, a careful check by the officer on the relevant systems, or other straightforward enquiry, to ensure the authorisation is in place and the undertaking is otherwise lawful, or a timely notification is given to the relevant personnel that the activity is to be terminated and the equipment removed or switched off. Errors are not confined to inexperienced officers or teams. Whilst it is understandable that mistakes as to documentation and processes are made on occasion in the 'heat' of an investigation, it is far more difficult to excuse errors that are repeated, particularly those that reveal a systemic problem.

14.15 The fault is sometimes the result of a failure to include key details in the authorisation documentation, such as a proper description of the subjects, vehicles or locations. This can be particularly acute with longer-running operations involving organised crime groups, when there can be a premium on keeping track of the relevant people, vehicles and places that are the subject of the covert activity. The success of a fast-moving and time-critical operation can depend on this understanding. Many of the incidents reported last year would not have arisen with improved attention to detail by those seeking, authorising and undertaking the relevant activity.

Oversight of the powers covered by the Interception of Communications Commissioner (Interception and acquisition of communications data by all public authorities)

Interception

14.16 In addition to the assistance which we hope is provided by setting out our generalised findings and recommendations (see above), the IPC has a particular duty under s.58(2) and (3) of RIPA 2000 to report any contravention of the provisions of the legislation, or any inadequate discharge of the s.15 safeguards, to the Prime Minister. Error reporting is an important part of IPCO's oversight regime, aiding accountability and enhancing public confidence. It is vital to achieve a consistent approach from all the interception agencies as to the thresholds, approach and reporting criterion that they utilise for errors.

14.17 During 2017, there were 66 interception errors reported to IOCCO and IPCO. Whilst this represents a marked decrease on the number of errors reported in 2016 (108), the figure is more in line with 2015. 59 of the errors related to the authorisation or administration of an interception warrant. 51 were by the interception agencies, one by a warrant granting department and 7 by Communication Service Providers (CSPs) when giving effect to interception warrants.

14.18 The remaining 7 interception errors did not relate to the authorisation or implementation of interception warrants. They were instead either caused by CSPs providing police forces or intelligence agencies with the content of communications when only communications data had been requested under Chapter 2 of Part 1 of RIPA; or as a result of a contravention of section 1(5) of RIPA, for example, when a police force did not have the necessary authority or consent to access stored communications.

14.19 The vast majority of the errors under this heading fell into six distinct categories, as exemplified below:

a. Over-collection

This generally relates to a software or hardware malfunction that results in the over-collection of intercepted material and related communications data. Errors in this category can be markedly varied, including as to the quantities of personal data collected. These errors have the potential to be highly complex and may take a number of months to investigate. The cause is almost invariably identified and satisfactorily resolved. A significant amount of work is usually undertaken to implement measures to prevent any recurrence, and this may include periodic sampling and other regular checks to increase the agency's ability to monitor and detect such errors. We stress that in all cases, steps are taken immediately to ensure that the erroneously collected material and data is deleted.

b. The interception of an incorrect communications address

The majority of these errors were human in nature although a small number were due to a failure of technical systems to update correctly. For example, these may be the result of an error in the transposition of a mobile telephone number, either by a member of staff at the interception agency or the CSP.

c. The unauthorised selection and examination of intercepted material

The most common errors in this category were, first, instances when an analyst mistakenly continued to select the communications of an individual who was thought to be based overseas after he or she had returned to the United Kingdom, and, second, when a technical mishap caused the selection of incorrect material.

d. The incorrect dissemination or misrouting of intercepted material

These errors, which constitute non-compliance with section 15(2) of RIPA, are mainly caused by the misdirection of intercepted material (and any related communications data) to the wrong interception agency. In all the cases examined, the interception was correctly authorised, the mistake was immediately identified by the (wrong) receiving agency and the material and data was deleted.

e. The failure to cancel an interception

These errors were in the main caused by staff within the interception agency, the warrant granting department or the CSP failing promptly or properly to effect the cancellation.

f. The interception of the wrong individual

Whilst these errors bear similarity to those described in category b) above, they represent instances when the interception agency has obtained a warrant and material relating to the wrong person has been intercepted, because (i) of technical reasons, (ii) the telephone was the property of someone not covered by the warrant, or (iii) the telephone was in the possession of someone not covered by the warrant. Generally in this situation, the correct communications address is set out on the warrant but the subject of interest is

using a different device from the one which is of interest. The analysts processing the data routinely detect these errors; they promptly suspend the interception and delete any material that has been gathered. It follows that although the interception of these communications was properly authorised, there was unintended intrusion into the privacy of individuals who were not of intelligence interest. The operational teams within the intercepting agencies must be alert to this risk, and immediately suspend interception whenever this mistake is detected.

14.20 IPCO accepts that it is inevitable that some errors, whether due to human or technical mistakes, will occur. Nonetheless, the interception agencies, warrant granting departments and CSPs are required to report them to IPCO promptly. They should provide an explanation as to what had occurred and demonstrate that the measures put in place to prevent any recurrence are sufficiently robust. They must facilitate any investigation by IPCO and ensure that any erroneously acquired material or data that was not of legitimate intelligence interest has been destroyed.

Acquisition of targeted communications data

14.21 Under the code of practice, an error can only occur after a DP has granted an authorisation and the acquisition of data has been initiated, or a notice has been given and it has been served on a CSP. The likelihood of errors occurring increases if the processes under the code of practice for acquiring or obtaining communications data have not been properly followed.

14.22 Errors that do not result in the return of any data should nonetheless be recorded by the relevant public authority and reviewed by the SRO. Consideration should be given to implementing measures that will prevent recurrence. Errors in this category clearly constitute 'near misses', in that individual rights were not breached.

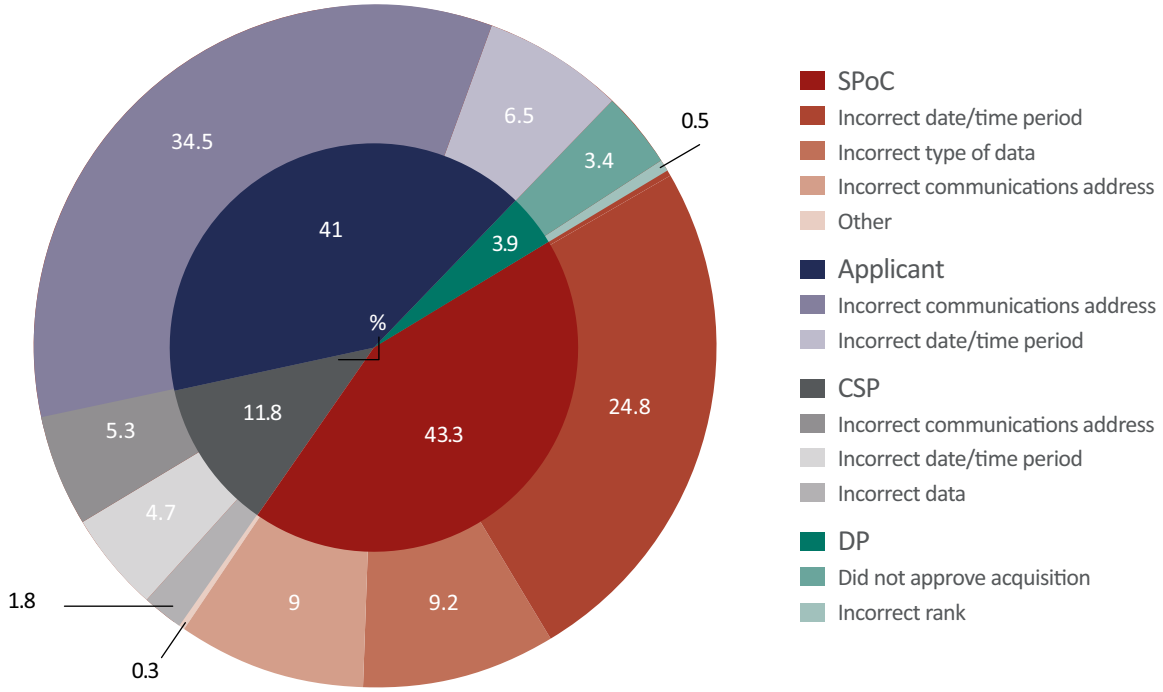
14.23 Errors that result in data being wrongly acquired are of greater concern, given the likelihood that privacy and other rights will have been infringed. These errors are reported to the Commissioner and an account is provided which details how the error occurred and any remedial action that has been taken to prevent recurrence.

14.24 If the Commissioner considers the error to be serious, he will instigate an investigation into the relevant circumstances and assess any adverse impact. The Commissioner may inform relevant individuals of the infringement, and anyone adversely affected may make a complaint the Investigatory Powers Tribunal.

14.25 In 2017, 926 errors were reported to the Commissioner by relevant public authorities, of which 33 were considered to be serious and resulted in further investigation (see Annex B). In 2016, IOCCO reported that it had been notified of 1,200 errors and conducted 29 serious error investigations. Whilst we are unable to say with absolute confidence whether this drop is significant and reflecting changes in the way in which data is being acquired, it is in all probability a positive development. It is interesting to note that the number of IP related errors dropped from 244 in 2016 to 200 in 2017 when the quantity of internet-related data acquired had generally increased (Figure 12 in CD Chapter). This may reflect the attention public authorities have given to the issue of erroneous IP address resolution following considerable focus by IOCCO on the issue in the past 3 years.

14.26 The 926 errors can be conveniently broken down in two ways: by responsible party and cause:

Fig. 17 Breakdown of communications data errors



14.27 As in 2016, the biggest single cause of error remains the submission of an incorrect communications address by the applicant. SPoCs are responsible for 43.6% of errors, largely because of the complexity of their role and errors in typing, given the large quantities of information that are still entered manually. These errors can occur because the applicant has to enter a communications address into an application from a crime or intelligence report, or the SPoC has to take the address from an application, transferring it into a separate CSP disclosure system. The error can be as simple as getting one digit of a telephone number or IP address wrong, which will result in erroneous data being returned.

14.28 The vast majority of the reportable errors considered by IOCCO and IPCO by public authorities and CSPs were 'self-reported' and it is to be noted that there remains a very strong culture of self-reporting by SPoCs and CSPs. However, if information is shared between departments or units within an authority, there is a risk that those with less experience and training will be unaware of the risks that are involved and the steps that must be taken if there is an error. A notable example of this is when mistakes are made with communications data. If the identifying information is not entered exactly, wholly innocent people can be suspected of crimes they did not commit (such as sharing indecent images of children), with dire consequences.

Serious error investigations

14.29 As explained in previous 2016 IOCCO annual report IPCO may classify an error as serious in circumstances which include:

- Technical errors relating to the CSP secure-disclosure systems which result in a significant number of erroneous disclosures;

- Errors when a public authority has, as a consequence of relying on the wrong data, 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).

- Errors which result in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

14.30 In cases where an error may have potentially occurred, an in-depth and detailed investigation is conducted to determine the circumstances and impact. During 2017, IPCO and IOCCO undertook 33 serious-error investigations (this broadly matched the numbers for 2016). 24 cases were classified as serious errors, whilst 9 were not assessed as not meeting the above criteria.

14.31 A description of the 24 cases assessed as serious are set out in Annex B.

14.32 19 of these were a result of human error and there were five system or technical errors, such as a system fault. The cases involving human error included instances in which data was misinterpreted and when data was entered incorrectly.

14.33 The impact of errors can be wide-ranging, including:

- executing a search warrant at an address of someone unconnected with an investigation or when individuals unconnected with the investigation are arrested. There were 11 cases in this category (19 people were affected, in that they were arrested or interviewed);

- the police visiting the home or work address of an individual with no sustainable link with an investigation. There were 7 cases in this category (10 people affected);

- delaying a welfare check on an individual potentially at risk (e.g. a young person at risk of sexual exploitation) because one or more incorrect addresses were investigated (in some cases wrong addresses were visited). There were six cases in this category (six people affected);

14.34 Errors in this context can have grave consequences for the victim of the mistake, together with his or her family and friends. This is particularly evident when homes or offices are searched and the nature of the investigation is revealed to members of the individual's family, and his or her neighbours or employer. Children are at risk of being taken into care and individuals in notifiable, and other, occupations may be suspended or dismissed. Strict bail conditions can result in a suspect having to leave his or her home. The analysis of computers, tablets and telephones can take a protracted period of time. Not infrequently it is only when nothing of suspicion is found on the electronic equipment which has been seized that consideration is given to the possibility that there was an error by the authorities in transcribing the information which links a particular device or an address to the communications data.

14.35 In January 2017 the National Police Chiefs' Council (NPCC) published a series of 'good practice guides'aimed at curbing the number of errors that occur when a public authority seeks to identify the user of a specific Internet Protocol (IP) address. These were based, at least in part, on recommendations from reports by IOCCO and IPCO. Indeed, the complexity of internet protocol address resolution (IPAR) was highlighted in IOCCO's final annual report. In a section devoted entirely to IPAR, the report detailed the many opportunities for error when a public authority seeks to resolve an IP address.

14.36 As a result of these sometimes acute problems, in 2017 our inspectors maintained particular focus upon IPAR.

Interpretation of data

14.37 Acquiring communications data from a variety of different sources and systems has become a frequently complex task. 7 of the 10 investigations related to the misinterpretation of source data containing the target communications address prior to the acquisition-process commencing (for example the applicant specified the wrong time a suspect was using an IP address because they misunderstood what had been reported to them). In three investigations the officer failed to understand the process by which IP addresses are assigned and reassigned, and as a result there was focus on the wrong date and time.

14.38 In two investigations, open-source research linked incorrect profiles to the incidents, and in a further case an interpreter provided the wrong time for a particularly crucial relevant telephone call.

14.39 Six search warrants were executed without justification in a single investigation because data was misinterpreted, leading to the incorrect conclusion that particular individuals had shared illegal files.

14.40 In another investigation, the error was the result of the incorrect way in which the IP address and its associated time and date had been set out in the application.

14.41 In two investigations, accurate requests were made to different CSPs. However, there were flaws in the subsequent manual searches to locate the relevant details, leading to the return of incorrect information.

Lack of corroboration

14.42 Whenever possible, those conducting an investigation in this context should seek to corroborate the IP activity which appears to reveal an offence. When a person is suspected of sharing illegal material, the systems public authorities use to identify this offence will usually capture the person's internet activity over a number of days. Analysing a 'spread' of an individual's online behaviour (often involving different IP addresses) will help confirm whether the correct account has been identified.

14.43 We are pleased that there has been a notable increase in the number of IPARs that are being submitted to provide corroboration for individual investigations.

14.44 In two investigations, in each of which a single customer account was being sought, the investigating officers were undeterred when two different customer accounts were returned. This should have halted both investigations because it was highly likely there had been human error when entering the information (unless there was a connection between the two accounts, which was not the position in either case). As a result, action was taken against households the members of which had no involvement in criminality.

14.45 Members of the same household will frequently share passwords for 'routers' and this poses a problem when investigators are seeking to identifying the device that is being used by a suspect.

14.46 One of the most challenging issues facing a public authority is when an application results in inaccurate data being returned by a service provider. In three investigations in which this occurred, if the authority had looked for corroborating material it is likely that ill-founded searches and arrests would not have taken place.

14.47 The same principle applies to flawed applications that are based on a transposition error: corroboration reduces the risk that mistakes will be made.

14.48 It follows that IPCO strongly recommends that corroboration is sought whenever possible.

Transposition

14.49 Transposition errors are reduced whenever public authorities adopt the Guide to Good Practice. This will happen, for instance, if an investigator types the wrong IP address when copying the information from one system or document to another. The Guide's requirement that the source of the IP address is attached for all IPAR requests has been of considerable assistance in reducing errors.

14.50 Urgent cases pose a particular problem because the relevant documents are not always available.

14.51 In one investigation the time and dates of two relevant IPs were confused.

14.52 In a further Investigation, a vital full stop was omitted when typing the username.

14.53 It follows that IPCO strongly recommends that every reasonable step is taken to ensure accuracy when transposing information. In his half yearly report in 2015, the then Interception of Communications Commissioner, Sir Anthony May, provided recommendations to reduce the incidence of errors, and these remain a useful guide to public authorities and CSPs:[64]

- Ensure that applicants, SPoCs, SROs and the CSP staff dealing with disclosure requests are fully aware of the potentially serious implications of human errors.
- Enhance the capability of applicants to improve their ability to transfer electronically (e.g. copy and paste) the communications addresses and relevant dates / times / time-zones into their applications when the original source information is electronically held.
- Greater adherence should be paid to paragraph 3.68 of the code – the telephone numbers (or other identifiers) should be read twice and then repeated back during an urgent oral process.
- When there is more than one IP address relating to an incident, or more than one date or time, the public authority should consider resolving more than a single instance to provide a comparison between the results.
- Enhance the ability of SPoCs to check the source information on which the applicant based their application, to enable the SPoC to check that the applicant correctly interpreted the source information (for example he or she converted the time zones correctly).

64 https://www.ipco.org.uk/docs/iocco/2015%20Half-yearly%20report%20(web%20version).pdf

- Enhance the ability of SPoCs to transfer electronically (e.g. copy and paste) the communications address and relevant dates / times / time-zones from the application into the CSP secure disclosure systems, a section 22(3) authorisation or a section 22(4) notice.
- Enhance the ability for CSPs to transfer electronically (e.g. copy and paste) the communications address and relevant dates / times / time-zones between their systems whenever possible.
- A requirement for the public authority receiving the information from the CSP (and any additional public authority to whom that intelligence is disseminated) to check and double check the material disclosed against the relevant requirements prior to taking action.
- Public authorities, whenever possible, should conduct research and carry out intelligence checks to seek corroboration prior to executing warrants.
- Provide instruction to applicants and investigating officers to revert straightaway to their SPoC, or to the agency who provided the information, in cases where they have cause to doubt the disclosure
- Ensure that the CSP secure disclosure systems are tested sufficiently prior to implementation and after any significant updates or upgrades.
- Ensure there is standardisation and consistency, to the extent achievable, in relation to the data-entry requirements on the different CSP secure disclosure systems.
- A requirement for the SPoC to inform the CSP immediately if an error is identified which might be the result of a technical system fault (even where the error has been classified as a recordable error).
- Ensure that there are regular quality-assurance audits of the CSP secure disclosure systems in order to identify faults.
- Ensure i) that the CSPs and system vendors are aware of the potential significant consequences of system errors; ii) that the public authorities are informed of any systems errors immediately; and iii) the causes of the errors in this category are corrected at the earliest opportunity.

Inaccurate data inputs

14.54 The CSP, as the owner, provides the relevant communications data once an application is approved. This data will often include subscriber and account information, service-use data and traffic data (the 'who, when and where' material). The data is then stored for direct retrieval by an accredited Single Point of Contact Officer (SPOC).

14.55 In one case an investigator sent out an urgent request and acted on the results, ignoring the 'flag' that indicated a fault required that the results should be manually checked (See Annex B – serious error investigation 16).

14.56 In another case, a public authority was provided with data for a property with no connection to the suspected illegal activity. A search of the premises took place (Annex B, serious error investigation 17). A subsequent investigation identified that wires in a street cabinet had been inadvertently crossed. This is now subject of an application before the Investigatory Powers Tribunal.

14.57 By way of a final example, the wrong house number was entered on the documentation for the suspect's home address.

System faults

14.58 Errors within the disclosure system of a CSP can self-evidently have a significant adverse impact on investigations.

14.59 On inspection, we observed a wide range of problems caused by faults in the relevant systems, including corrupted billing information and installation addresses; reliance on incorrect time zones; and changes to the format of time zones occurring without notification. Events of this kind can lead to serious adverse consequences.

The need to notify errors in accordance with the code of practice para 6.19 (3)

14.60 On occasion, errors are reported for the first time months, or even years, after they occurred.

14.61 Under the current code of practice for the Acquisition and Disclosure of Communications Data, when a reportable error occurs, the relevant public authority must establish the facts and report them to IPCO within no more than five working days.[65]

14.62 The cases involving late reporting shared the common feature that the data acquisition was undertaken by one public authority but the relevant executive action was taken by another authority. A lack of any feedback to the SPoC office which initially acquired the data could result in other 'packages' of data being acted on as a result of incorrect communications data. The public authorities involved in the cases we investigated have addressed this issue by making their legal departments aware of paragraph 6.19 of the Code. IPCO is currently ensuring that all other relevant public authorities are made aware of this obligation.

14.63 Whenever a serious error occurs, the IPCO investigation provides the IPC with sufficient information to make a determination as to whether to inform the affected individual of their right to make a complaint to the Investigatory Powers Tribunal (IPT).

14.64 Since 2013, 135 IPCO or IOCCO investigations have resulted in 23 substantive recommendations.

Bulk communications data

14.65 There is no statutory requirement under section 94 of the Telecommunications Act 1984 to report an error when acquiring or accessing bulk communications data. No errors have been reported in the relevant period as regards the acquisition of bulk communications data by means of a section 94 direction.

14.66 MI5 has, however, developed and implemented an internal policy process to report instances when data that is retained as a consequence of a section 94 direction is subsequently accessed in error. In 2017 MI5 reported 17 errors in this context.

14.67 A breakdown of the causes of the errors is as follows:

- **5** were caused by the investigator or analyst acquiring data on an incorrect communications address or identifier;

65 'When a reportable error has been made, the public authority which made the error, or established the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the IOCCO within no more than five working days or the error being discovered. All errors should be reported as they arise...' Para 6.19 Acquisition and Disclosure of Communications Data Code Of Practice (2015)

- **2** were the result of the applicant acquiring communications data for an incorrect date or time period;
- **3** were 'non-MI5 errors'
- **6** were caused by excess data being acquired which fell outside the scope of the authorisation; and
- **1** was caused by undertaking conduct which was not compliant with MI5's handling arrangements.

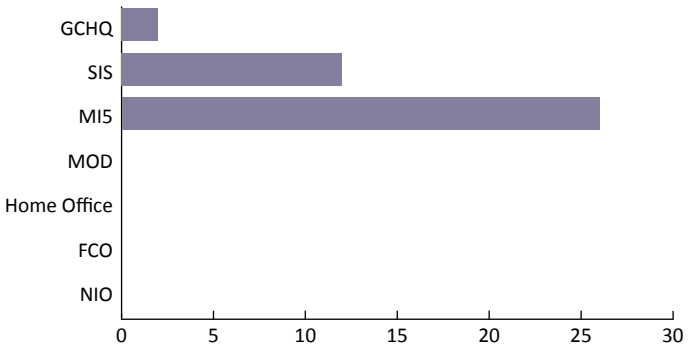
14.68 As previously stated, GCHQ, in the main, merges the bulk communications data with other datasets containing communications data.[66] GCHQ have a mechanism for reporting errors to the IPC, but they cannot easily differentiate the source from which the data is derived without compounding any potential intrusion (for example, by rerunning the erroneous query). No errors have been reported to the IPC that relate to data obtained under a s.94 direction.

Oversight of the powers covered by the Intelligence Services Commissioner

Summary of errors in relation to powers formerly overseen by the Intelligence Services Commissioner

14.69 There were 40 errors reported in relation to powers formerly overseen by the Intelligence Services Commissioner during 2017. There were 38 errors in the previous year. Although the total number of errors is slightly up on the previous year, the error rate across the intelligence agencies remains low in relation to the total number of authorisations and renewals obtained during the year. The majority were the result of human error and there is no evidence of deliberate or systematic attempts to circumvent safeguards. We are satisfied that the intelligence agencies have taken or are taking appropriate action to mitigate recurrence of these errors. It should be noted that MI5 obtain a considerably larger number of warrants and authorisations than the other intelligence agencies and that their error rate is low as a proportion of authorisations.

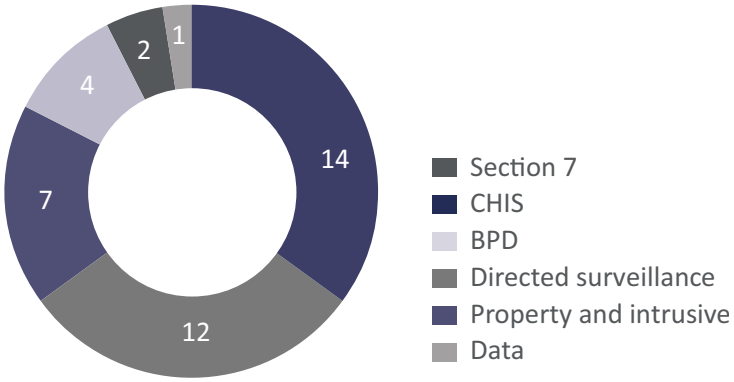
Fig.18 This graph shows the number of errors reported by agency and warrant issuing department.



66 See section 20 of the Regulation of Investigatory Powers Act 2000 for definition of 'related communications data' http://www.legislation.gov.uk/ukpga/2000/23/section/20

14.70 The graph below shows a breakdown of errors by investigatory power.

Fig.19 Number of errors reported by agency and warrant issuing department



14.71 The largest number of errors reported was in relation to CHIS activity; 10 of these related to SIS. 12 errors related to Directed Surveillance, of which 11 were reported by the MI5. All 7 errors in relation to property interference and or intrusive surveillance were reported by MI5. Both GCHQ errors were in relation to activities authorised under Section 7 of the Intelligence Services Act. 3 of the 4 BPD errors were reported by MI5 and the other by SIS.

Data errors

14.72 There was one complex error reported by MI5 in relation to the retention of data on an area within their IT systems. MI5 is undertaking work to remedy this problem and delete data which has been retained erroneously.

CHIS and undercover activity

14.73 All the errors in this area resulted in unauthorised interference with privacy. The majority of the errors related to unauthorised activity in the UK by SIS agents. This typically occurred where an agent normally operating overseas was met and tasked, or conducted online activity, whilst in the UK. This was routinely the result of human error and SIS has put a number of measures in place to ensure that officers are aware to a greater extent than hitherto of the requirements under RIPA. All four MI5 CHIS errors related to a failure to renew authorisations before they expired (largely the result of misinterpreting renewal dates).

Directed surveillance

14.74 In one operation, SIS failed to obtain a DSA to cover the audio recording device element of an operation resulting in unauthorised intrusion. The majority of MI5 errors in this area related to a failure to renew authorisations before they expired resulting in periods of unauthorised intrusion into privacy. One error was a failure to obtain the correct level of authorisations in relation to LPP material. Each of these cases was the result of human error, addressed by speaking to the officers and teams involved and, in some cases, through issuing new guidance and introducing new procedures. In one case MI5 equipment was deployed in a way that resulted in the over collection of data and therefore constituted an unauthorised interference with privacy. In this instance the MI5 updated their operational procedures to ensure future deployments of this equipment were fully compliant.

Property interference and intrusive surveillance

14.75 All 7 errors relating to property Interference and Intrusive surveillance were reported by MI5. Of these, five were the result of human error whilst two were the result of technical failures. In one case property was interfered with where the individual had the same surname as the intended target of the operation. In another case a small number of operational deployments were not subject to scrutiny by senior managers as laid out in MI5 internal guidance and agreed with the Home Secretary. There is no concern that the operation was improperly planned or carried out. To prevent recurrence MI5 has conducted training workshops and issued further guidance to staff. In addition they plan to build additional validation checks into the relevant IT systems to prevent further failures of this kind. In other cases staff have been reminded of the correct processes to follow and, in one case, the wider investigative community has been made aware of a technical issue that could result in the targeting of incorrect IP addresses. Overall we are satisfied that appropriate action has been taken or is underway to mitigate the likelihood of similar errors occurring in the future.

Bulk personal datasets

14.76 Breaches are a significant concern in any area of agency work but they are particularly notable in this area because they point to potential failures in training and the understanding of officers who have access to sensitive data. We received briefings from each agency on their protective monitoring and audit processes. The methodology of this monitoring is highly classified within each organisation.

14.77 Early this year, SIS reported a higher than usual number of breaches relating to access to BPDs. These had fallen by the time of the December inspection.

14.78 An SIS officer must conduct searches on internal systems in order to view existing records before interrogating any BPD, in order to prevent unnecessary intrusion. Broadly, although the breaches reported related to a legitimate business use of the data, officers had not conducted appropriate checks on less intrusive systems before conducting searches against a BPD. We probed this issue at the December inspection, to understand the steps taken by SIS to improve compliance in this area. This had involved a 'refresh' of the protective monitoring process, to gain a clearer snapshot of potential breaches, and an office-wide compliance training programme was undertaken, to ensure that all staff were aware of the appropriate standards. We were content from the statistics that this programme was proving successful but we will continue to monitor this throughout 2018.

14.79 GCHQ and MI5 reported a low level of breaches, which strongly indicates that there is no deliberate or systemic abuse of data.

Consolidated guidance

14.80 The Consolidated Guidance does not make any provision for what is to occur in the event of non-compliance. It does not address how breaches are to be identified and reported. It is necessary, therefore, for IPCO to explain the approach that we will take as part of our oversight responsibilities. Most critically, non-compliance will include any substantive failure to apply the Guidance appropriately, including: (i) continuing to pass or receive intelligence relating to a detainee when the assessment of the risk of mistreatment, including the utility of any mitigation, has changed to the extent that a review is necessary; (ii) failing to take appropriate action when in possession of information relating to a serious risk of torture or CIDT; (iii) failing to inform a Minister when it is known or believed, or there is an unmitigated serious risk, that torture or CIDT is taking place; and (iv) failing

to consider whether the detainee or individual may have been or may be subjected to unacceptable standards of detention or treatment before interviewing or seeking intelligence from detainees in the custody of a liaison service, or before soliciting an individual's detention by a liaison service.

14.81 We identified occasional instances when intelligence was shared without full adherence to the Guidance, albeit this never involved a serious risk of torture or CIDT. Whenever there is a material failure to follow the Guidance, the agency should fully investigate whether intelligence was shared or requested without either a proper assessment of the risks or a failure to secure effective mitigation. In the event that an intelligence exchange has taken place in these circumstances, it will usually be appropriate for the agency to follow up the matter with the foreign liaison service, unless there is reason to suspect that this would make the situation worse for the detainee. The internal investigation into the cause of the breach should reveal whether additional training or other safeguards are necessary. We have recommended that the agencies adopt a consistent policy on breaches, which should include an obligation to report any breach to IPCO. We have also recommended to the Cabinet Office that this requirement should be reflected in the Guidance.

14.82 The Agencies' current lack of a policy for breaches has meant that oversight in this area has been incomplete. Nonetheless, Ml5 identified three minor breaches during the December inspection, none of which involved a serious risk of torture or CIDT. In each instance, the breach was appropriately addressed.

14.83 At GCHQ, we identified eight cases in which intelligence had been passed without complete adherence to the Guidance. Each case was minor and in none was there reason to believe harm had resulted. For example, in one case intelligence was passed to an ECHR signatory without consulting the central team. This is contrary to GCHQ policy but there was no risk of harm.

15. Engagement with the Investigatory Powers Tribunal and other bodies

15.1 IPCO and the Investigatory Powers Tribunal (IPT) are the two principal oversight bodies for investigatory powers, discharging different, but complementary, functions. When requested, IPCO works closely with the IPT, in an effort to ensure that the exercise and performance of investigatory powers are at an appropriate standard and that individuals adversely affected by the inappropriate or incorrect use of these powers are in a position to obtain redress.

15.2 When an error in the acquisition and use of communications data is of a serious nature or when individuals have been affected by a wilful or reckless failure during the acquisition of communications data by a public authority, the IPC has the opportunity to inform those affected that they are entitled to make an application to the IPT. When inspectors from IPCO suspect an error or serious failure has occurred, they will undertake a detailed review of the available material and prepare a report for the IPC. For this purpose, the relevant authority is required to provide all such assistance and information as necessary.

15.3 If the IPC determines that an individual ought to be informed in this way, sufficient information should be disclosed to enable him or her to engage effectively with the IPT. There were notifications of this kind in eight cases in 2017. It is to be observed that in the majority of instances when the IPC notified an affected person, the public authority had already provided information as to the role of the IPT. It is also of note that not all those notified make an application to the IPT.

15.4 The IPC is obliged to provide the Tribunal with all such assistance as the IPT requires, including disclosing records and giving an opinion on any matters before the IPT. Assistance of this kind was provided on a number of occasions during 2017, and in particular in case IPT/15/110/CH, which related to the acquisition and use by the intelligence agencies of bulk communications data (pursuant to section 94 directions) and of bulk personal data. The issue in the case related to the lawfulness of the acquisition regimes. The acquisition of bulk personal data was first publicly avowed in March 2015, and of bulk communications data in November 2015. The majority of the relevant material related to the period before the creation of IPCO and a significant amount of work was required to identify and disclose any relevant material from the archives of our predecessor organisations. In addition, we responded to numerous requests for clarification or additional information.

15.5 Within the same litigation, the IPT requested IPCO's assistance in verifying the results of numerous searches the claimants had requested the agencies undertake as part of the discovery process, in order to determine the extent of particular types of data that had been acquired (e.g. communication addresses and travel information). This work took a number of inspectors several days to complete and resulted in a detailed report.

15.6 When consistent with our statutory responsibilities and any limitation on the disclosure of information, and when IPCO's resources reasonably permit, we have assisted other third parties and statutory bodies. This work has included assisting Her Majesty's Inspectorate of Constabulary and the Independent Office for Police Conduct on matters within their jurisdiction.

16. IPCO and predecessors' budgets

As this is a year of transition from three bodies to one new body (IPCO) we have 4 financial statements to report.

Intelligence Services Commissioner (IScom) (Period 01/04/17 – 30/09/17)

Staff costs	£126,491.49
Travel and subs	£7,106.96
Legal	£5,310.00
IT	£1,917.60
Office – cost	£–
Total	**£140,826.05**

Interception of Communications Commissioner's Office (IOCCO) (Period 01/04/17 – 30/09/17)

Staff cost	£485,129.86
Travel and subs	£78,364.33
IT	£4,252.65
Training	£–
Office	£5,184.40
Conference	£6,766.22
Other	£835.52
Total	**£580,532.98**

Office for Surveillance Commissioners (OSC) (Period 01/04/17 – 30/09/17)

Staff costs, including recruitment and training	£548,301.40
Travel and subs	£71,261.32
Conference and teetings	£6,956.73
IT and telecoms	£7,099.93
Stationery, including printing, postage and publications	£1,081.47
Office and security equipment	£905.52
Accommodation	£–
Other	£1,427.00
Total	**£637,033.37**

IPCO (Period 01/10/17 – 31/03/18)

Staff costs	£1,854,907.07
Travel and subs	£121,096.99
IT and telecoms	£67,688.95
Training and recruitment	£1,838.40
Accommodation (building)	£670,701.67
Conferences and meetings	£16,450.30
Office supplies (stationery, printing)	£14,644.49
Legal	£3,883.20
Other	£332.20
Total	**£2,751,543.27**

17. Annex A: Communications Data acquisition by public authority

Table containing number of items of data acquired by each of the 600 public authorities we oversee, broken into 4 sections for the public authority types.

Type	Public Authority	The number of items of communications data sought, for each notice given, or authorisation granted. Including orally.
Law Enforcement	Avon and Somerset Constabulary	16,288
Law Enforcement	British Transport Police	2,733
Law Enforcement	Bedfordshire	4,938
Law Enforcement	Cambridgeshire	3,900
Law Enforcement	Cheshire Constabulary	11,151
Law Enforcement	City of London Police	3,630
Law Enforcement	Cleveland Police	6,861
Law Enforcement	Cumbria Constabulary	4,262
Law Enforcement	Derbyshire Constabulary	5,515
Law Enforcement	Devon and Cornwall Police	18,706
Law Enforcement	Dorset Police	3,817
Law Enforcement	Durham Constabulary	7,045
Law Enforcement	Dyfed Powys Police	3,301
Law Enforcement	Gloucestershire Constabulary	3,101
Law Enforcement	Greater Manchester Police	37,657
Law Enforcement	Gwent Police	5,543
Law Enforcement	Hampshire Constabulary	12,150
Law Enforcement	Hertfordshire Constabulary	12,338
Law Enforcement	HMRC	19,277
Law Enforcement	Humberside Police	5,950
Law Enforcement	Kent & Essex SCD	22,618
Law Enforcement	Lancashire Constabulary	18,075
Law Enforcement	Leicestershire Police	10,156
Law Enforcement	Lincolnshire Police	5,138
Law Enforcement	Ministry of Defence Police	202

Type	Public Authority	The number of items of communications data sought, for each notice given, or authorisation granted. Including orally.
Law Enforcement	Merseyside Police	23,477
	Metropolitan Police	112,002
	Norfolk Constabulary & Suffolk Constabulary	6,206
	North Wales Police	7,006
	North Yorkshire Police	6,047
	Northamptonshire Police	8,568
	Northumbria Police	7,479
	Nottinghamshire Police	12,502
	Police Scotland	39,381
	Police Service of Northern Ireland	7,686
	Royal Air Force Police	34
	Royal Military Police	694
	Royal Navy Police	27
	National Crime Agency	50,785
	South Wales Police	13,553
	South Yorkshire Police	11,807
	Staffordshire Police	8,565
	Surrey Police	7,823
	Sussex Police	6,117
	Thames Valley Police	13,508
	The Home Office (Immigration Enforcement)	7,770
	Warwickshire Police and West Mercia Police	18,657
	West Midlands Police	53,548
	West Yorkshire Police	27,529
	Wiltshire Police	6,498
Intelligence Agency	GCHQ	9,807
	MI5 (Security Service)	38,995
	Secret Intelligence Service (MI6)	474

Type	Public Authority	The number of items of communications data sought, for each notice given, or authorisation granted. Including orally.
Other Public Authority	Competition and Markets Authority	8
	Department of Enterprise, Trade and Investment (Based in NI) – Northern Ireland Trading Standards Service	87
	Department of Health – MHRA	194
	Financial Conduct Authority	2,710
	Gambling Commission	2
	Gangmasters Licensing Authority	41
	Health & Safety Executive	7
	HMPS NOMS	1,405
	Information Commissioner's Office	187
	IPCC	112
	Maritime & Coastguard Agency	11
	NHS Protect	2
	Ofcom	4
	Serious Fraud Office	1,523

The following 'Other Public Authorities' reported that they had not used their powers to acquire communications data in 2017:

Criminal Cases Review Commission
Department for Transport – Air Accident Investigation Branch
Department for Transport - Marine Accident Investigation Branch
Department for Transport – Rail Accident Investigation Branch
Department of Work & Pensions – Child Maintenance Group (CMG)
Marine Management Organisation
NHS Scotland
NI Health & Social Services Agency (was Central Services Agency)
Northern Ireland Office (NIPS)
Police Investigations Review Commissioner
Police Ombudsman for Northern Ireland
Prudential Regulation Authority
Scottish Criminal Cases Review Commission

Also, no Fire and Rescue Service or Ambulance Service reported using their powers to acquire communications data in 2017.

Type	Public Authority	The number of items of communications data sought, for each notice given, or authorisation granted. Including orally.
Local Authority	Bath and North East Somerset Council	11
	Bedford Borough Council	2
	Birmingham City Council	15
	Brentwood Borough Council	2
	Bristol City Council	47
	Bury Metropolitan Borough Council	5
	Caerphilly County Borough Council	29
	Cheshire West and Chester Council	19
	City And County Of Swansea	3
	City of London Corporation	6
	City of Westminster Council	4
	Cornwall Council	3
	Derby City Council	17
	Dover District Council	14
	Dudley Metropolitan Council	3
	Durham County Council	7
	East Sussex County Council	3
	Epsom and Ewell Borough Council	1
	Essex County Council	36
	Gateshead Metropolitan Borough Council	19
	Gloucestershire County Council	4
	Hampshire County Council	6
	Hartlepool Borough Council	5
	Hertfordshire County Council	14
	Kent County Council	52
	Lancashire County Council	23
	Leicester City Council	9
	Leicestershire County Council	4
	Lincolnshire County Council	17
	London Borough of Brent Council	18
	London Borough of Bromley Council	8
	London Borough of Croydon Council	46
	London Borough of Enfield Council	6

Type	Public Authority	The number of items of communications data sought, for each notice given, or authorisation granted. Including orally.
Local Authority	London Borough of Hammersmith Council	79
	London Borough of Harrow Council	2
	London Borough of Merton Council	1
	London Borough of Wandsworth	3
	Manchester City Council	2
	Milton Keynes Borough Council	3
	Mole Valley District Council	4
	Newport City Council	1
	Norfolk County Council	11
	North Norfolk District Council	4
	North Yorkshire County Council	22
	Nottinghamshire County Council	10
	Oldham Metropolitan Borough Council	1
	Redcar and Cleveland Borough Council	43
	Rhondda Cynon Taff County Borough Council	6
	Royal Borough of Kingston Upon Thames Council	3
	Sandwell Metropolitan Borough Council	1
	Sheffield City Council	8
	South Oxfordshire District Council	3
	St. Helens Metropolitan Borough Council	4
	Stockport Metropolitan Borough Council	1
	Stockton On Tees Borough Council	2
	Stoke on Trent City Council	8
	Surrey County Council	5
	Telford & Wrekin Council	2
	Tewkesbury Borough Council	5
	Thurrock Borough Council	6
	Torbay Borough Council	2
	Warrington Borough Council	5
	Warwickshire County Council	4
	West Berkshire Council	25
	West Sussex County Council	11
	Wolverhampton City Council	1
	York City Council	41

18. Annex B : Serious Error Investigations

Error Investigation 1

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Incoming call data
Description	A public authority had reported to them the site where a body had been deposited. This information was passed into the public authority by a third person unconnected to the incident. From the information gleaned through a translator the public authority sought to trace the original informant. The incoming call data covering the time period advised by the translator captured just one number that led to the arrest of its subscriber on suspicion of murder. A later review established the call to have been mistranslated.
Consequence	Innocent person arrested and interviewed.

Error Investigation 2

Responsible Party	Public Authority
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber information relating to an IP address
Description	A public authority was investigating the uploading of indecent images of children (IIOC). The officer identified 3 relevant IP addresses used by the offender during their upload and sought their resolution into customer details. After authorisation the time zone for each was incorrectly entered into the portal of the Internet Service Provider (ISP). As a consequence the results were out by one hour risking the wrong account(s) being attributed to the offence. In two the same customer details was found, with the third returning details of another customer. No connection between the two customers could be found. Action was taken at both addresses.
Consequence	Police visited the premise of an individual unconnected to their investigation. Computer equipment seized.

Error Investigation 3

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Social Profile – IP log on and access history
Description	A public authority was trying to locate a vulnerable missing person. Open source research was used to identify whether the missing person had a social media presence. This research found what they thought to be their profile. The profile found had the same name, description and lived in the same area. The public authority undertook a welfare visit only to find the person had the same name but no connection to the missing person.
Consequence	Police visited the premise of an individual unconnected to their search. Delayed welfare check. Missing person was found safe and well.

Error Investigation 4

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Subscriber information relating to an IP address
Description	Investigation into the uploading of indecent images of children (IIOC) identified offending IP address, time and date. From the original data the applicant strung the IP address time and date into one continuous set of figures 12.123.345.1519/04/2011@09:09:09. Instead of the application being 12.123.345.15 on 19/04/2011@09:09:09 the application read 12.123.345.151 on 09/04/2011@09:09:09. (NB – fictitious addresses used) The result was passed to another force for action. These events took place in 2011 and not reported as an error to IOCCO in accordance with the code of practice.
Consequence	Innocent person arrested and interviewed.

Error Investigation 5

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Subscriber information relating to an IP address
Description	A report was sent to a public authority detailing concern for the welfare and safety of a young child. The report provided sufficient information for the public authority to try and establish a postal address for when this concern was first raised. The application made an incorrect assumption when it linked the IP address used to first register the account to the time and date of the concern. A gap of 8 months. The result brought back a customer living in the same county as the information suggested.
Consequence	Police visited the premise of a household unconnected to their investigation. Application corrected and actual address established.

Error Investigation 6

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Subscriber information relating to 2 IP address
Description	A report was sent to a public authority concerning the sexual exploitation of two children. The report provided sufficient information for the public authority to try and establish a customer name and postal address based on the IPs used to make this inappropriate contact. Two IP address resolutions were submitted. In one the applicant incorrectly linked the IP address used to first register an account to the time and date of its last known activity. A gap of 5 months. In the other an accurate application had been made. The CSP provided details of two different customers, with the details for one clearly pointing suspicion upon them. No link could be found between the two customers save living in the same area. Despite this, police visited both addresses simultaneously and arrested a male at the home where suspicion was strongest. This male who later confessed. At the second house no arrests were made.
Consequence	Search warrant executed at the home of an innocent family. Devices seized for examination.

Error Investigation 7

Responsible Party	Public Authority
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber information relating to an IP address
Description	A public authority was trying to locate a vulnerable missing person. Details of an online username were correctly obtained. During an urgent verbal request an extra letter became added to the username. As a consequence details of an innocent person were obtained albeit with the same last name as the missing person. A public authority then undertook a welfare visit only to find the person had no connection to the missing person.
Consequence	Police visited the premise of an individual unconnected to their search. Delayed welfare check. Missing person was found safe and well.

Error Investigation 8

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Incoming call data
Description	A public authority had reported to them the site where a body had been deposited. This information was passed into the public authority by a third person unconnected to the incident. From the information gleaned through a translator the public authority sought to trace the original informant. The incoming call data covering the time period advised by the translator captured just one number that led to the arrest of its subscriber on suspicion of murder. A later review established the call to have been mistranslated.
Consequence	Innocent person arrested and interviewed.

Error Investigation 9

Responsible Party	Public Authority
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber information relating to an IP address
Description	A public authority was trying to locate a young person in crisis. With the child having made contact with a charity via the internet an IP address time and date was identified. To ensure the assigned customer for the time in question was captured the SPoC sought data to include the 90 minute period before the contact with the charity had been made (as advised by the CSP concerned to ensure the relevant IP address was captured). This brought back the account number for the correct customer and that of its previous user. When seeking to change the account number into the customers name and address the account number for the previous user of this IP was used instead. Police made contact with account holder using the IP previous to the young child. It was later confirmed that the mother of the actual child in question had reported the matter via another channel.
Consequence	Police visited the premise of an individual unconnected to their search.

Error Investigation 10

Responsible Party	Public Authority
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber information relating to an IP address
Description	A public authority was investigating the grooming of a young female via social media. The suspect's own profile led officers to believe he was using other peoples broadband to log on and interact with the female. When seeking to resolve the accounts using two pertinent IP addresses the applicant inadvertently swopped the times and dates of each over. When the results were returned, the customers at two different postal addresses were visited. With neither having any connection to the suspect witness statements were taken to confirm this.
Consequence	Police contact made with two families unconnected with their investigation with statements taken.

Error Investigation 11

Responsible Party	Public Authority
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber information relating to an IP address linked to a social media username...
Description	Sexualised chat upon social media involving a young child led to a mother to report the facts to police. The contact identified the suspect's username. When a RIPA application was made around this username the applicant entered xxx.xxxxx11 instead of xxx.xxxxx.11 Further acquisitions based on the wrong username led officers to the home of an innocent male. To exacerbate matters these events started in 2013 passed to another public authority in 2016 when the arrest took place. This error wasn't reported to IPCO until September 2017.
Consequence	Innocent person arrested and interviewed.

Error Investigation 12

Responsible Party	Public Authority
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber information relating to customers ID account number
Description	Inappropriate contact with a child via a social media site (grooming). Officers submitted details of three different IP address date and times all linked to the same customer account number. When the three separate IP activities were entered into the CSPs portal, in the third the SPoC entered a different customer account number. This led to the first two results coming back to the same customer and the third to another albeit within the same police area. Despite corroboration not being achieved a package was sent out to the force covering both postal addresses. Upon receipt local intelligence checks flagged one of the addresses of interest. It was this address that two of the three IP results had been resolved to. An approach was made to the other address for them to be eliminated.
Consequence	Police visit to a home of a family unconnected to their investigation.

Error Investigation 13

Responsible Party	Public Authority
Human or Technical	Human
Cause	Use of a corrupted and out date Macro to convert IPv6 addresses
Data Acquired	Subscriber information relating to an IP address
Description	A public authority investigation into harassment over the internet by a named suspect. In order to prove the offence officers sought the resolution of four IP addresses all of which had been used at the time of contact. Three of the IPs had been captured in a version known IPv6. The fourth had been captured in an older format IPv4. To acquire the customer details from an IPv6 address the SPoC must convert the string using a Macro. Once converted this new string is provided to the CSP. An out of date version of the Macro was used drawing back the same customer account for all three IPv6 resolutions. Only in the resolution of the IPv4 address did the suspects appear. Believing the suspect might be using a friends/family home broadband, officers made contact with the customer whose had wrongly been connected to the IPv6 results.
Consequence	Police visit to a home of a family unconnected to their investigation.

Error Investigation 14

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data
Data Acquired	Subscriber information relating to an IP address
Description	A public authority received information of sexualised chat taking over social media involving a minor. The contact identified the suspect's username, time/date of its registration and time/date of the activity. When a RIPA application was made, the applicant wrongly assigned the time/date of the activity to the IP address used when registering their account. These events started in 2015 passed to another public authority in 2016 when the arrest took place. This error wasn't reported to IPCO until November 2017.
Consequence	Two innocent persons arrested and interviewed. Investigation yet to be finalised.

Error Investigation 15

Responsible Party	Public Authority
Human or Technical	Human
Cause	Misinterpretation of data.
Data Acquired	Subscriber information relating to IP addresses
Description	A public authority 's officers identified the Peer to Peer sharing of indecent images of children by six unique users. In turn this led to the execution of eight search warrants. When nothing incriminating was found on any of the devices examined a review was undertaken. This review found the data upon which all IP address resolutions were based upon was flawed. This remains an ongoing IPCO investigation.
Consequence	Search warrants executed upon eight innocent households. Equipment seized. Investigation yet to be finalised.

Error Investigation 16

Responsible Party	Communication Service Provider (CSP)
Human or Technical	Human
Cause	Limited number of recycled mobiles still having previous subscriber assigned to it
Data Acquired	Subscriber
Description	Public Authority trying to trace the subscriber for a mobile number used to make an abandoned 999 call. Under urgent provision the Public Authority accessed the CSP's portal and obtained the subscriber details. To combat a known issue within the disclosure system of this particular CSP staff will recheck any request to checks its accuracy. If an inaccuracy was found the CSP would advise Public Authority. Given the urgency the Public Authority had taken action before the CSP was able to advise them of an error.
Consequence	Visit made to home unconnected to this incident.

Error Investigation 17

Responsible Party	Communication Service Provider (CSP)
Human or Technical	Human
Cause	Cross wires within street furniture
Data Acquired	Subscriber information relating to an IP address
Description	Peer to Peer sharing of indecent images of children (IICO) identified by a public authority. IP address resolution led officers to a home. Equipment seized no incriminating data found. Three months later similar activity was again linked to the same home, police revisit house nothing incriminating found. Further activity was identified two months later and home revisited. Examination of the router found an anomaly with the IP address assigned to it. The CSP contacted and their investigation found cross wires within the street furniture. The crossing of two wires assigned the internet activity of one house as that of the other and vice versa.
Consequence	Three visits to the home of an innocent family. Equipment seized. Safeguarding protocol enacted. IPT aware.

Error Investigation 18

Responsible Party	Communication Service Provider (CSP)
Human or Technical	Human
Cause	Transposition
Data Acquired	Subscriber
Description	Public Authority trying to trace the subscriber for a mobile number connected to a missing person enquiry. An application for the subscriber check was made and the detail was correctly passed to the CSP. In a combination of transposition and lack of experience the Disclosure Officer provided the Public Authority with incorrect subscriber details.
Consequence	Visit made to home unconnected to this incident. Delayed welfare check. Missing person was found safe and well.

Error Investigation 19

Responsible Party	Internet Service Provider (ISP)
Human or Technical	Technical
Cause	Failure to advise changes to Time Zone format
Data Acquired	Subscriber information relating to an IP address
Description	An Internet Service Provider (ISP) changed the format in how time is recorded from a 24hrs format to 12 hrs. This change wasn't notified to any US or UK authority. The change in format didn't include any AM or PM against the time stamp provided. This created a number of applications where the actual time sought was out by 12 hours. Example: Time stamp from ISP read 12:34:29 taken by the Public Authority as 12:34:29 PM. In fact the actual time was 12:34:29 AM or 00:34:29 if the 24 hour clock was still being used. Once discovered immediate steps were put in place to halt all activity involving results from this ISP. Every public authority was contacted and asked to complete a questionnaire. The results identified 173 incidents involving this ISP and could be broken down as follows; 153 no error. In these the actual time e.g. 12:34:29 was PM that when applied for in the 24hr format was one in the same. 17 recordable errors. In these the actual time was e.g. 00:34:29 but applied for as 12:34:39 (24hr clock). However the same user held the IP across both times. 3 reportable errors. In these the IP had moved, e.g. the customer for the IP at 00:34:29 had changed to another by 12:34:39 (times of the application).
Consequence	Search warrant executed at the address of an innocent person. EU national linked but couldn't be traced. Package stopped before action taken.

Error Investigation 20

Responsible Party	Communication Service Provider (CSP)
Human or Technical	Technical
Cause	Mismatch of addresses stored within retention records
Data Acquired	Subscriber information relating to an IP address
Description	In two separate investigations (Peer to Peer sharing of indecent images of children and sexualised contact over social media) application made to resolve IP address linked to these investigations. In both the results returned the customers name and a postal address. In one the named account holder couldn't be linked to the postal address. In the other a connection was found but the information was over 10 years ago. Search warrants were executed 4 months apart with the occupant at one arrested and at the other devices only were seized. Forensic examinations revealed nothing from either warrant. A third investigation 2 months later identified activity at one of the addresses subject above. Before any action was taken contact with the CSP was made to check its veracity. Having checked the CSP concluded a fault was present in a small number of accounts. In these the installation and billings address has fallen out of sync when updates had been made. Upon receipt of this information the Public Authority took no action. The CSP reviewed 9,500 similar requests records and found another 19 corrupted files. 17 were found to contain accurate data. As regards the remaining two it transpires that police visited both addresses in their efforts to locate vulnerable children.
Consequence	Search warrant and arrest of an innocent person. Search warrant executed at the address of an innocent person. Delayed welfare checks and visits (2) to homes of persons unconnected with efforts vulnerable children.

Error Investigation 21

Responsible Party	Internet Service Provider (ISP)
Human or Technical	Human
Cause	Incorrect house number entered when setting up a broadband account (2014)
Data Acquired	Subscriber information relating to 2 IP addresses
Description	A public authority received information of sexualised chat taking place over social media. The contact identified two IP addresses (time and date) when contact with the child had occurred from within the UK. A RIPA application was made to resolve the customers assigned each IP. The results from different ISPs brought back the same account name but for two different houses albeit within the same street. No other link could be found between the two houses. Search warrants were drawn. In a phased approach officers approached one of the houses and quickly eliminated the occupier. The search warrant wasn't executed and no property was seized. The warrant was executed; the occupant was arrested and later charged.
Consequence	Visit made to home of an innocent family.

Error Investigation 22

Responsible Party	Internet Service Provider (ISP)
Human or Technical	Human
Cause	Clerical Error
Data Acquired	Subscriber information relating to an IP addresses
Description	A public authority was investigating the uploading of indecent images of children (IIOC). The officer identified an IP address used by the offender during their upload and sought its resolution into customer details. Once authorised a Notice was served upon the ISP who provided the public authority with details of a company. Contact with the company was made and enquires commenced to try and ascertain the likely perpetrator. The Chairman of the company was able to eliminate his company as the IP in question hadn't been in use. Liaison with the ISP quickly established a clerical error on their part. With two customers having very similar company names the ISP inadvertently disclosed details against the wrong company.
Consequence	Contact made with the Chairman of a company unconnected to the investigation.

Error Investigation 23

Responsible Party	Communication Service Provider (CSP)
Human or Technical	Technical
Cause	Corruption of data following updates to certain accounts
Data Acquired	Subscriber information relating to telephony and IP addresses
Description	Two public authorities sought communications data from a CSP for unconnected incidents. In both the CSP provided incorrect data (wrong name and address). Both incidents sought the assistance of the account holders. Each visit quickly established the likelihood of an error with the data used to take officers to each address.. The CSP was contacted and their investigation identified that in very unique circumstances changes to certain accounts could lead to errors in the recording of data.
Consequence	Contact made with customers (2) unconnected to either incident.

Error Investigation 24

Responsible Party	Communication Service Provider (CSP)
Human or Technical	Technical
Cause	Incorrect background setting (time zone).
Data Acquired	WiFi usage by IP address
Description	A CSP reported to IPCO an error in their resetting of Wifi usage data around the time zone. This had the potential of making results out by one hour. An immediate check was made of the results previously provided to public authorities seeking WiFi usage.. This work identified 19 potential errors spread across 14 public authorities. A questionnaire was sent out to each the following results obtained. 15 – No impact on the investigation/incident. In the remaining 4 the following action occurred: • Search warrant executed and devices seized at home of innocent person. • Repeat visits no one home further visits stopped upon notification. • Discrepancy with the location of a missing person (later found) • Location information at variance to other evidence submitted. Full disclosure to CPS and defence
Consequence	Search warrant executed at the address of an innocent person. Investigation yet to be finalised.

19. Glossary for Public Authority Categories

The following explains how in this annual report IPCO has categorised public authorities that can utilise investigatory powers

Intelligence Agencies	• Secret Intelligence Service (SIS) • Security Service (MI5) • GCHQ References to 'UKIC' mean the United Kingdom Intelligence Community and include the three intelligence agencies and Defence Intelligence
Law Enforcement Agencies (LEAs)	This refers to • All territorial police forces in the UK • All other police forces including the British Transport Police, MOD Police, Royal Military Police, RAF Police, Royal Navy Police, Civil Nuclear Constabulary, Port of Dover Police, Port of Liverpool Police • HMRC • National Crime Agency • The Home Office (Border Force & Immigration Enforcement)

Other Public Authorities (OPAs)	• British Broadcasting Corporation • Care Quality Commissioner • Centre for Environment, Fisheries and Aquaculture Science (CEFAS) • Charity Commission • Common Services Agency for the Scottish Health Service • Criminal Cases Review Commission • Department for Business Innovation & Skills • Department for Communities and Local Government • Department for the Environment, Food & Rural Affairs (DEFRA) • Department of Transport – Air Accident Investigation Branch (AAIB) • Department of Transport – Driver and Vehicle Standards Agency (DVSA) • Department of Transport – Marine Accident Investigation Branch (MAIB) • Department of Transport – Maritime & Coastguard Agency (MCA) • Department of Transport – Rail Accident Investigation Branch (RAIB)
Other Public Authorities (OPAs) continued	• Environment Agency / Natural Resources Wales • Food Standards Agency • Food Standards Scotland • Gambling Commission • Gangmasters and Labour Abuse Authority • General Pharmaceutical Council • Health & Safety Executive • HM Chief Inspector of Education, Childrens Services and Skills (OFSTED) • Independent Police Complaints Commission (IPCC) • Information Commissioner • Marine Scotland • National Health Service Business Services Authority (NHS Protect) • Northern Ireland Office (Prison Service for Northern Ireland) • Office of Communications (OFCOM) • Office of the Police Ombudsman for Northern Ireland (PONI) • Police Investigations and Review Commissioner (PIRC) • Prudential Regulation Authority • Royal Mail
Local Authorities	All UK local authorities
Fire & Rescue Services	All separately constituted Fire & Rescue services in the UK

Contact us

Email: Info@ipco.org.uk
Follow us: Twitter = @IPCOffice
Visit our website: https://www.ipco.org.uk

Designed by Design102

design102 Find out more at design102.co.uk
Design that makes a difference

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

CCS0119377508
ISBN: 978-1-5286-0971-5