HM Government

HM Government Transparency Report 2018:

Disruptive and Investigatory Powers

July 2018

Cm 9609

HM Government Transparency Report 2018:

Disruptive and Investigatory Powers

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

July 2018

Cm 9609

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk

ISBN 978-1-5286-0719-3
CCS0418538240 07/18

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

Foreword

The proportionate use of investigatory and disruptive powers is essential to tackle the threats we face from terrorism and crime. But in a democracy it is right that those powers are only used when it is necessary to do so and that the Government is as transparent as possible about their use. Since the last of these reports was published in February 2017, the Government has continued to take new steps to keep the public as informed as possible about the way in which public authorities undertake their investigations, and the ways in which terrorists and criminals are disrupted. The Government is committed to increasing the transparency of the work of our security and intelligence and law enforcement agencies and we have gone further than ever before to put information in the public domain about the activity undertaken by these agencies to keep the public safe. This includes bringing into force, fives Codes of Practice in Parliament under the Investigatory Powers Act 2016 and holding a public consultation on proposed legislative changes in respect of communications data.

I am pleased to continue that process with the publication of this third edition of the Transparency Report. The horrific attacks that we have seen since the last Report have focused the public's attention on investigations and the disruption of terrorist activity.

Following these attacks, we have recognised that there has been a significant shift in the terrorist threat to the UK. We recently published an updated and strengthened counter-terrorism strategy, CONTEST, following a fundamental review of our entire approach to ensure that we have the best response to the heightened threat in the coming years.

We also continue to plan and prepare for the risk posed by those wishing to return to Britain, who travelled to the conflict in Syria and Iraq. Many of the most dangerous individuals remain overseas and given their training, indoctrination, experience and contacts they pose significant challenges for the security and intelligence agencies and for law enforcement. In addition to seeking prosecution for returners, we are using a range of tools and powers to disrupt and diminish that threat. The use of these tools is reflected in the figures in this report.

We are also working towards full implementation of the Investigatory Powers Act, which was given Royal Assent on 29 November 2016. This has included the establishment of a stronger and more transparent oversight regime, with the creation of a new Investigatory Powers Commissioner (IPC), to oversee and inspect the use of investigatory powers by the police, law enforcement and security and intelligence agencies. In addition to consolidating the functions of the Chief Surveillance Commissioner, Interception of Communications Commissioner, and Intelligence Services Commissioner, the IPC will have new powers, including a judicial 'double-lock', which will require the Secretary of State's decision to issue a warrant to be approved by a Judicial Commissioner. This demonstrates the Government's commitment to building a transparent legal framework and robust regulatory regime.

This is the third edition of this report and, as was the case in both previous iterations, it brings together and seeks to explain information, both in relation to the threats we face and what we do to counter them. It provides extensive statistical information about the various disruptive and investigatory powers used by our law enforcement and security and intelligence agencies. In addition, it provides a detailed explanation of why these powers are required, how they are used, and, crucially, how their use is overseen and subject to safeguards.

Through this process we seek to provide the public with a comprehensive understanding of the tools that are available to our law enforcement and security and intelligence agencies, and the essential part those tools play in protecting the public and defending our national security.

Sajid Javid MP

Home Secretary

2 - Introduction

The first priority of any Government is keeping the United Kingdom safe and secure. In 2015 the Government published the National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) and undertook to report annually to Parliament on progress with their implementation.

While Departments remain focused on implementing the SDSR, the Government is also undertaking a National Security Capability Review (NSCR) to ensure we have the policies, strategies, skills and capabilities we need to respond to emerging and evolving threats to national security in the light of changes in our global context since 2015. The NSCR will ensure that the underlying polices and plans across the national security system are as joined-up, efficient, and effective as possible.

Under the Government's counter-terrorism strategy CONTEST, we work to reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence.

However, as the threat we face from terrorism has become more complex, our strategies have needed to evolve. Following the attacks in London and Manchester last year, the former Home Secretary, Amber Rudd, asked David Anderson QC, the former Independent Reviewer of Terrorism Legislation, to review and report on the post-attack and operational improvement reviews carried out by counter-terrorism police and MI5. Mr Anderson endorsed, as far as he felt able, the conclusions and recommendations made in these reviews and considered that the recommendations will, on the whole, strengthen the ability of MI5 and the police to stop most terrorist attacks in the future. Mr Anderson was chosen to conduct this assurance work due to his standing as an eminent independent expert.

Drawing on lessons learned from the attacks in London and Manchester, in June of last year the Prime Minister outlined the Government's commitment to review CONTEST, the results of which have recently been published in an updated and strengthened strategy.

Over the course of 2017, the UK threat level, set by the Joint Terrorism Analysis Centre, was raised twice from SEVERE to CRITICAL. On both occasions Operation TEMPERER was brought into effect – providing military support to backfill armed guarding duties, to free up police resource to respond to the incidents.

Throughout the year we continued to use the full range of capabilities available to disrupt and manage the return of individuals from Syria and Iraq. Approximately 900 individuals of national security concern have travelled to the Syria/Iraq region to take part in the conflict. We estimate that 40 per cent of these people have returned and approximately 20 per cent have been killed in the region. As we have previously confirmed, a significant proportion of those who have already returned were assessed as no longer being of national security concern. However those who travelled to, or remained in Syria or Iraq from 2014 are more likely to be a current national security concern.

We continue to seek to prosecute foreign fighters where there is evidence that crimes have been committed, and to ensure that they do not pose a threat to our national security. In addition to seeking prosecution, the powers covered in this report have been and will be used to reduce the cohort of overseas individuals of national security concern who can return, and to mitigate the threat they pose. Where appropriate, we have used nationality and immigration

powers to deprive individuals of their British citizenship and to exclude foreign nationals from the UK who presence here would not be conducive to the public good. We have also disrupted the ability of people to travel abroad, and to return to the UK, including through the lawful temporary seizure of passports at the border, and the introduction of Temporary Exclusion Orders (TEOs).

The UK is facing a number of different and enduring terrorist threats. The increased threat has mainly been caused by the rise of Daesh, combined with the persistent threat from Al Qa'ida. Extreme right wing terrorism is a growing threat: during 2017, the Home Office laid an order recognising two aliases for the proscribed far right group, National Action. Alongside this, there is an ongoing threat from Northern Ireland Related Terrorism (NIRT). The threat to Northern Ireland from NIRT is assessed to be SEVERE, indicating an attack is highly likely. The threat to Great Britain from NIRT is currently assessed to be MODERATE meaning an attack is possible, but not likely.

Serious and organised crime (SOC) is an inherently transnational security threat and evolves at pace. Its impact is wide-ranging, continuous and cumulatively damaging. In 2018, we are aware of over 4,600 organised crime groups operating in the UK. Serious and organised criminals target vulnerable individuals, public services and the private sector. They are continually looking for new victims and novel methods to make money, particularly online. The resulting harm to the economy, communities and citizens is extensive; SOC affects more UK citizens, more often, than any other national security threat and leads to more deaths in the UK each year than all other national security threats combined.

Organised criminal groups can also provide specialist services that are used by terrorists and other hostile actors.

In March 2017 the former Home Secretary announced a review of the Government's Serious and Organised Crime Strategy. A new strategy will be published in 2018. In light of the changing threat and building on progress made under the current strategy, the new strategy will ensure our response keeps pace with the activities and methodologies of serious and organised criminals.

Hostile state activity, including espionage, continues to pose a serious threat to British interests. The March 2018 nerve agent attack in Salisbury, highly likely conducted by the Russian state, demonstrates that hostile states can pose a direct threat to life and wider public safety in the UK. We have also seen examples over the last year of the increasing threat from state-linked cyber incidents including the WannaCry attack. The 2015 NSS set out the Government's determination to address cyber threats and put in place tough and innovative measures as a world leader in cyber security. Since its launch in October 2016 as part of the National Cyber Security Strategy, the National Cyber Security Centre has been a key means for government to deliver many elements of strengthened cyber security for the UK.

To counter these and other threats, it is crucial that we have the necessary powers and that they are used appropriately and proportionately.

This report is split into two main sections. The first includes figures on the use of disruptive and investigative powers. It explains their utility and outlines the legal frameworks that ensure they can only be used when necessary and proportionate, in accordance with the statutory functions of the relevant public authorities. The second section explains the roles of the Commissioners and other bodies who provide independent oversight and scrutinise the use of these powers.

There are limitations concerning how much can be said publically about the use of certain sensitive techniques. To go into too much detail may encourage criminals and terrorists to change their behaviour in order to evade detection.

However, it is extremely important that the public are confident that the security and intelligence and law enforcement agencies have the powers they need to protect the public and that these powers are used proportionately. The agencies rely on many members of the public to provide support to their work. If the public do not trust the police and security and intelligence agencies, that mistrust would result in a significant operational impact.

The purpose of this report is therefore to provide the public with a complete guide, in one place, of the powers used to combat threats to the security of the United Kingdom, the extent of their use and the safeguards and oversight in place to protect against their misuse.

3 – Terrorism Arrests and Outcomes

Conviction in a court is one of the most effective tools we have to stop terrorists. The Government is therefore committed to pursuing convictions for terrorist offences where they have occurred. Terrorism-related arrests are made under the Police and Criminal Evidence Act 1984 (PACE). They can also be made under the Terrorism Act 2000 (TACT) in circumstances where arresting officers require additional powers of detention or need to arrest a person suspected of terrorism-related activity without a warrant. Whether to arrest someone under PACE or TACT is an operational decision to be made by the police.

In the year ending 31 March 2018, 441 persons were arrested for terrorism-related activity, an increase of 17% from the 378 arrests in the previous year. This reflects a large number of arrests being made following terrorist attacks in London and Manchester. In the year ending March 2018, there were 23 arrests in connection to the terrorist attack in Manchester (22 May 2017), 21 arrests in connection to the London Bridge attack (3 June 2017), one arrest made in connection to the Finsbury Park Mosque attack (19 June 2017) and 7 arrests made in connection with the Parsons Green attack (15 September 2017). This was the highest number of arrests in a year since the data collection began in September 2001.

Of the 441 arrests, 143 (32%) resulted in a charge, and 80% of these charges (relating to 114 individuals) were considered to be terrorism-related. Many of these cases are ongoing. Therefore, the number of charges resulting from the 441 arrests in the year ending 31 March 2018 can be expected to rise over time.

Of the 114 people charged with terrorism-related offences, 41 have been prosecuted and 67 are awaiting prosecution. 39 of the prosecution cases led to individuals being convicted of an offence: 37 for terrorism-related offences and two for non-terrorism related offences.

As at 31 March 2018, there were 228 persons in custody in Great Britain[1] for terrorism-related offences. This total was comprised of 186 persons (82%) in custody who held Islamist-extremist views, 29 (13%) who held far right-wing ideologies and a further 13 other persons.

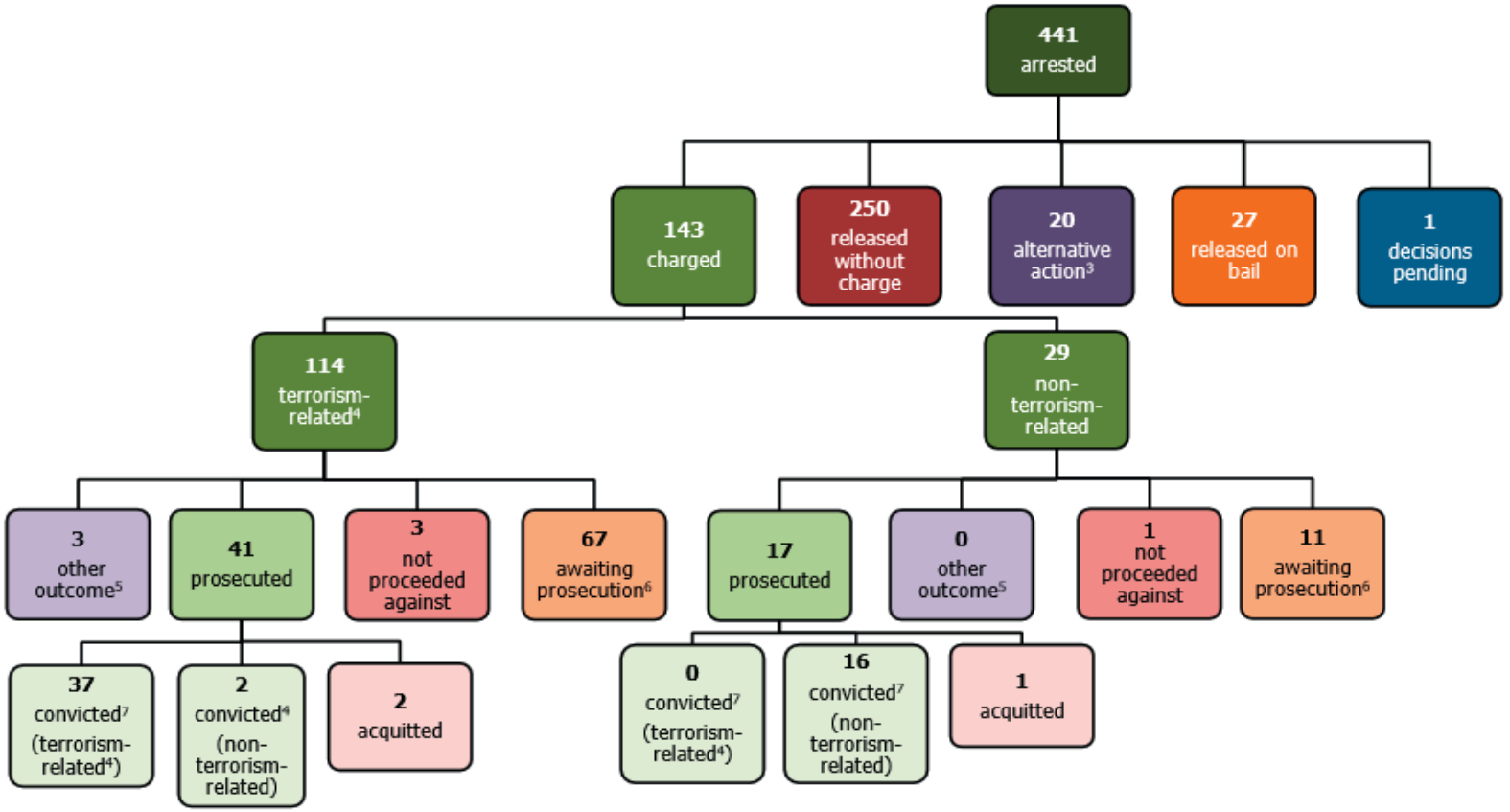
This was an increase of 48 persons compared to the 180 persons in custody as at 31 March 2017. The number of individuals in custody for terrorism-related offences has shown a steady increase in recent years, across all ideologies.

Terrorism arrests and outcomes are often highly reliant on the investigatory powers and tools outlined in this report.

[1] Data are provided to the Home Office by Her Majesty's Prison and Probation Service and the Scottish Prison Service. As such, the statistics set out in this Chapter provide information on the number of persons in custody for terrorism-related offences in Great Britain, not all areas of the United Kingdom.

Figure 2: Arrests and outcomes[1] year ending 31 March 2018[2]

The flow chart is designed to summarise how individuals who are arrested on suspicion of terrorism-related activity are dealt with through the criminal justice system. It follows the process from the point of arrest, through to charge (or other outcomes) and prosecution.



Source: *Home Office, 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation', data tables A.01 to A.07*

Notes:

1. Based on time of arrest.
2. Data presented is based on the latest position with each case as at the date of data provision from National Counter-Terrorism Police Operations Centre (13 April 2018).
3. 'Alternative action' includes a number of outcomes, such as cautions, detentions under international arrest warrant, transfer to immigration authorities etc. See https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-financial-year-ending-march-2018data tables for a complete list.
4. Terrorism-related charges and convictions include some charges and convictions under non-terrorism legislation, where the offence is considered to be terrorism-related.
5. The 'other' category includes other cases/outcomes such as cautions, transfers to UK Border Agencies, the offender being circulated as wanted, and extraditions.
6. Cases that are 'awaiting prosecution' are not yet complete. As time passes, these cases will eventually lead to a prosecution, 'other' outcome, or it may be decided that the individual will not be proceeded against.
7. Excludes convictions that were later quashed on appeal.

4 – Serious Organised Crime Arrests and Outcomes

The National Crime Agency (NCA) is responsible for leading and coordinating the fight against serious and organised crime affecting the UK.

The NCA published its latest Annual Report and Accounts in July 2017.[2] This report explained the NCA's response to the threat we face from serious and organised crime between 1 April 2016 and 31 March 2017. An outline of this activity is below.

It should be noted that these figures provide only an indication of the response to serious and organised crime. The NCA is focused on the disruptive impact of its activities against priority threats and high priority criminals and vulnerabilities, rather than merely on numbers of arrests or volumes of seizures. Furthermore, the UK's overall effort to tackle serious and organised crime also involves the work of a wide range of other public authorities, including police forces, Immigration Enforcement, Border Force and HM Revenue and Customs.

Arrests and Convictions

A significant part of the NCA's activity to disrupt serious and organised crime is to investigate those responsible in order that they can be prosecuted. In the period from 1 April 2016 to 31 March 2017, 1,441 individuals were arrested in the UK by NCA officers, or by law enforcement partners working on NCA-tasked operations and projects. In the same period, there were 657 convictions in relation to NCA casework in the UK and 1,738 disruptions. NCA activity also contributed to 1,176 arrests overseas.

Interdictions

Between 1 April 2016 and 31 March 2017, activity by the NCA resulted in the interdiction of 147.5 tonnes of drugs, including 79.3 tonnes of cocaine, 3.8 tonnes of opium and 5.6 tonnes of heroin. In addition, during this period NCA activity resulted in the seizure of 528 guns and 71 other firearms.

Criminal Finances

In the period from 1 April 2016 to 31 March 2017 the NCA recovered assets worth £28.3 million. In addition, the agency denied assets of £82.8 million. Asset denial activity included cash seizures, restrained assets and frozen assets.

Child Protection

In this reporting period, NCA activity led to 1,896 children being protected or safeguarded. Child protection is when action is taken to ensure the safety of a child, such as taking them out of a harmful environment. Child safeguarding is a broader term including working with children in their current environment, such as working with a school or referring a child for counselling.

[2] "The National Crime Agency: Annual Report and Accounts 2016/2017" is available in full at www.nationalcrimeagency.gov.uk/publications

As with terrorism arrests and convictions, serious and organised crime outcomes, such as those outlined above, are often highly reliant on the investigative powers outlined in this report.

5 – Disruptive Powers

5.1 - Stops and Searches

Powers of search and seizure are vital in ensuring that the police are able to acquire evidence in the course of a criminal investigation, and are powerful disruptive tools in the prevention of terrorism.

Section 47A of the Terrorism Act 2000 (TACT) enables a senior police officer to make an authorisation, specifying an area or place where they reasonably suspect that an act of terrorism will take place. Within that area and for the duration of the authorisation, a uniformed police constable may stop and search any vehicle or person for the purpose of discovering any evidence – whether or not they have a reasonable suspicion that such evidence exists – that the person is or has been concerned in the commission, preparation or instigation of acts of terrorism, or that the vehicle is being used for such purposes.

The authorisation must be necessary to prevent the act of terrorism which the authorising officer reasonably suspects will occur, and it must specify the minimum area and time period considered necessary to do so. The authorising officer must inform the Secretary of State of the authorisation as soon as is practicable, and the Secretary of State must confirm it. If the Secretary of State does not confirm the authorisation, it will expire 48 hours after being made. The Secretary of State may also substitute a shorter period, or a smaller geographical area, than was specified in the original authorisation.

Until September 2017, this power had not been used in Great Britain since the threshold of authorisation was formally raised in 2011. This reflects the intention that the power should be reserved for exceptional circumstances, and the requirement that it only be used where necessary to prevent an act of terrorism that it is reasonably suspected is going to take place within a specified area and period. However, following the Parsons Green attack, on 15 September 2017, the power was authorised for the first time. The four forces were British Transport Police (BTP), City of London Police, North Yorkshire Police and West Yorkshire Police. There were a total of 128 stop and searches conducted (126 of which were conducted by BTP), which resulted in 4 arrests (all BTP).

One authorisation has been made in Northern Ireland under section 47A, in unusual circumstances which are described by the Independent Reviewer at paragraph 6.9 of his report on The Terrorism Acts in 2013. On 9 May 2013, the Court of Appeal held that the widely used stop and search powers under sections 21 and 24 of the Justice and Security (Northern Ireland) Act 2007 were not properly exercisable, since adequate safeguards to prevent their arbitrary use, in the form of a Code of Practice, were not in place. Considering that the statutory conditions for a section 47A authorisation were present, an Assistant Chief Constable of the PSNI issued an authorisation that day, covering parts of Northern Ireland. That authorisation was confirmed by the Secretary of State on 10 May 2013, and remained in place until a Code of Practice was introduced on 15 May 2013. 70 persons were stopped under the authorisation. The Independent Reviewer inspected the authorisation on a visit to Belfast in September 2013,

at the request of the PSNI, and it was also inspected on another occasion by the Human Rights Advisor of the Northern Ireland Policing Board[3].

Under sections 43 and 43A of TACT, police officers have further powers to stop and search, respectively, a person or vehicle. These powers do not require a section 47A authorisation to be in place. Instead they require the officer to reasonably suspect that the person is a terrorist or that the vehicle is being used for terrorist purposes.

In the year ending 31 March 2018, 768 persons were stopped and searched by the Metropolitan Police Service under section 43 of TACT (this data is not available in relation to other police forces). This represents a 70% increase from the previous year's total of 453. However, over the longer term, there has been a 38% fall in the number of stop and searches, from 1,229 in the year ending 31 March 2010 (the first comparator year that figures are available for) to 768 in the year ending 31 March 2018. In the year ending 31 March 2018, there were 64 resultant arrests; the arrest rate of those stopped and searched under section 43 was 8%, up from 7% in the previous year.[4]

5.2 - Port and Border Controls

Schedule 7 to the Terrorism Act 2000 (Schedule 7) helps protect the public by allowing an examining police officer to stop and question and, when necessary, detain and search individuals travelling through ports, airports, international rail stations or the border area. The purpose of the questioning is to determine whether that person appears to be someone who is, or has been, involved in the commission, preparation or instigation of acts of terrorism. The Schedule 7 power also extends to examining goods to determine whether they have been used in the commission, preparation or instigation of acts of terrorism.

Prior knowledge or suspicion that someone is involved in terrorism is not required for the exercise of the Schedule 7 power. Examinations are also about talking to people in respect of whom there is no suspicion but who, for example, are travelling to and from places where terrorist activity is taking place or emerging, to determine whether those individuals are, or have been, involved in terrorism. This is particularly important given the current threat from Syria and Iraq.

The Schedule 7 Code of Practice for examining officers provides guidance on the selection of individuals for examination. The most recent version of the Code came into effect on 25 March 2015.[5] Selection for questioning under Schedule 7 is based on the current terrorist threat to the UK posed by the various terrorist groups active in and outside the UK. Selection is made on the basis of informed considerations. This can include intelligence, which may be imprecise and relate to events and places rather than to specific people. Requiring suspicion of individuals would severely curtail the ability of the police to examine people to determine their involvement in terrorism.

---

[3] Further details may be found at https://terrorismlegislationreviewer.independent.gov.uk

[4] Full statistical releases on the operation of police powers under the Terrorism Act 2000, including stop and search powers, are available at www.gov.uk/government/collections/counter-terrorism-statistics

[5] The full Schedule 7 Code of Practice is available at https://www.gov.uk/government/publications/code-of-practice-for-examining-officers-and-review-officers-under-schedule-7-to-the-terrorism-act-2000

When an individual is examined under Schedule 7 they are given a Public Information Leaflet. The Public Information Leaflet is available in multiple languages and outlines the purpose and provisions of, and obligations under Schedule 7. Key points of the Code of Practice include an individual's rights and relevant contact details (including those needed to provide feedback or make a complaint). An individual can be examined for more than an hour only if that person is formally detained. This requirement ensures examinees' rights are safeguarded: for example, entitling them to receive legal advice from a solicitor.

An individual can complain about a Schedule 7 examination by writing to the Chief Officer of the police force for the area in which the examination took place. Additionally, the Independent Reviewer of Terrorism Legislation is responsible for reporting each year on the operation of the Schedule 7 power.

Statistics on the operation of Schedule 7 powers are published by the Home Office on a quarterly basis.[6] In the year ending 31 March 2018, a total of 15,391 persons were examined under this power in Great Britain, a fall of 15% on the previous year. Throughout the same period, the number of detentions following examinations increased by 16% from 1,530 in the year ending 31 March 2017 to 1,776 in the year ending 31 March 2018.

Of those individuals that were detained (excluding those who did not state their ethnicity), 34 % categorised themselves as 'Chinese or Other'. The next most prominent ethnic groups were 'Asian or Asian British' at 31% and 'White' at 13%. The proportion of those that categorised their ethnicity as 'Black or Black British' or 'Mixed' made up 14% and 9% respectively.

Certain travel routes are given greater focus, use of Schedule 7 is informed by the current terrorist threat to the UK and intelligence underpinning the threat assessment. Self-defined members of ethnic minority communities do comprise a majority of those examined under Schedule 7. However, the proportion of those examined should correlate not to the ethnic breakdown of the general population, or even the travelling population, but to the ethnic breakdown of the terrorist population. In successive reports the former Independent Reviewer of Terrorism Legislation, David Anderson QC, has confirmed that he has no reason to believe that Schedule 7 powers are exercised in a racially discriminatory way. This assessment was endorsed in 2015 by the Supreme Court in their comments in the case of Beghal. In the year ending 31 March 2018, 15,391 people were stopped under Schedule 7 power in Great Britain.[7] There has been a year on year increase in the number of passengers that travelled through UK Ports, which exceeded 300 million in 2016.[8]

Since April 2016, the Home Office has collected data relating to the use of these powers. This data includes the number of goods examinations (sea and air freight), the number of strip searches conducted, and the number of refusals following a request by an individual to

---

[6] Full statistical releases on the operation of police powers under the Terrorism Act 2000 are available at: www.gov.uk/government/collections/counter-terrorism-statistics

[7] Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, quarterly update to March 2018. Available online at: https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-financial-year-ending-march-2018

[8] NAO report (October 2017) The UK border Issues and challenges for government's management of the border in light of the UK's planned departure from the European Union. Available online: https://www.nao.org.uk/wp-content/uploads/2017/10/The-UK-border.pdf

postpone questioning. In the year ending 31 December 2017, a total of 2,549 air freight and 6,715 sea freight examinations were conducted in Great Britain. Regarding strip searches over the same period, there were five instances carried out under Schedule 7. Postponement of questioning (usually to enable an individual to consult a solicitor) was refused on one occasion.

5.3 - Terrorist Asset-Freezing

Terrorist asset-freezing is an important disruptive tool, which aims to stop terrorist acts by preventing funds, economic resources or financial services from being made available to, or used by, someone who might use them for terrorist purposes. The power to freeze assets can be exercised where the statutory test is met, and does not require a criminal prosecution.

The UK's autonomous asset-freezing regime (set out in the Terrorist Asset-Freezing etc. Act 2010 - "TAFA")[9] meets obligations placed on the UK by Resolutions of the UN Security Council and associated European Union Regulations. Meeting these obligations is, in turn, also part of the 40 standards on anti-money laundering and counter-terrorist financing set out by the Financial Action Task Force (FATF). FATF will evaluate the UK's compliance with its standards, and how effectively the UK is implementing those standards, in 2018.

TAFA gives the Treasury the power to impose financial restrictions on individuals and entities. These restrictions have the effect of freezing any funds or assets in the UK (or with a UK nexus) owned held or controlled by a designated person or entity. They also make it an offence for any person to make funds, financial services or economic resources available (directly or indirectly) to, or available for the benefit of, a designated person or entity where that persons knows, or has reasonable cause to suspect, the individual or entity is designated. The Treasury does not proactively identify targets for asset freezes. Rather, the Treasury is advised by operational partners, including the police and Security Service, who identify possible targets for asset freezes and present the evidence supporting the freeze to the Treasury to consider. It is also possible for third countries to identify possible targets, although this is less common.

The UK's terrorist asset-freezing regime contains robust safeguards to ensure the restrictions remain proportionate. Under section 2(1)(a) of TAFA, the Treasury may only designate persons where it has reasonable grounds to believe that they are, or have been, involved in terrorist activity, or are owned, controlled (directly or indirectly) or acting on behalf of or at the direction of someone who is, or has been, involved in terrorist activity. Under section 2(1)(b), financial restrictions may only be applied where the Treasury considers it necessary for purposes connected with protecting members of the public (anywhere in the world) from terrorism. The requirements of both section 2(1)(a) and 2(1)(b) must be met for a designation to be made. In addition to meeting the statutory test, a designation will only be imposed where an asset freeze it is considered to be the most proportionate tool available.

In addition, there are a number of other safeguards to ensure that the UK's terrorist asset-freezing regime is operated fairly and proportionately:

- The Treasury may grant licences to allow exceptions to the asset freeze, ensuring that human rights are taken account of, whilst also ensuring that funds are not diverted to terrorist purposes.

[9] The Terrorist Asset-Freezing etc. Act 2010 is available at www.legislation.gov.uk/ukpga/2010/38/contents

- Designations expire after a year unless reviewed and renewed. The Treasury may only renew a designation where the requirements under sections 2(1)(a) and (b) of TAFA continue to be met.

- Designations must generally be publicised but can be notified on a restricted basis and not publicised when one of the conditions in section 3(3) of TAFA is met. Conditions are that:
  the Treasury believe that the designated person is under 18; or
  the Treasury consider the disclosure of the designation should be restricted:
  i) in the interests of national security;
  ii) for reasons connected with the prevention or detection of serious crime; or
  iii) in the interests of justice.

- Where a designation is notified on a restricted basis, the Treasury can also specify that people informed of the designation treat the information as confidential.

- A designated person (or entity) has a right of appeal against a designation decision in the High Court, and anyone affected by a licensing decision (including the designated person (or entity)) can challenge on judicial review grounds any licensing or other decisions of the Treasury under TAFA. There is a closed material procedure available for such appeals or challenges using specially cleared advocates to protect closed material whilst ensuring a fair hearing for the affected person.

- Individuals are notified, as far as it is in the public interest to do so, of the reasons for their designation. This information is kept under review and if it becomes possible to release more detailed reasons the Treasury will do so.

- The Independent Reviewer of Terrorism Legislation, Max Hill QC, may conduct a review of, and report on, the operation of TAFA[10].

- The Treasury is required to report to Parliament, quarterly, on its operation of the UK's asset freezing regime. In addition, the Treasury also reports on the UK's operation of the EU and UN terrorist asset-freezing regimes.

The following table sets out the volumes of funds frozen, and number of accounts frozen as at 31 December 2017 under TAFA:

	TAFA 2010
Total funds frozen (GBP equivalent at the end of the quarter)	£9,000
Total accounts frozen (at the end of the quarter)	6
Accounts frozen (during the quarter)	0

[10] Full statistical reports for this and previous periods can be found at www.gov.uk/government/collections/operation-of-the-uks-counter-terrorist-asset-freezing-regime-quarterly-report-to-parliament

Accounts unfrozen (during the quarter)	0

The following table sets out the number of natural and legal persons, entities or bodies designated under each of the three regimes as at 31 December 2017:

	TAFA 2010
Total number of designations (at the end of the quarter)	20
Total number of designated individuals (at the end of the quarter)	14
Total number of designated groups and entities (at the end of the quarter)	6
New public designations (during the quarter)	0
New confidential designations[11] (during the quarter)	0
Total number of current confidential designations (at the end of the quarter)	0
Total delistings (during the quarter)	0
Total renewals of designations by HMT (during the quarter)	5

Listings

1. TAFA is one of several CT financial sanctions regimes. Information on all the regimes and the current financial sanctions designations can be found on the OFSI website:

   https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

2. Consolidated list of all the individuals, organisations and businesses subject to financial sanctions in the UK:

   https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

3. Current designations under the UN ISIL-AQ regime & EU Regulation 2016/1686 (Designations under this regulation will be identified as “EU Listing only”):

   https://www.gov.uk/government/publications/current-list-of-designated-persons-al-qaida

11 Confidential designations can be made under section 3(2)-(4) and section 7(2)-(4) of TAFA 2010.

4. Current designations under TAFA and EU 2580/2001 found at: https://www.gov.uk/government/publications/current-list-of-designated-persons-terrorism-and-terrorist-financing

- 'UK listing only' – listed under TAFA 2010 only
- 'Both UK and EU listing' – listed under TAFA 2010 and under the EU's asset freezing regime 2580/2001
- 'EU listing only' – listed under EU's asset freezing regime. The prohibitions are found in Council Regulation (EC) No 2580/2001 with penalties given by TAFA 2010

5.4 - Terrorism Prevention and Investigation Measures

Terrorism Prevention and Investigation Measures (TPIMs) allow the Home Secretary to impose a powerful range of disruptive measures on a small number of people who pose a real threat to our security but who cannot be prosecuted or, in the case of foreign nationals, deported. Subjects could include individuals who intended to travel to fight for Daesh in Syria, or who may have returned from suspected terrorist activity in Syria or Iraq. These measures can include: overnight residence requirements, including relocation to another part of the UK; police reporting; an electronic monitoring tag; exclusion from specific places; limits on association; limits on the use of financial services and use of telephones and computers; and a ban on holding travel documents.

It is the Government's assessment that, for the foreseeable future, there will remain a small number of individuals who pose a real threat to our security but who cannot be either prosecuted or deported. We are clear that there continues to be a need for powers to protect the public from the threat these people pose. This is why we need TPIMs.

The use of TPIMs is subject to stringent safeguards. Before the Secretary of State decides to impose a TPIM notice on an individual, he must be satisfied that five conditions are met, as set out at section 3 of the Terrorism Prevention and Investigation Measures Act 2011 (TPIM Act)[12]. The conditions are that:

- the Secretary of State considers, on the balance of probabilities, that the individual is, or has been, involved in terrorism-related activity (the "relevant activity");
- where the individual has been subject to one or more previous TPIM orders, that some or all of the relevant activity took place since the most recent TPIM notice came into force;
- the Secretary of State reasonably considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, for Terrorism Prevention and Investigation Measures to be imposed on the individual;
- the Secretary of State reasonably considers that it is necessary, for purposes connected with preventing or restricting the individual's involvement in terrorism-related activity, for the specified Terrorism Prevention and Investigation Measures to be imposed on the individual; and
- the court gives permission, or the Secretary of State reasonably considers that the urgency of the case requires Terrorism Prevention and Investigation Measures to be imposed without obtaining such permission.

[12] The Terrorism Prevention and Investigation Measures Act 2011 is available at www.legislation.gov.uk/ukpga/2011/23

The Secretary of State must apply to the High Court for permission to impose the TPIM notice on the individual, except in cases of urgency where the notice must be immediately referred to the court for confirmation.

All individuals upon whom a TPIM notice is imposed are automatically entitled to a review hearing at the High Court relating to the decision to impose the notice and the individual measures in the notice. They may also appeal against any decisions made subsequent to the imposition of the notice, i.e. a refusal of a request to vary a measure, a variation of a measure without their consent, or the revival or extension of their TPIM notice. The Secretary of State must keep under review the necessity of the TPIM notice and specified measures during the period that a TPIM notice is in force.

A TPIM notice initially lasts for one year and can only be extended for one further year. No new TPIM may be imposed on the individual after that time unless the Secretary of State considers, on the balance of probabilities that the individual has engaged in further terrorism-related activity since the imposition of the notice.

In recognition of the severity of the threats we face, the Counter-Terrorism and Security Act 2015 enhanced the powers available in the TPIM Act, including introducing the ability to relocate a TPIM subject elsewhere in the UK (up to a maximum of 200 miles from their normal residence, unless the TPIM subject agrees otherwise) and a power to require a subject to attend meetings as part of their ongoing management, such as with the probation service or Jobcentre Plus staff. The Home Secretary published factors that are considered appropriate to take into account when considering whether to relocate a subject under the overnight residence measure[13]. These are: the need to prevent or restrict a TPIM subject's involvement in terrorism-related activity; the personal circumstances of the individual; proximity to travel links including public transport, airports, ports and international rail terminals; the availability of services and amenities, including access to employment, education, places of worship and medical facilities; proximity to prohibited associates; proximity to positive personal influences; location of UK resident family members; and community demographics.

The last Independent Reviewer of Terrorism Legislation review of the operation of the TPIM Act was published in March 2015[14]. Changes made to the Independent Reviewer's remit through the Counter-Terrorism and Security Act 2015 allowed for a more flexible arrangement in respect of the frequency of this review.

Under the TPIM Act the Secretary of State is required to report to Parliament, as soon as reasonably practicable after the end of every relevant three month period, on the exercise of his TPIM powers.

The most recent published reports cover the period from 1 December 2017 to 28 February 2018 and 1 March 2018 to 31 May 2018.

As at 28 February 2018, there were eight TPIM notices in force, seven of which related to British citizens. During the reporting period:

- one TPIM was revived;
- one TPIM was extended, no TPIMs were revoked;

[13] Written Ministerial Statement on Terrorism Prevention and Investigation Measures, laid on 12 February 2015.

[14] The last report on the operation of TPIMs from the Independent Reviewer of Terrorism Legislation is available at https://terrorismlegislationreviewer.independent.gov.uk/category/reports/tpims-control-orders/

- six variations were made to measures specified in TPIM notices;
- one application to vary measures was refused; and
- eight TPIM subjects were relocated.

As at 31 May 2018, there were eight TPIM notices in force, seven of which related to British Citizens. During the reporting period:

- no TPIMs were extended;
- no TPIMs were revoked or revived;
- 10 variations were made to measures specified in TPIM notices;
- seven applications to vary measures were refused; and
- eight TPIM subjects were relocated[15].

5.5 - Royal Prerogative

The Royal Prerogative is a residual power of the Crown which is used widely across Government in a number of different contexts. In relation to national security, the Royal Prerogative can be used to refuse a passport application, or withdraw an existing passport, under the public interest criteria. The Royal Prerogative is an important tool used to disrupt individuals who seek to travel on a British passport to engage in terrorism-related activity and who would return to the UK with enhanced capabilities to do the public harm.

A passport remains the property of the Crown at all times. HM Passport Office issues or refuses passports under the Royal Prerogative and there are a number of grounds for withdrawal or refusal. The Home Secretary has the discretion, under the Royal Prerogative, to refuse to issue or to withdraw a British passport on public interest grounds. This criterion supports the use of the Royal Prerogative in national security cases. Secretaries of State exercise a range of prerogative powers in different contexts and the courts have upheld the legitimacy of prerogative powers that are not based in primary legislation.

Using the Royal Prerogative, persons may be refused a British passport or may have their existing passport withdrawn on a number of grounds, including that the grant to them, or their continued enjoyment, of passport facilities is contrary to the public interest. Public interest grounds include seeking to harm the UK or its allies by travelling on a British passport to, for example, engage in terrorism-related activity. This power was and is therefore an important tool in managing the threat from individuals seeking to travel to Syria to join the conflict, for example.

On 25 April 2013, the Government redefined the public interest criteria to refuse or withdraw a passport in a Written Ministerial Statement to Parliament[16].

The policy allows passports to be withdrawn, or refused, where the Home Secretary is satisfied that it is in the public interest to do so. This may be the case for:

[15] The latest quarterly report on the exercise of TPIMs is available in full at www.parliament.uk

[16] The full Written Ministerial Statement is available at www.gov.uk/government/speeches/the-issuing-withdrawal-or-refusal-of-passports

"A person whose past, present or proposed activities, actual or suspected, are believed by the Home Secretary to be so undesirable that the grant or continued enjoyment of passport facilities is contrary to the public interest." (Written Ministerial Statement to Parliament 25 April 2013)

There may be circumstances in which the application of legislative powers is not appropriate to the individual applicant but there is a need to restrict the ability of a person to travel.

The application of discretion by the Home Secretary will primarily focus on preventing overseas travel. There may be cases in which the Home Secretary believes that the past, present or proposed activities (actual or suspected) of the applicant or passport holder should prevent their enjoyment of a passport facility whether overseas travel is or is not a critical factor.

Under the public interest criterion, in relation to national security, the Royal Prerogative was exercised to deny access to British passport facilities to:

- 14 individuals in 2017;
- 17 individuals in 2016;
- 23 individuals in 2015;
- 24 individuals in 2014; and
- six individuals in 2013.

An individual may ask for a review of the decision, or apply for a new passport at any time (prompting a review of the decision). In addition, if significant new information comes to light a case review may be triggered. Since 2014, there have been:

- 21 reviews in 2017;
- six reviews in 2016;
- nine reviews in 2015; and
- two reviews in 2014.

As a result of these reviews, passport facilities have been restored to five individuals.

5.6 – Seizure and Temporary Retention of Travel Documents

Schedule 1 of the Counter-Terrorism and Security Act 2015 enables police officers at ports to seize and temporarily retain travel documents to disrupt immediate travel, when they reasonably suspect that a person intends to travel to engage in terrorism related activity outside the UK.

The temporary seizure of travel documents provides the authorities with time to investigate an individual further and consider taking longer term disruptive action such as prosecution, exercising the Royal Prerogative to withdraw or refuse to issue a British passport, or making a person subject to a TPIM order.

Travel documents can only be retained for up to 14 days while investigations take place. The police may apply to the courts to extend the retention period but this must not exceed 30 days in total.

Since February 2015, the power has been exercised:

- 14 times in 2017;
- 15 times in 2016; and
- 24 times in 2015.

Of these, travel documents were retained beyond the 14 day period 36 times.

5.7 – Exclusions

The Secretary of State (usually the Home Secretary) may decide to exclude a non-European Economic Area (EEA) national if he or she considers that the person's presence in the UK would not be conducive to the public good. If a decision to exclude is taken it would need to be reasonable, consistent and proportionate based on the evidence available. The exclusion power arises under the Royal Prerogative. It is normally used in circumstances involving national security, unacceptable behaviour (such as extremism), international relations or foreign policy, and serious and organised crime.

European Economic Area nationals and their family members may be excluded from the UK on grounds of public policy or public security, if they are considered to pose a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.

Between 1 January 2016 to 31 December 2016 the Government excluded 30 people from the United Kingdom, including 20 exclusions on national security grounds. There were 26 exclusions made between 1 January 2017 to 31 December 2017- all on national security grounds.

The Secretary of State uses exclusion powers when justified and based on all available evidence. In all matters, the Secretary of State must act reasonably, proportionately and consistently. Exclusion powers are very serious and the Government does not use them lightly. This power can be used to prevent the return to the UK of foreign nationals suspected of taking part in terrorist related activity in Syria due to the threat they would pose to public security.

5.8 - Temporary Exclusion Orders

The Counter Terrorism and Security Act 2015 introduced Temporary Exclusion Orders (TEOs). This is a statutory power which allows the Secretary of State (usually the Home Secretary) to disrupt and control the return to the UK of a British citizen who has been involved in terrorism-related activity outside the UK. The tool is important in helping to protect the public from any risk posed by certain individuals involved in terrorism-related activity in Syria or Iraq.

The policy was developed in line with the UK's international legal obligations including the European Convention on Human Rights and the EU Free Movement Directive.

A TEO makes it unlawful for the subject to return to the UK without engaging with the UK authorities. It is implemented through cancelling the TEO subject's travel documents and adding them to watch lists (including the authority to carry ('no fly') list), ensuring that when individuals do return, it is in a manner which the UK Government controls. The subject of a TEO commits

an offence if, without reasonable excuse, he or she re-enters the UK not in accordance with the terms of the order.

A TEO also allows for certain obligations to be imposed once the individual returns to the UK and during the validity of the order. These might include reporting to a police station, notifying the police of any change of address, or attending appointments such as a de-radicalisation programme. The subject of a TEO also commits an offence if, without reasonable excuse, he or she breaches any of the conditions imposed.

There are two stages of judicial oversight for TEOs. The first is a court permission stage before a TEO is imposed by the Secretary of State. The second is a statutory review of the decision to impose a TEO and any in-country obligations after the individual has returned to the UK.

The power came into force in the second quarter of 2015. No TEOs were imposed in 2016. The number of TEOs served from 1 January 2017 to 31 December 2017 is 9.

5.9 - Deprivation of British Citizenship

The British Nationality Act 1981 provides the Secretary of State with the power to deprive an individual of their British citizenship in certain circumstances. Such action paves the way for possible immigration detention, deportation or exclusion from the UK and otherwise removes an individual's right of abode in the UK.

The Secretary of State may deprive an individual of their British citizenship if satisfied that such action is 'conducive to the public good' or if the individual obtained their British citizenship by means of fraud, false representation or concealment of material fact. Deprivation is particularly important in helping prevent the return to the UK of certain dual-national British citizens involved in terrorism-related activity in Syria or Iraq.

When seeking to deprive a person of their British citizenship on the basis that to do so is 'conducive to the public good', the law requires that this action only proceeds if the individual concerned would not be left stateless (no such requirement exists in cases where the citizenship was obtained fraudulently).

The Government considers that deprivation on 'conducive' grounds is an appropriate response to activities such as those involving:

- national security, including espionage and acts of terrorism directed at this country or an allied power;
- unacceptable behaviour of the kind mentioned in the then Home Secretary's statement of 24 August 2005 ('glorification' of terrorism etc)[17];
- war crimes; and
- serious and organised crime.

By means of the Immigration Act 2014, the Government introduced a power whereby in a small subset of 'conducive' cases – where the individual has been naturalised as a British citizen and acted in a manner seriously prejudicial to the vital interests of the UK – the Secretary of State may deprive that person of their British citizenship, even if doing so would leave them stateless.

[17] see UK Home Office Press Release 124/2005

This action may only be taken if the Secretary of State has reasonable grounds for believing that the person is able, under the law of a country outside the United Kingdom, to become a national of that country.

In practice, this power means the Secretary of State may deprive and leave a person stateless (if the vital interest test is met and they are British due to naturalising as such), if that person is able to acquire (or reacquire) the citizenship of another country and is able to avoid remaining stateless.

The Immigration Act 2014 also required this additional element of the deprivation power to be reviewed after the first year of being in force (and at three-year intervals thereafter). Therefore in July 2015, David Anderson QC, the Independent Reviewer of Terrorism Legislation, accepted an invitation from the then Immigration Minister to carry out the statutory review. The review covered the period 30 July 2014 to 29 July 2015 and was published on 21 April 2016.[18]

The Government considers removal of citizenship to be a serious step, one that is not taken lightly. This is reflected by the fact that the Home Secretary personally decides whether such action should be taken, where it is considered that it may be conducive to the public good to deprive an individual of citizenship.

Between 1 January 2016 and 31 December 2016, 14 people were deprived of British citizenship on the basis that to do so was 'conducive to the public good'. Between 1 January 2017 and 31 December 2017, 104 people were deprived, again as to do so was considered to be 'conducive to the public good'.[19]

5.10 - Deportation with Assurances

Where prosecution is not possible, the deportation of foreign nationals to their country of origin may be an effective alternative means of disrupting terrorism-related activities. Where there are concerns for an individual's safety on return, government to government assurances may be used to achieve deportation in accordance with the UK's human rights obligations.

Deportations with Assurances (DWA) enables the UK to reduce the threat from terrorism by deporting foreign nationals who pose a risk to our national security, while still meeting our domestic and international human rights obligations. This includes Article 3 of the European Convention on Human Rights, which prohibits torture and inhuman or degrading treatment or punishment.

Assurances in individual cases are the result of careful and detailed discussions, endorsed at a very high level of government, with countries with which we have working bilateral relationships. We may also put in place arrangements – often including monitoring by a local human rights body – to ensure that the assurances can be independently verified. The use of DWA has been consistently upheld by the domestic and European courts.

---

[18] A copy of the Independent Reviewer's subsequent report can be found at https://www.gov.uk/government/publications/citizenship-removal-resulting-in-statelessness

[19] Figures derived from internal Home Office information.

We asked the then Independent Reviewer of Terrorism Legislation, David Anderson QC, to review the legal framework of DWA and to examine whether the process can be improved, including by learning from the experiences of other countries. In July 2017 we published Mr Anderson's review[20]. Mr Anderson notes that the UK has taken the lead in developing rights-compliant procedures for DWA; that future DWA proceedings are likely to take less time now that the central legal principles have been established by the highest courts; that for as long as the UK remains party to the ECHR, the provisions of the ECHR will remain binding on the UK in international law; that the key consideration in developing safety on return processes is whether compliance with assurances can be objectively verified; and that assurances can be tailored to particular categories of deportee, or to particular outcomes.

We are considering Mr Anderson's comments and intend to respond via a Command Paper which will be laid in Parliament.

A total of 12 people have been removed from the UK under DWA arrangements.

5.11 - Proscription

Proscription is an important tool enabling the prosecution of individuals who are members or supporters of, or are affiliated with, a terrorist organisation. It can also support other disruptive powers including prosecution for wider offences, immigration powers such as exclusion, and terrorist asset freezing. The resources of a proscribed organisation are terrorist property and are therefore, liable to be seized.

Under the Terrorism Act 2000, the Home Secretary may proscribe an organisation if he believes it is concerned in terrorism. For the purposes of the Act, this means that the organisation:

- commits or participates in acts of terrorism;
- prepares for terrorism;
- promotes or encourages terrorism (including the unlawful glorification of terrorism); or
- is otherwise concerned in terrorism.

"Terrorism" as defined in the Act, means the use or threat of action which: involves serious violence against a person; involves serious damage to property; endangers a person's life (other than that of the person committing the act); creates a serious risk to the health or safety of the public or section of the public; or is designed seriously to interfere with or seriously to disrupt an electronic system. The use or threat of such action must be designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public and be undertaken for the purpose of advancing a political, religious, racial or ideological cause.

If the statutory test is met, there are other factors which the Home Secretary will take into account when deciding whether or not to exercise the discretion to proscribe. These discretionary factors include:

- the nature and scale of an organisation's activities;
- the specific threat that it poses to the UK;
- the specific threat that it poses to British nationals overseas;
- the extent of the organisation's presence in the UK; and

[20] https://www.gov.uk/government/publications/deportation-with-assurances

- the need to support other members of the international community in the global fight against terrorism.

Proscription under the Terrorism Act 2000 makes it a criminal offence to:

- belong, or profess to belong, to a proscribed organisation (section 11 of the Act);
- invite support for a proscribed organisation (and the support is not, or is not restricted to the provision of money or other property) (section 12 (1));
- arrange, manage or assist in arranging or managing a meeting in the knowledge that the meeting is to support or further the activities of a proscribed organisation, or is to be addressed by a person who belongs or professes to belong to a proscribed organisation (section 12 (2)); or to address a meeting if the purpose of the address is to encourage support for, or further the activities of, a proscribed organisation (section 12 (3)); or
- wear clothing or carry or display articles in public in such a way or in such circumstances as arouse reasonable suspicion that an individual is a member or supporter of the proscribed organisation (section 13).

The penalties for proscription offences under sections 11 and 12 are a maximum of 10 years in prison and/or a fine. The maximum penalty for a section 13 offence is six months in prison and/or a fine not exceeding £5,000.

Under the Terrorism Act 2000 a proscribed organisation, or any other person affected by a proscription, may submit a written application to the Home Secretary, asking that a determination be made whether a specified organisation should be removed from the list of proscribed organisations. The application must set out the grounds on which it is made. The precise requirements for an application are contained in the Proscribed Organisations (Applications for Deproscription etc) Regulations 2006 (SI 2006/2299).

The Home Secretary is required to determine the application within 90 days from the day after it is received. If the deproscription application is refused, the applicant may make an appeal to the Proscribed Organisations Appeals Commission (POAC). The Commission will allow an appeal if it considers that the decision to refuse deproscription was flawed, applying judicial review principles. Either party can seek leave to appeal the POAC's decision at the Court of Appeal.

If the Home Secretary agrees to deproscribe the organisation, or an appeal by the group concerned is successful, the Home Secretary will lay a draft order before Parliament removing the organisation from the list of proscribed organisations. The Order is subject to the affirmative resolution procedure so must be agreed by both Houses of Parliament.

Under the same legislation proscription decisions in relation to Northern Ireland are a matter for the Secretary of State for Northern Ireland, including deproscription applications for Northern Ireland groups.

Since 2000, the following three groups have been deproscribed;

- the Mujaheddin e Khalq (MeK) also known as the Peoples' Mujaheddin of Iran (PMOI) was removed from the list of proscribed groups in June 2008 as a result of judgments of the POAC and the Court of Appeal;
- the International Sikh Youth Federation (ISYF) was removed from the list of proscribed groups in March 2016 following receipt of an application to deproscribe the organisation; and

- Hezb-e Islami Gulbuddin (HIG) was removed from the list of proscribed groups in December 2017 following receipt of an application to deproscribe the organisation.

There are currently 74[21] terrorist organisations proscribed under the Terrorism Act 2000. In addition, there are 14 organisations in Northern Ireland that were proscribed under previous legislation. The Government laid an Order in September 2017 recognising Scottish Dawn and NS131 (National Socialist Anti-Capitalist Action) as alternative names for the organisation National Action, which was proscribed in December 2016.

The most recent proscription order came in to force in December 2017 which proscribed the following four groups:

- the al-Ashtar Brigades including its aliases Saraya al-Ashtar, the Wa'ad Allah Brigades, the Islamic Allah Brigades, the Imam al-Mahdi Brigades and the al-Haydariyah Brigades;
- the al-Mukhtar Brigades, including Saraya al-Mukhtar;
- Hasam, including Harakat Sawa'd Misr and Harakat Hasm; and
- Liwa al-Thawra.

Information about these groups' aims was given to Parliament at the time that they were proscribed. These details, for each proscribed international terrorist organisation, are included at **ANNEX A**.

5.12 - Closed Material Procedure

The Justice and Security Act 2013 introduced a statutory closed material procedure (CMP), which allows for sensitive material which would be damaging to national security to be examined in civil court proceedings.[22] CMPs ensure that government departments, the Security and Intelligence Agencies, law enforcement bodies and indeed any other party to proceedings have the opportunity to properly defend themselves or bring proceedings, in the civil court, where sensitive national security material is considered by the court to be involved. CMPs allow the courts to scrutinise matters that were previously not heard because disclosing the relevant material publicly would have damaged national security.

A declaration permitting closed material applications is an "in principle" decision made by the court about whether a CMP should be available in the relevant case. This decision is normally based on an application from a party to the proceedings, usually a Secretary of State. However, the court can also make a declaration of its own motion.

Where a Secretary of State makes the application, the court must first satisfy itself that the Secretary of State has considered making, or advising another person to make an application for public interest immunity in relation to the material. The court must also be satisfied that material would otherwise have to be disclosed which would damage national security, and that closed proceedings would be in the interests of the fair and effective administration of justice. Should the court be satisfied that the above criteria are met, then a declaration may be made.

[21] The actual number of proscribed organisations is lower than this figure as some groups appear on the list of proscribed organisations under more than one name, for example, 'Al Ghurabaa' and 'The Saved Sect' both refer to the group commonly known as 'Al Muhajiroun'.

[22] The Justice and Security Act is available at www.legislation.gov.uk/ukpga/2013/18/contents

During this part of proceedings a Special Advocate may be appointed to act in the interests of parties excluded from proceedings.

Once a declaration is made, the Act requires that the decision to proceed with a CMP is kept under review, and the CMP may be revoked by a judge at any stage of proceedings, if it is no longer in the interests of the fair and effective administration of justice.

A further hearing, following a declaration, determines which parts of the case should be dealt with in closed proceedings and which should be released into open proceedings. The test being considered here remains whether the disclosure of such material would damage national security.

The Justice and Security Act requires the Secretary of State to prepare (and lay before Parliament) a report on CMP applications and subsequent proceedings under section 6 of the Act. Under section 12(4) of the Act, the report must be prepared and laid before Parliament as soon as reasonably practicable after the end of the 12 month period to which the report relates. The first report covered the period 25 June 2013 (when the Act came into force) to 24 June 2014.[23] The most recent report, relating to the period 25 June 2016 to 24 June 2017, was published on 14 December 2017.[24]

In the latest reporting period from 2016 to 2017, there were 13 applications for a declaration that a CMP application may be made (eight of them by the Secretary of State, and five by persons other than the Secretary of State). There were 14 declarations that a CMP application may be made in proceedings during the reporting period (seven in response to applications made by the Secretary of State during the reporting period, four in response to applications made by the Secretary of State during previous reporting periods, two in response to applications made by persons other than the Secretary of State during previous reporting periods, and one on the court's own motion). Two applications were made during the reporting period by persons other than the Secretary of State to revoke a declaration, however none of the declarations were revoked during the reporting period.

There were five final judgments made during this period regarding the outcome of the application for a CMP. None were disclosed judgments.

5.13 – Tackling Online Terrorist Content

The open internet is a powerful tool which terrorists exploit to radicalise and recruit individuals, and to incite and provide information to enable terrorist attacks. Terrorist groups like Daesh make extensive use of the internet to spread their messages through a growing social media presence and compelling propaganda designed to reach a vast audience. Our objective is to make the online space a hostile environment for terrorists to operate and to prevent the dissemination of terrorist content online.

We are taking robust action to tackle radicalisation online, by securing the removal of terrorist-related content, by helping civil society to counter the extremists' poisonous ideology and by equipping people in communities with the ability to reject those narratives.

---

[23] https://www.gov.uk/government/publications/report-on-use-of-closed-material-procedure-june-2013-to-june-2014

[24] https://www.gov.uk/government/collections/use-of-closed-material-procedure-reports

Our dedicated police Counter Terrorism Internet Referral Unit (CTIRU) refers content that they assess as contravening UK terrorism legislation to communications service providers (CSPs). If CSPs agree that it breaches their terms and conditions they remove the content voluntarily. Since its inception in February 2010, the CTIRU has secured the removal of over 300,000 pieces of terrorist-related content. The Europol Internet Referral Unit replicates this model at European level and services all Member States.

We are working with industry to encourage them to take a more proactive role in tackling terrorist abuse of their platforms. This government was instrumental in getting the major industry players to set up the Global Internet Forum to Counter Terrorism (GIFCT), which was launched in June 2017 and is an international, industry-led forum to tackle terrorist use of the internet. We want to see the GIFCT leading the cross industry response to reduce the availability and spread of terrorist content on the internet, making it a hostile space for terrorists to operate. Ultimately, we want to get to a point where we are collectively preventing terrorist content from being made available to users in the first place.

We have encouraged CSPs to increase the use of technology to automate the detection and removal of content where possible. In February 2018, the Home Office announced the development of new technology in partnership with ASI Data Science which uses advanced machine learning to determine whether a video could be Daesh propaganda. We are talking to smaller companies who may benefit from implementing the tool.

Alongside our effort to squeeze the space terrorists and extremists operate online, we work with a range of civil society groups to counter extremist ideologies and to equip people in communities with the ability to reject those narratives.

5.14 – Tackling Online Child Sexual Exploitation

The Government is undertaking a significant programme of work to enhance the UK's response to online child sexual exploitation (CSE).

Collaborative working between Police forces and the NCA is resulting in around 450 arrests each month for online CSE offences, and the safeguarding of around 500 children each month. A Joint Operations Team, a collaborative venture between the NCA and GCHQ, is targeting the most sophisticated offenders. In addition, the Home Secretary recently announced an additional £20 million funding over three years has been provided to the Regional Organised Crime Units (ROCUs) to significantly increase the undercover online (UCOL) capability which is being used to target online grooming of children.

Internet users in the UK, including members of the public, who find illegal images of child sexual abuse are able to report them to the Internet Watch Foundation (IWF). The web pages containing such images can be blocked by Internet Service Providers (ISPs). The IWF is an independent organisation that acts as the UK hotline for the reporting of criminal content online. The purpose of the IWF is to minimise the availability of child sexual abuse images hosted anywhere in the world and non-photographic child sexual abuse images hosted in the UK.

The IWF has authority to hold and analyse this content through agreement with the Crown Prosecution Service and the Association of Chief Police Officers (ACPO) - now the National Police Chief's Council (NPCC). In 2016, the IWF recorded 102,932 webpages containing child sexual abuse material. If the site hosting the image is hosted in the UK, the IWF will pass the details to law enforcement (the Child Exploitation and Online Protection Command of the

National Crime Agency or local police forces) and the website host will be asked to take down the webpage.

If outside the UK, the IWF will alert the hotline in the relevant country to enable them to work with law enforcement in that country to take down the webpage. In countries where a hotline does not exist, this liaison is carried out via INTERPOL. Although the IWF is not part of Government, the Home Office maintains regular contact with the organisation, and Ministerial responsibility for policy relating to online child sexual exploitation. The responsibility for the legislation in respect of illegal indecent imagery of children and sexual contact with a child online sits with the Ministry of Justice.

The former Home Secretary announced UK investment in Project Arachnid, which is a collaboration between international hotlines that includes web-crawler technology developed by the Canadian Centre for Child Protection that is being deployed across websites, forums, chat services and newsgroups to detect known illegal content on the open web. Project Arachnid speeds up the time it takes to locate a known indecent image on the internet, without the need for human eyes. It also provides an Application Programming Interface (API) which allows companies who wish to make use of the tool to upload images suspected of being child abuse material to be checked against Arachnid's database of imagery or to be reviewed by analysts. It also enables companies who provide hosting to websites to check URLs against Arachnid's crawler. Companies have made approximately 34 million checks against the API, and Arachnid has analysed approximately one billion URLs and analysed approximately 42 billion images for child sexual abuse material. The Canadian Centre for Child Protection has partnered with the US National Center for Missing and Exploited Children to expand the pool of analysts and to reduce duplication between organisations as part of the Project.

The WePROTECT Global Alliance strategy, published in 2015, sets out the high level strategic goals of the initiative: to build national action with countries and to galvanise global action through high-level political engagement and work with the technology industry. To-date WePROTECT Global Alliance has focused on implementing its public strategy, to engage high-level decision makers and achieve action on the ground. Throughout 2017, key global players such as China and Saudi Arabia have signed up to the initiative, as well as the governments of the Gulf Cooperation Council and regional organisations such as the African Union, SAIEVAC, ASEAN and the Organisation of American States. All member governments have signed commitments to develop a comprehensive national response to tackle online child sexual exploitation. In July 2017, the first £10m of the UK's £40m ODA donation to the Fund to End Violence against Children was disbursed to 15 global capacity building projects. These projects will support the delivery of Model National Response capabilities in countries that are in need of support. In February 2018, WePROTECT Global Alliance published the Global Threat Assessment highlighting the growing dangers posed to children by the growth of smart phone technology and an expanding online community of tech offenders.

6 – Investigatory Powers

The use of a range of covert investigatory techniques is critical to law enforcement and the security and intelligence agencies' ability to counter the threats we face from terrorism, crime, and state-based threats. This chapter explains key investigatory powers and describes the safeguards that apply to their use.

6.1 – Investigatory Powers Act 2016

The current legislative framework which governs investigatory powers, including the interception of communications and the retention and acquisition of communications data, primarily consists of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016. These pieces of legislation ensure that these powers can only be used where it is necessary and proportionate to do so and for a specific set of purposes.

Following its consideration by both Houses of Parliament, the Investigatory Powers Act 2016 received Royal Assent on 29 November 2016.

The Investigatory Powers Act transforms the law relating to the use and oversight of investigatory powers, strengthening safeguards and introducing world-leading oversight arrangements. It does three things:

- First, it brings together powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It ensures that these powers – and the safeguards that apply to them – are clear and understandable.
- Second, the Act radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for the most intrusive powers, so that warrants cannot be issued by the Secretary of State until the decision to do so has been approved by a Judicial Commissioner who must hold or have held high judicial office (e.g. have been a High Court judge). And it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used.
- Third, it ensures powers are fit for the digital age. The Act makes provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications services to which a device has connected. This restores capabilities that have been lost as a result of changes in the way people communicate.

The data retention provisions in Part 4 of the Act have largely been commenced and oversight of the use of investigatory powers, and authorisation of police surveillance warrants and notices, has now transitioned to the Investigatory Powers Commissioner. A number of other provisions in the Investigatory Powers Act have also commenced, including the security and intelligence agencies and Ministry of Defence's ability to apply for interception and equipment interference warrants.

6.2 – Overview of Interception

Interception is the power to obtain a communication in the course of its transmission. Interception is currently provided for under the Regulation of Investigatory Powers Act (RIPA) 2000 and the Investigatory Powers Act 2016. Interception could additionally be authorised under the Wireless Telegraphy Act 2006, but the relevant provisions have been repealed and replaced by the Investigatory Powers Act 2016.

The use of interception, subject to strict controls and oversight, is a vital tool in the fight against terrorism, serious crime and other national security threats such as espionage. Terrorists increasingly use a range of communications services to radicalise, recruit and plan their attacks. Criminals use these services to commit crime and evade detection. The interception of the content of communications provides crucial intelligence on the plans and actions of terrorists and serious criminals, which allows law enforcement and the intelligence agencies to disrupt or frustrate them. As highlighted by David Anderson QC, the Independent Reviewer of Terrorism Legislation, "*interception can be of vital importance for intelligence, for disruption, and for the detection and investigation of crime*".[25] The majority of MI5's priority investigations rely on interception in some form to identify, understand or disrupt plots seeking to harm the UK and its citizens.

The ability to obtain an interception warrant is only available to nine agencies. These are: the Security Service (MI5), the Secret Intelligence Service (SIS), the Government Communications Headquarters (GCHQ), the National Crime Agency (NCA), the Metropolitan Police Service (MPS), the Police Service of Northern Ireland (PSNI), Police Scotland, HM Revenue and Customs (HMRC), and the Ministry of Defence (MoD).

The National Technical Assistance Centre (NTAC) provides technical assistance to law enforcement and the security and intelligence agencies in relation to interception. NTAC does not itself apply for interception warrants. Rather, it manages the delivery of intercepted communications to the agencies that have a lawful authorisation in place to acquire them.[26]

RIPA, the Investigatory Powers Act and the Interception of Communications Code of Practice, sets out a comprehensive legal framework, approved by Parliament, for the regulation of the interception of communications. RIPA provides that an interception warrant must be personally authorised by a Secretary of State or Scottish Minister (dependant on the organisation applying for the warrant this will usually be: the Foreign Secretary, the Home Secretary, the Defence Secretary, the Secretary of State for Northern Ireland, or the Cabinet Secretary for Justice for Scotland). Under the Investigatory Powers Act, the decision to issue a warrant must also be approved by a Judicial Commissioner. An interception warrant can only be authorised for limited and specified purposes, and only when the Secretary of State considers that it is both necessary and proportionate and the decision to issue the warrant must then be approved by a Judicial Commissioner.

There are two types of interception warrants provided for in Investigatory Powers Act: one authorises targeted interception, the other bulk interception.

---

[25] "A Question of Trust", June 2015, can be accessed at: https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

[26] Further information on NTAC's role is available at: https://www.gchq.gov.uk/features/national-technical-assistance-centre

Targeted interception, is primarily an investigative capability and relates to obtaining the content of communications of a particular individual, group of individuals or single set of premises. Bulk interception, is a strategic intelligence gathering capability and usually involves the process of collecting a large volume of communications followed by the selection for examination of specific communications where it is necessary and proportionate for a specific statutory purpose. Bulk interception warrants allow for the collection of communications of persons who are outside the UK in order to discover threats that could not otherwise be identified.

The use of interception is subject to independent oversight by the Investigatory Powers Commissioner. The Commissioner reports to the Prime Minister and his reports are published and laid before Parliament (see also Chapter 8.2). The Investigatory Powers Commissioner's Office started performing its oversight function from September 2017 so the latest annual report, covering 2016, was published by one of its predecessor organisations, the Interception of Communications Commissioner's Office, on 20 December 2017.

6.3 – Targeted Interception Warrants

Targeted interception warrants may be issued to intercept communications to, or from, a specified person (or persons), a group of persons or premises carried on any postal service or telecommunications system. A targeted interception warrant must name or describe either a person (or persons) as the interception subject, or a single set of premises to which the interception warrant relates.

An application for a targeted interception warrant under the Investigatory Powers Act will contain a consideration of necessity and proportionality, including:

- the statutory ground(s) on which the warrant sought is considered necessary;
- the background to the operation or investigation in the context of which the warrant is sought and what the operation or investigation is expected to deliver;
- where a warrant would relate to a particular person or organisation or to a single set of premises, a name or description of that person or organisation or those premises;
- where a warrant would relate to a group of persons who share a common purpose or who carry on (or may carry on) a particular activity, a description of that purpose or activity, and a name or description of as many of those persons as it is reasonably practicable to name or describe;
- where a warrant relates to more than one person or organisation or more than one set of premises for the purposes of a single investigation or operation, a description of the investigation or operation and a name or description of as many of those persons or organisations, or as many of those sets of premises as it is reasonably practicable to name or describe;
- Where a warrant relates to any testing or training activities, a description of those activities and a name or description of as many of the persons whose communications will or may be intercepted, or from whose communications secondary data will or may be obtained, as it is reasonably practicable to name or describe;

- where it is not reasonably practicable for a thematic warrant to name or describe persons, organisations or sets of premises, an explanation of why not; or, where the warrant describes persons, organisations or sets of premises using a general description, an explanation of why it was not practicable to name or describe persons, organisations or sets of premises individually;

- a description of the communications to be intercepted or the secondary data to be obtained, details of the telecommunications operator or postal operator, an assessment of the feasibility of the interception to the extent known at the time of the application and an outline of how obtaining the material will benefit the investigation or operation;

- a description of the conduct to be authorised or the conduct it is expected will be necessary to undertake in order to carry out what is authorised or required by the warrant. This conduct may include the interception of other communications not specifically identified by the warrant; it may also include conduct for obtaining secondary data from communications;

- consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including, whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;

- consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

- where the purpose or one of the purposes, of the warrant is to authorise or require the interception of items subject to legal privilege, a statement to that effect and explanation of why there are exceptional and compelling circumstances that make the interception of such items necessary and details of the arrangements for the handling, retention, use and destruction of such items;

- where the applicant considers it likely that items subject to legal privilege will be intercepted, a statement to that effect, an assessment of how likely it is that such items will be included in the communications, and details of the arrangements for the handling, retention, use and destruction of such items;

- where one of the purposes, of the warrant is to authorise or require the interception of communications that would otherwise be subject to legal privilege, the application should set out the reasons for believing that the communications will be or were made with the intention of furthering a criminal purpose;

- where the purpose of the warrant is to authorise or require the interception of the communications of a member of a relevant legislature (as defined in section 26) (see Chapter 9), a statement to that effect and details of the arrangements for the handling, retention, use and destruction of such items;

- where the purpose, or one of the purposes, of the warrant is to authorise or require the interception of communications which the applicant believes will contain confidential journalistic material or where the purpose, or one of the purposes of the warrant is to identify or confirm the source of journalistic information, a statement to that effect and details of the arrangements for the handling, retention, use and destruction of such items;

- where an application is urgent, the supporting justification;

- an assurance that all the material obtained under the warrant will be kept for no longer than necessary and handled in accordance with the safeguards required by sections 53 and 54 of the IP Act (see chapter 9).

6.4 – Bulk Interception Warrants

Bulk Interception warrants may be issued in respect of external communications. External communications are defined as those which are sent or received outside the British Islands. They include those that are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands in the course of their transmission, such as a domestic email that is transmitted via a server in another country.

Conduct authorised under a Bulk Interception warrant may sometimes result in the incidental interception of communications that were both sent and received in the British Islands; the Investigatory Powers Act permits this only if it is necessary to intercept the external communications that are the target of the warrant. In his 2016 Annual Report, the Interception of Communications Commissioner provided details of the interception warrants issued and the selection of material acquired under a bulk interception warrant.[27]

As with an application for a Targeted Interception warrant, an application for a Bulk Interception warrant must contain a consideration of necessity and proportionality. Specifically, this will include:

- background to the application;
- description of the communications to be intercepted and/or from which secondary data will be obtained, details of any telecommunications operator(s) who may be required to provide assistance and an assessment of the feasibility of the operation where this is relevant to the extent known at the time of the application;
- description of the conduct to be authorised, which must be restricted to the interception of overseas-related communications, the obtaining of secondary data from such communications, and the conduct (including the interception of other communications not specifically identified by the warrant it is necessary to undertake in order to carry out what is authorised or required by the warrant.
- the operational purposes for which the content and secondary data may be selected for examination and an explanation of why examination is or may be necessary for those operational purposes proposed in the warrant;
- consideration of whether intercepted content or secondary data obtained under the warrant (excluding intelligence reports) may be made available to any other security and intelligence agency or an international partner, where it is necessary and proportionate to do so;
- an explanation of why the conduct is considered to be necessary for one or more of the statutory purposes, which must always include an explanation of why the interception is necessary in the interests of national security;

[27] This report is available at: www.ipco.org.uk/publications

- a consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, explaining why what is sought to be achieved could not reasonably be achieved by other less intrusive means;
- an assurance that material obtained under a warrant will be selected for examination only so far as it is necessary for one or more of the operational purposes specified on the warrant and that it meets the conditions of section 152 of the Act (safeguards relating to examination of material); and
- an assurance that all content and data intercepted will be kept for no longer than necessary and handled in accordance with the safeguards required by the IP Act.

Interception Statistics

The Interception of Communications Commissioner published (and in future the Investigatory Powers Commissioner will publish) figures in relation to interception, including the total number of interception warrants authorised (see also Chapter 8.2). For 2016, this figure was 3,007. In 2015 it was 3,057, and in 2014, 2,795. The Commissioner's report also publishes the breakdown of the total number of warrants issued by statutory purpose. In 2016, 65% of warrants were issued for the purpose of the prevention and detection of serious crime presenting no change from 2015; 33% were issued in the interest of national security compared to 34% in 2015, and 2% were issued in relation to a combination of statutory purposes, up from 1% in 2015.

Warrants which were approved under the urgency procedure made up 2.2% of the total authorised for 2016. This means 67 warrants were approved in exceptionally urgent cases where, for example, there was an imminent, credible threat to national security, or a unique opportunity to obtain intelligence of vital importance in relation to preventing or detecting a serious crime.

The annual report of the Interception of Communications Commissioner for 2016 highlighted that the total number of extant interception warrants as at 31 December 2016 was 1,602, a 5.5% increase on 2015. Given that 3,007 warrants were authorised over the course of the year, this indicates that many interception warrants may be in place for no more than a matter of months. Of the 1,602 warrants that were extant at 31 December 2016, 13 were issued under section 8(4) of RIPA.

The Commissioner's 2016 annual report made available the number of warrants which were subject to challenge or further information requests by senior officials or the relevant Secretary of State prior to their being approved, or that were rejected by the Secretary of State. On 10 occasions further information was requested, and on five occasions a Secretary of State refused an application for an interception warrant. The Commissioner's report makes clear that these figures relate to a mixture of new warrant applications, and renewals, and hence should not be taken as a percentage of the 3,007 warrants issued in 2016. The publication of these figures is a step towards greater transparency, but does not represent the actual scale of the guardian and gatekeeper function provided in warrant granting departments such as the Home Office, or Foreign and Commonwealth Office. Teams of officials responsible for handling warrants provide day to day scrutiny at a series of levels of seniority, with many warrants daily being subject to requests for further clarification or adjustment. Some warrants are withdrawn by warrant requesting agencies following challenge, and before they reach a Secretary of State. Records of such exchanges exist on each file, but reliable statistics representing the scale of this activity in quantitative are not yet available.

6.5 – Targeted Communications Data

Communications data is information about who was communicating, when, from where, how and with whom; but not the content of a communication - i.e. what was said or written. For example, it can include the address to which a letter is sent; for mobile phones it might include, the time and duration of a phone call, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made; and for online communications, the internet protocol (IP) addresses identifying the individual who sent an email or posted a message on the internet, or the device that was used to make the communication.

Communications data is an essential tool for the full range of law enforcement activity and national security investigations. It enables the police, and other public authorities, to build a picture of the contacts and whereabouts of suspects and victims. Requests may be made for communications data in order to identify the location of a missing person or to establish a link (through call records) between a suspect and a victim. Communications data is used to investigate crime, keep children safe, support or disprove alibis and tie a suspect to a particular crime scene, among many other things. Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud. Communications data has played a role in every major Security Service counter-terrorism operation over the past decade. It can also be used in evidence and has been used in 95% of all serious organised crime prosecution cases handled by the Crown Prosecution Service.

The acquisition of communications data is stringently regulated, by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA ensures that communications data can be acquired from telecommunications or postal operators only by certain public authorities for specified statutory purposes. Applications for communications data must be authorised by a designated person in a relevant public authority, and can only be authorised where necessary and proportionate in relation to a specific investigation from which the designated person is independent. The relevant provisions in RIPA will be replaced by provisions in Part 3 of the Investigatory Powers Act in due course.

Beyond the powers which permit the acquisition of communications data, it is also necessary to be able to require telecommunications and postal operators to retain data that they would otherwise delete. The relevant provisions of the Data Retention and Investigatory Powers Act 2014 (DRIPA), which provided for the Secretary of State to give notices to telecommunications operators requiring the retention of communications data, have been repealed and replaced by provisions in Part 4 of the Investigatory Powers Act 2016, which came into force in December 2016.

The Investigatory Powers Commissioner took on statutory responsibility for the oversight of communications data powers in 2017. The Investigatory Powers Act requires the Information Commissioner to audit compliance by telecommunications operators and postal operators with respect to the security, integrity and deletion of retained data.

Currently, two codes of practice, both revised in March 2015, provide guidance on the procedures to be followed when acquiring, disclosing or retaining communications data under the legislation described here. The Acquisition and Disclosure of Communications Data Code of Practice is currently in force as a statutory code and sets out rules for the granting authorisations to acquire data, the giving of notices to require disclosure of data and the keeping or records, including records of errors.

The Retention of Communications Data Code of Practice ceased to have effect with the repeal of DRIPA but is used as guidance and covers: the issue, review, variation and revocation of data retention notices; the telecommunications operators' ability to recover their costs; data security; oversight by the Information Commissioner; and safeguards on the disclosure and use of retained data by telecommunications operators. A new draft statutory Code of Practice on communications data under the Investigatory Powers Act 2016 has been laid before Parliament.

Legislative changes being introduced to the Investigatory Powers Act 2016

On 21 December 2016 the Court of Justice of the European Union (CJEU) handed down the judgment in two cases, including a reference from the Court of Appeal relating to a challenge to the UK's then legislation governing data retention (DRIPA). The CJEU's judgment set out requirements that need to be in place for a data retention regime to be considered compliant with EU law. On 30 January 2018, the Court of Appeal handed down its judgment on the application of the CJEU judgment to DRIPA. The Court held, in accordance with a concession made by the Government following the CJEU ruling, that DRIPA was unlawful because it did not provide for independent authorisation of requests for access to communications data, and permitted access to communications data for the investigation of non-serious crimes.

On 27 April, the High Court handed down judgment in a challenge to the communications data regime in the Investigatory Powers Act. In a landmark judgment, the High Court agreed with the Government on every count. On the areas where the Government had already accepted that changes to the regime were needed to comply with the requirements of EU law, namely independent authorisation and a restriction to serious crime, the court agreed that it was not in the public interest to strike down the legislation with immediate effect and the court agreed with the Government that the practical arrangements could follow later.

In a detailed analysis, the Court also found that data retention regime is neither general nor indiscriminate, stating, "…we do not think it could possibly be said that the legislation requires, or even permits, a general and indiscriminate retention of communications data".

The Government intends to make amendments to the Investigatory Powers Act 2016 through regulations under section 2(2) of the European Communities Act 1972 to ensure our regime is consistent with EU law. Section 2(2) permits the Secretary of State to amend primary legislation by regulations to implement EU law obligations. The High Court judgment requires that legislative changes be made by 1 November 2018. In line with this timetable the Government laid the Regulations and code of practice in Parliament on 28 June for both Houses of Parliament to debate and vote on (via secondary legislation) in the Autumn.[28]

The draft Regulations will provide for an independent authorisation regime for most communications data requests. The Investigatory Powers Commissioner will have the power to authorise most communications data requests, through a new 'Office for Communications Data Authorisations' (OCDA) which will be under his control. The Regulations will also restrict the crime purpose for which certain data types can be retained and acquired to serious crime. We plan to make these legislative changes to Part 3 of the Investigatory Powers Act and then

[28] Information relating to the regulations can be found at https://www.gov.uk/government/consultations/investigatory-powers-act-2016

commence the whole of Part 3, to replace the relevant provisions in RIPA, as soon as OCDA is ready to begin authorising requests.

Communications Data Statistics

The Interception of Communications Commissioner's Office (and in future the Investigatory Powers Commissioner) will publish latest annual report covering 2016 contains extensive detail on the use of communications data by public authorities, as outlined below.

754,559 items of communications data were acquired by public authorities during 2016 under Chapter 2 of Part 1 of RIPA. An item of data is a request for data on a single communications address or other descriptor. For example, 30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data. Equally, a request for the details of a subscriber to a communications service would be counted as one item of data.

Communications data may be acquired in exceptionally urgent circumstances by virtue of an oral application and approval. It might be the case, for example that there is an immediate threat to life, or an urgent operational requirement, with little or no time to complete the normal written process. In 2016, 10% of data requirements were approved orally under these urgency provisions.

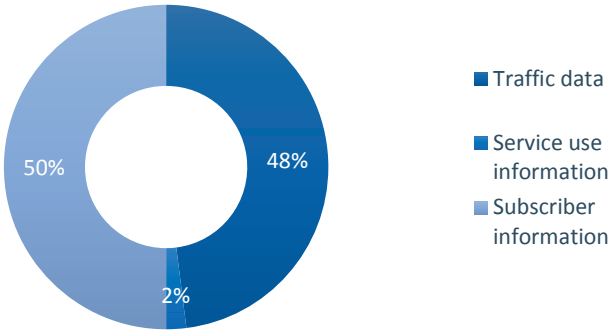
After the period of urgency, a written process must be completed, demonstrating the consideration given to the circumstances and the decisions taken. In addition, written notice must be given to the relevant communications service provider retrospectively within one working day, of the oral notice being given. Failure to do so constitutes an error, which must be recorded by the public authority that made the request.

The Commissioner's 2016 report includes details of the total number of items of communications data acquired, broken down in a number of ways. First, it includes a breakdown by data types acquired, in relation to the three data types at section 21(4) of RIPA. Traffic data, at section 21(4)(a), is data about a communication and the equipment used in transmitting it, such as information about the location of a mobile phone, or the IP address used to communicate over the internet. Service use data, at section 21(4)(b), is information about the use a person makes of a communications service and might include itemised telephone call records, or whether someone has diverted their telephone. Subscriber data, at section 21(4)(c), is information held by a communications service provider about people to whom they provide a service (such as their name, address and telephone number).

There are statutory restrictions on the categories of communications data that public authorities can access. For example local authorities cannot access traffic data.

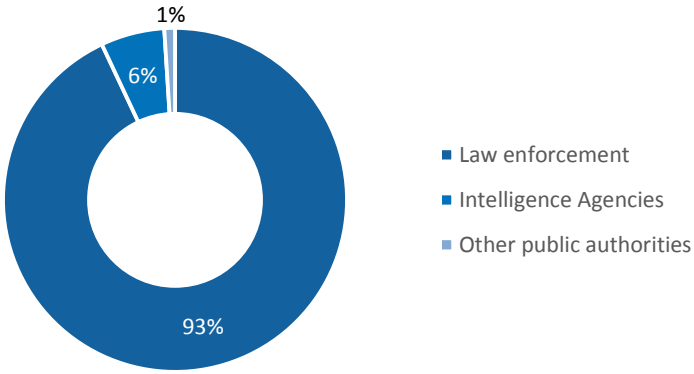
In 2016, 50% of communications data acquired was subscriber data; 48% was traffic data; and 2% was service use data. The majority of items of data acquired (81%) related to telephony identifiers, such as landline or mobile phone numbers; 15% related to internet identifiers, such as email addresses or IP addresses; 2% related to postal identifiers, such as postal addresses; and the remaining 2% related to "other" identifiers, such as bank account or credit card numbers.

Figure 1: Communications data acquired by data type, 2016



The Commissioner's report also breaks down the total number of items of data acquired, except those granted on an urgent oral basis, by the type of public authority requesting the data. This shows that the large majority of communications data requests made in 2016 were from the police and law enforcement agencies, comprising 93% of total communications data acquired. The security and intelligence agencies accounted for 6% of the total, and 1% was acquired other public authorities.

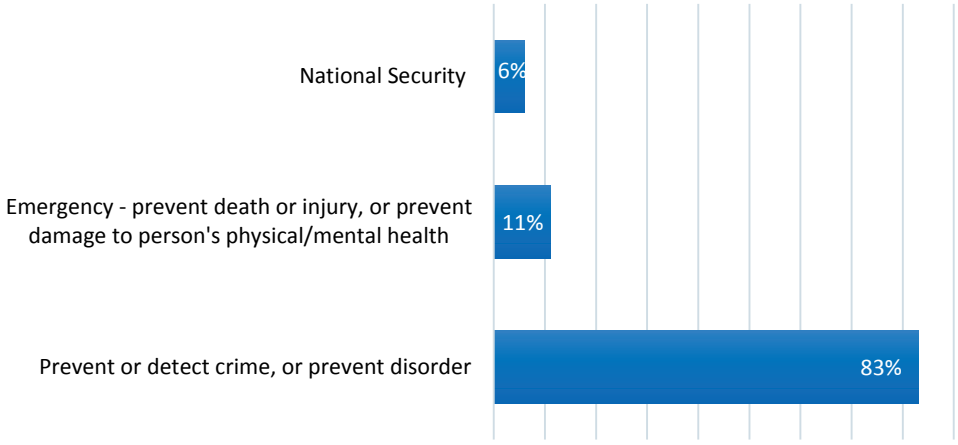
Figure 2: Communications data acquired by data type, 2016



The report also breaks this category down further, and includes the total number items of data approved by each public authority. The full list is included at **ANNEX B.**

The Commissioner's report also breaks down the total number of items of data by the statutory purpose for which it was acquired. During 2016, the prevention and detection of crime or prevention of disorder (section 22(2)(b) of RIPA) was the statutory purpose for which communications data was most often acquired, accounting for 83% of communications data acquired. The next most common statutory purposes were preventing death or injury in an emergency situation (11%) (section 22(2)(g) of RIPA) and national security (6%).

Figure 3: Communications data acquired by data type, 2016



Public authorities are required to record, for each item of data, whether that item relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation.

The Commissioner's report showed that during 2016, 71% of applications to acquire communications data related to criminal suspects or persons of interest for national security purposes. 15% of requests related to people who were not suspected of any nefarious activity, for example where data was requested to identify witnesses or locate vulnerable people.

6.6 – Bulk Communications Data Acquisition

The security and intelligence agencies use a range of techniques under existing legislation to acquire information in volume. This information, sometimes referred to as 'bulk data', is used to generate intelligence about threats that cannot be acquired by more targeted means.

Section 94 of the Telecommunications Act 1984 ('section 94') provides a power for the Secretary of State to issue directions 'of a general character' to telecommunications operators in the interests of national security or relations with the government of a country or territory outside the United Kingdom. Directions given under this power enable the agencies to obtain communications data in bulk from telecommunications operators, where the Secretary of State considers that such a direction is necessary and proportionate to what is sought to be achieved.

The use of this power to provide for bulk communications data acquisition was avowed in November 2015, when in the interests of transparency the then Home Secretary, the Rt. Hon. Theresa May MP, set out its existence in a statement in the House of Commons.

Alongside this avowal, and in the absence of a provision to publish a code of practice relating to the exercise or performance and duties under section 94 directions, the security and intelligence agencies published their joint Arrangements for the Acquisition of Bulk Communications Data Pursuant to Directions under section 94 of the Telecommunications Act 1984.

The security and intelligence agencies conduct internal six-monthly reviews of directions issued under section 94 to acquire communications data in bulk in order to assess whether the reasons and justifications for the directions remain valid. Conclusions are submitted to the Secretary of

State, and the operators are also informed of their obligations to continue to comply with section 94 directions.

And when a section 94 direction to disclose bulk communications data is no longer required, the agency informs both the Secretary of State and the relevant telecommunications operator. Where there is a requirement to modify or cease a section 94 direction, a submission is sent to the Secretary of State setting out the justification for the change and the agency consults with the telecommunications operator in the same way as it would with a new section 94 direction.

Copies of directions given in relation to bulk communications data acquisition have not been laid before Parliament as the Secretary of State considers it is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person to do so.

The Investigatory Powers Act (IPA) will replace section 94 (in so far as it is used to obtain communications data in bulk) with a clear, transparent power to issue warrants for the acquisition of communications data in bulk, subject to enhanced safeguards. The enhanced safeguards for this power include a 'double lock', so that a Judicial Commissioner must approve the Secretary of State's decision to issue a warrant before it can be issued, and the introduction of 'operational purposes' governing the circumstances in which data can be selected for examination.

Fast, secure access to communications data is essential to the agencies in pursuing their investigations. The ability to acquire and access this data in bulk, subject to strict safeguards and oversight, is vital to the security and intelligence agencies' effectiveness, providing unique intelligence that cannot be obtained by other means. In some cases bulk communications data may be the only investigative lead that the security and intelligence agencies have to work with.

It is clear that these capabilities have helped to protect the UK. The analysis of bulk data, for example, has:

- played an important part in every major counter terrorism investigation of the last decade, including in each of the 22 plots thwarted in the last four years;
- enabled over 90% of the UK's targeted military operations during the campaign in the south of Afghanistan;
- was essential in identifying 95% of the cyber-attacks on people and businesses in the UK discovered by the agencies in the latter part of 2016; and
- been used to identify serious criminals seeking to evade detection online, and who cannot be pursued by conventional means, supporting the disruption of over 50 paedophiles in the UK in the last three years.

Bulk communications data acquisition capabilities were first used at scale in the UK in 2001 after the 9/11 attacks in New York, and later extended following the attacks on the London transport system on 7 July 2005 to respond to the domestic terrorist threat. They are regularly used alongside other capabilities to investigate known, high-priority threats and to identify emerging threats from individuals not previously known to the security and intelligence agencies.

Bulk communications data is therefore among the most important tools that the security and intelligence agencies can use to obtain intelligence on subjects of interest, and whilst the security and intelligence agencies can also make individual communications data requests to communication service providers under RIPA (and Part 3 of the IPA when these provisions are

commenced), the ability to access data in bulk is critical, because it enables the agencies to conduct searches, where necessary and proportionate, across all the relevant data, in a secure way. This enables more complex analysis to be undertaken, particularly when the results are matched against other data holdings, and where there is very limited lead intelligence, or when communications have been deliberately concealed. By using bulk communications data, links can be established that would be impossible or significantly slower (potentially taking many days) to discover through a series of individual requests to communication service providers. This can sometimes be the difference between identifying and disrupting a plot, and an attack taking place. This crucial investigative tool also allows the agencies to reduce the risk of an incomplete intelligence picture which makes it difficult to assess the entirety of a threat posed by a known subject – a point made forcefully in the report by the Intelligence and Security Committee of Parliament into the murder of Fusilier Lee Rigby in 2013.

Prior to 8 September 2017, oversight of these powers was conducted by the Interception of Communications Commissioner. From that date, oversight responsibilities passed to the Investigatory Powers Commissioner.

Bulk Communications Data Acquisition Statistics

Section 94 does not provide for any requirement for record keeping in relation to directions given under this power or the use of any communications data acquired in bulk under such directions. When he commenced oversight of directions given under this power in early 2015, the Interception of Communications Commissioner instigated record-keeping requirements. The IPA will introduce record-keeping requirements in line with those currently in place for the targeted acquisition of communications data under RIPA.

The Interception of Communications Commissioner's July 2016 report of his review of directions given under section 94 includes those statistics currently available on the acquisition of communications data in bulk by the agencies, as outlined below.

At the time the review took place, there were fifteen extant section 94 directions relating to the acquisition of bulk communications data. A number of the directions have been modified over the years, for example, to expand or to cease the acquisition of certain data, and this has led in some instances to the direction being re-issued.

Only GCHQ and the Security Service use section 94 directions to acquire bulk communications data. In 2015, GCHQ identified 141, 251 communications addresses or identifiers of interest from communications data acquired in bulk pursuant to section 94 directions which directly contributed to an intelligence report.

In 2015, the Security Service made 20,042 applications to access communications data obtained pursuant to section 94 directions. These applications related to 122,579 items of communications data. The Commissioner concluded that overall the Security Service applications examined were submitted to an excellent standard and satisfied the principles of necessity and proportionality.

All of the extant requirements for bulk communications data are for traffic data as defined in section 21(4)(a) of RIPA. All of the current directions require regular feeds of bulk communications data to be disclosed by the relevant telecommunications operator.

One operator had historically been required (since 2001) to supply subscriber information to GCHQ in addition to traffic data as part of a section 94 direction. This requirement ceased in August 2015 after an internal review and the subscriber information obtained was destroyed.

The agency handling arrangements for the acquisition of bulk communications data published in November 2015 state clearly that:

"*The communications data collected is limited to "Traffic Data" and "Service Use Information…The data provided does not contain communication content or Subscriber Information*…"

All of the section 94 directions specified that they were necessary under section 94(1) of the Telecommunications Act 1984 "*in the interests of national security*". None of the section 94 directions specified that they were necessary for "*relations with the government of a country or territory outside the United Kingdom*".

6.7 – Covert Surveillance, Covert Human Intelligence Sources and Property Interference

The use of a range of covert techniques is an important weapon in the fight against terrorism and crime, including serious or organised crimes such as the trafficking of drugs and firearms, and child abuse. Covert surveillance (both intrusive and directed surveillance) and the use of covert human intelligence sources are regulated by Part II of the Regulation of Investigatory Powers Act 2000 (RIPA). Additionally, the Police Act 1997[29], and the Intelligence Services Act 1994[30], provide for property interference to be undertaken by the law enforcement and security and intelligence agencies, where necessary and proportionate, in accordance with the strict criteria set out in those Acts.

The use of all of these powers is subject to rigorous independent oversight. Since September 2017 that oversight has been provided by the Investigatory Powers Commissioner (IPC) (see section 7.2). Prior to that the exercise of the powers by the security and intelligence agencies and the Ministry of Defence was overseen by the Intelligence Services Commissioner (see also section 7.3), and their use by the police and other public authorities was overseen by the Office of Surveillance Commissioners (see also section 7.4).

Intrusive Surveillance

Intrusive surveillance is surveillance which takes place inside residential premises or private vehicles, whether by human or technical means. The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained.

Only a limited number of public authorities are able to undertake this type of surveillance and its use is robustly safeguarded. Intrusive surveillance can only be conducted in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interest of the economic well-being of the UK.

When consideration is being given to the authorisation of intrusive surveillance, there must be a consideration as to whether the information sought could reasonably be acquired by other means. Any application by the security and intelligence agencies, the Ministry of Defence and

[29] The Police Act 1997 is available at www.legislation.gov.uk/ukpga/1997/50/contents

[30] The Intelligence Services Act 1994 is available at www.legislation.gov.uk/ukpga/1994/13/contents

HM Armed Forces requires authorisation by the Secretary of State. Applications by the police and other public authorities are authorised internally at Chief Constable or equivalent level. However, these applications additionally require the prior approval of an independent Judicial Commissioner.

Directed Surveillance

Directed surveillance is covert surveillance conducted at any location (including online), other than within residential premises or private vehicles, that is likely to result in the obtaining of private information about a person. A wider group of public authorities, including local authorities, can undertake this form of surveillance. Authorisation is obtained from a senior designated person within the organisation and can only be granted where necessary and proportionate, for a specific statutory purpose, and in relation to an individual investigation.

Local authorities in England, Wales and Northern Ireland[31] must also obtain judicial approval for the use of directed surveillance, under measures introduced by Protection of Freedoms Act 2012[32]. In addition to seeking judicial authorisation, local authorities in England and Wales may only make use of directed surveillance in relation to the investigation of criminal offences which attract at least a six month sentence, or in relation to offences relating to the sale of alcohol or tobacco to children.

Covert Human Intelligence Sources

A covert human intelligence source (CHIS) is anyone who is asked by a public authority to start or maintain a relationship for a covert purpose. This includes undercover officers employed by the public authority, or members of the public acting as informants. Provisions in RIPA ensure that the use of a CHIS may only be authorised at a suitably senior level where necessary and proportionate for a statutory purpose approved by Parliament. Local authorities must also obtain judicial approval for use of a CHIS. In addition, section 29(4) of RIPA sets out further safeguards regarding the use of a CHIS, including the requirement that a qualifying person in the relevant public authority must have day-to-day responsibility for dealing with the CHIS, and for the CHIS's security and welfare.

The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 increased the authorisation levels required before an undercover officer can be deployed and enhanced oversight by the Office of Surveillance Commissioners (now transferred to the IPC). Specifically, any deployment of an undercover law enforcement officer must be authorised by an Assistant Chief Constable, or equivalent, and notified to the Investigatory Powers Commissioner. Any deployment which lasts more than 12 months must be authorised directly by the Chief Constable, or equivalent, and must be approved by a Judicial Commissioner. This same level of authorisation and approval must be obtained for any authorisation lasting more than three months where the authorisation involves matters subject to legal privilege.

[31] In Northern Ireland this requirement only applies to authorisations where the grant or renewal relates to a Northern Ireland excepted or reserved matter. Where such an authorisation is required by a local authority in Northern Ireland, an application for a grant or renewal should be made to a district judge.

[32] The Protection of Freedoms Act is available at www.legislation.gov.uk/ukpga/2012/9/contents

Property Interference

Property interference may be authorised for law enforcement agencies with an authorisation issued under Part III of the Police Act 1997. This allows them to enter or interfere with property, or wireless telegraphy, for the purpose of preventing or detecting serious crime. Similar powers are available to the security and intelligence agencies under section 5 of the Intelligence Services Act 1994.

Property interference is subject to a stringent authorisation regime, ensuring it can only be used where it is necessary and proportionate and where the desired outcome cannot be achieved by other means. In the case of law enforcement agencies, an authorisation can only be obtained from a Chief Constable, or equivalent. Where a member of a law enforcement agency authorises property interference, he or she must, as soon as reasonably practical, inform a Judicial Commissioner. In addition, prior approval for a property interference authorisation must be sought from a Judicial Commissioner where the property in question is used wholly or mainly as a dwelling or is a hotel bedroom or office premises. Approval by a Judicial Commissioner is also required where the interference might involve acquiring knowledge of matters subject to legal privilege, journalistic material or confidential personal information.

The security and intelligence agencies require a warrant signed by the Secretary of State to conduct property interference. The Secretary of State may only authorise a warrant where he or she is satisfied that it is necessary and proportionate, and he or she must also consider whether the relevant information could be reasonably obtained by other means. In many cases, an operation using covert techniques may involve both directed or intrusive surveillance and property interference, such as where a covert device needs to be placed inside a residential property for the purpose of conducting intrusive surveillance. This can be authorised as a combined authorisation, although the specific criteria for authorisation of each activity must be considered separately.

Under the Investigatory Powers Act 2016, interference with equipment such as computers and mobile devices previously authorised under property interference powers, will be authorised by an equipment interference warrant where it is carried out for the purpose of acquiring communications, information or equipment data with a British Islands connection, and if a Computer Misuse Act offence would otherwise be committed. Further information about these powers is provided at Section 6.8 below. Interference with equipment that is not for the purpose of obtaining communications, information or equipment data, e.g. where the purpose of the interference is to disable the equipment, will continue to fall under existing property interference powers. Interference with other forms of property and with wireless telegraphy will not be affected by this change and continue to be authorised under the existing property interference powers.

Codes of Practice

The Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice provide guidance to public authorities on the use of these powers. The Codes are issued under section 71 of RIPA and public authorities are required under the Act to have regard to the Codes. Both Codes were updated in 2014 to reflect, among other things, the enhanced authorisation procedures for law enforcement agencies' use of CHIS, and for local authorities' use of directed surveillance and CHIS.

The codes are now being revised to reflect the changes introduced by the Investigatory Powers Act 2016. At the same time some further minor updates and clarifications will be made to ensure that public authorities apply best practice in the use of the powers. For example they will provide expanded guidance on the use of surveillance and CHIS powers in online investigations, and include amendments intended to reinforce the protection of those acting as CHIS. Draft revised codes were published in November 2017 for a period of public consultation, which closed on 28 December 2017. A response to the consultation was published on 13 June 2018, when these revised codes were laid before Parliament.

Since 2014, the CHIS Code has stipulated that all police officers in England and Wales must comply with and uphold the principles and standards of professional behaviour set out in the College of Policing Code of Ethics, introduced in July 2014.

The Code of Ethics states clearly that covert tactics must be appropriately authorised and any deployments must be shown to be proportionate, lawful, accountable, necessary and ethical. The Code of Ethics also states that officers must not establish or pursue an improper sexual or emotional relationship with a person with whom they come into contact in the course of their work who may be vulnerable to an abuse of trust or power.

Statistics for covert techniques

Security and Intelligence Agencies

The annual report of the Intelligence Services Commissioner included statistics on the total number of warrants and authorisations approved for the security and intelligence agencies and Ministry of Defence (see also Section 7.3).

At the end of 2016, the total number of extant warrants and authorisations was 1,926.

Law Enforcement Agencies and Other Public Authorities

The annual report of the Chief Surveillance Commissioner included statistics on the use of intrusive surveillance, directed surveillance, CHIS and property interference by law enforcement agencies and other public authorities (see also Section 7.4). The Commissioner's latest report covered the period 1 April 2016 to 31 March 2017. It advised that there were 237 authorisations for intrusive surveillance, compared to 289 in the previous period. None were quashed by Commissioners during the year.

Law enforcement agencies authorised the use of directed surveillance on 6,237 occasions, with 2,299 extant at the end of March 2017. These figures were lower than in the previous reporting period, where the Commissioner reported that 7,118 authorisations were given, with 1,057 extant at the end of the year. The total number of authorisations for directed surveillance by other public authorities was 1,887, a small reduction from 2,029 the previous year. These figures fit into a continuing downward trend of the use of directed surveillance by these authorities. The Department for Work and Pensions (DWP) continues to account for the majority of authorisations within this category. The number of directed surveillance authorisations given by the DWP during this reporting period decreased slightly from 1,258 to 1,203.

During the reporting period, 2,310 CHIS were authorised by law enforcement agencies and as at 31 March 2017, there remained 2,299 authorised, including some which may have been

authorised in preceding years. Over the course of the year, 2,184 CHIS authorisations were cancelled. In addition to this, 1,158 “relevant sources” (better known as undercover officers) were notified to the Office of Surveillance Commissioners, 1,032 were cancelled and 93 were submitted for the prior approval renewal process.[33] At the end of the reporting period, there were 76 active CHIS in other public authorities. Only a very small proportion of these public authorities (6.6%) used CHIS during the year. This will often be for matters such as trading standards investigations. During the reporting period, and excluding renewals, property interference authorisations were granted on 1,842 occasions. This was a decrease of 228 on the previous year. Three of these authorisations were quashed by Commissioners.

Figure 6: Summary of key activity in relation to the use of covert techniques in the year ending 31 March 2017

	Intrusive surveillance authorisation	Property interference authorisation	Relevant sources notified	Directed surveillance authorisation	Authorised CHIS at 31/03/2017
Law Enforcement	237	1842	1158	6237	2299
Other Public Authorities				1887	76

6.8 – Equipment Interference

Equipment interference authorisations will allow the security and intelligence agencies, law enforcement agencies and the armed forces to interfere with electronic equipment such as computers and smartphones in order to obtain data, such as communications, from a device. Equipment interference encompasses a wide range of activity from remote access to computers, to downloading covertly the contents of a mobile phone during a search.

Where necessary and proportionate, law enforcement agencies and the security and intelligence agencies need to be able to access communications or other information held on devices, in order to gain valuable intelligence in national security and serious crime investigations and to help gather evidence for use in criminal prosecutions. The armed forces will use equipment interference with the support of the security and intelligence agencies in some situations to gather data in support of military operations.

The use of equipment interference to obtain this data will play an important role in mitigating the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption and attempts to evade detection. It may sometimes be the only method by which to acquire the data.

Equipment interference will be used by law enforcement agencies, defence intelligence and the security and intelligence agencies; more sensitive and complex techniques are generally only

[33] These figures represent the number of times a single individual undercover officer has been authorised for deployment on a specific police operation. As such, the total number of authorisations does not reflect the number of undercover operations undertaken during the year.

used by the security and intelligence agencies and a small number of law enforcement agencies, including the National Crime Agency.

Equipment interference powers under the Investigatory Powers Act are yet to come into force for law enforcement agencies, but have been commenced for the security and intelligence agencies and Ministry of Defence. Until these powers are commenced, equipment interference by law enforcement agencies is authorised under general property interference powers in the Police Act 1997.

The use of equipment interference by the security and intelligence agencies is governed by a new Equipment Interference Code of Practice under the Investigatory Powers Act which was approved by Parliament and which will govern the use of this power for law enforcement agencies upon commencement. The approved Code of Practice has been published and is available on the Gov.uk website.

Building on recommendations made by David Anderson QC (the former Independent reviewer of terrorism legislation from his June 2015 report "A Question of Trust", and August 2016 report "Bulk Powers Review"), and the Intelligence and Security Committee of Parliament's report on the draft Investigatory Powers Bill in February 2016, the Investigatory Powers Act 2016 provides for an explicit, more transparent equipment interference regime that will govern the use of these techniques by law enforcement agencies, the security and intelligence agencies and the armed forces, introducing new, enhanced safeguards. The use of this power will be limited to the same statutory purposes as interception (these being for the purpose of preventing or detecting serious crime, in the interests of national security and in the interests of the economic well-being of the UK). Law enforcement agencies' use of equipment interference will also be permitted for the prevention and detection of serious crime and preventing death or preventing or mitigating any injury or damage to a person's physical or mental health.

Prior to the Investigatory Powers Act, use of these powers by the security and intelligence agencies required authorisation by the Secretary of State which continues under the Investigatory Powers Act. Under the Act, authorisations for law enforcement agencies may be issued by the relevant law enforcement chief, typically a Chief Constable. The Act also strengthens authorisation safeguards so that the decision to issue a warrant will also be subject to approval by a Judicial Commissioner.

In his final report (published in 2017 and prior to the Investigatory Powers Commissioner taking over), the Intelligence Services Commissioner, set out that he believes that changes brought about by the 2016 Act will provide greater clarity that the agencies are proactively engaging with recommendations made in the past and that steps are being taken to improve compliance with the Code of Practice (Equipment Interference Code under RIPA) which only applies to the security and intelligence agencies. The Commissioner reports that in general, he is satisfied that necessity and proportionality considerations are carefully considered, and that the case for intrusion into privacy is made clear to the person carrying out the authorisation, in relation to equipment interference authorisations. The Intelligence Service Commissioner reports that following the agencies' explanation of their internal processes for identifying and handling confidential material, he is satisfied that this material is being handled appropriately and in accordance with the Code of Practice in place at the time.[34] Going forward, The Investigatory Powers Commissioner will oversee the use of equipment interference powers by law enforcement, the security and intelligence agencies, and the armed forces under the Investigatory Powers Act 2016, following implementation.

[34] The report can be found in full at www.ipco.org.uk/publications

6.9 – Investigation of Protected Electronic Information

The ability to investigate electronic information protected by encryption is an important tool for the security and intelligence and law enforcement agencies. Information security technologies, from the use of passwords to advanced cryptography, enable businesses and individuals to protect their electronic data when going about their lawful business. However, terrorists and criminals use the same technologies in order to conceal their conduct and to evade detection.

Part III of Regulation of Investigatory Powers Act 2000 (RIPA) enables a notice to be served on a holder of protected electronic information requiring them to put that information into an intelligible form, where the information has been lawfully obtained by a public authority. This may include, for example, requiring a suspect in a criminal investigation to provide the password to their mobile phone when it has been seized by the police. The use of this power does not mitigate the increased use of end-to-end encrypted services, as this power requires the assistance of the holder of the protected electronic information.

The use of these powers is subject to stringent safeguards. Permission to require that protected information is put into an intelligible form may only be granted where necessary and proportionate. These powers can only be exercised:

- in the interests of national security;
- to prevent or detect crime;
- in the interests of the economic well-being of the UK; or
- where necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty.

In addition, these powers must not be used where it is reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice.

Schedule 2 of RIPA sets out additional safeguards relating to the giving of a notice. A person may only serve a notice in relation to protected information if they have been granted permission by a relevant authority in accordance with Schedule 2.

The National Technical Assistance Centre (NTAC) is the lead national authority for matters relating to the processing of protected information into an intelligible form and to disclosure of key material. NTAC provides technical support to public authorities, particularly law enforcement agencies and the security and intelligence agencies, including a facility for the processing of lawfully obtained protected electronic information.

The Code of Practice issued under RIPA, sets out that no public authority may serve any notice, or when the authority considers it necessary, seek to obtain appropriate permission without the prior written advice of NTAC or another appropriate public body, either in relation to an individual case or category of cases. The Codes are now being revised to reflect the changes introduced by the Investigatory Powers Act 2016. At the same time some minor amendments were made, including:

- a change to the role of NTAC from an “approval” to an “advisory” role;
- providing that NTAC may give advice in relation to a particular Part III notice or a category of case types, in order to simplify the application procedure for public authorities in certain circumstances;
- A provision to permit a possible future transfer of NTAC’s role to another appropriate public body.

Draft revised codes were published in November 2017 for a period of public consultation, which closed on 28 December 2017. A response to the consultation was published on 13 June 2018, when these revised codes were laid before Parliament.

Where protected information has been, or is likely to be, obtained under a warrant issued by a person holding judicial office, public authorities may obtain appropriate permission from such a person holding judicial office. Such permission might be granted, for example, in relation to a production order obtained under the Police and Criminal Evidence Act 1984.

Where protected information is likely to be, or has been, obtained under a warrant issued by the Secretary of State, for example an interception warrant, appropriate permission for giving a notice in respect of that information may be obtained from the Secretary of State.

Where protected information is likely to be, or has been, obtained through an authorisation under Part III of the Police Act 1997 (authorisation of otherwise unlawful action in respect of property) appropriate permission for giving a notice may be obtained from an authorising officer within the meaning of that Act.

The Police, National Crime Agency, HMRC and members of HM forces have appropriate permission, without a requirement to seek permission from a judicial authority or Secretary of State, in relation to protected information in certain circumstances. This is the case where that information is likely to be, or has been, obtained by the exercise of a statutory power and is not information obtained under a warrant issued by the Secretary of State or a person holding judicial office, or an authorisation under Part III of the Police Act 1997, or information obtained by the intelligence agencies. For example, this could be in relation to information obtained under section 19 of the Police and Criminal Evidence Act 1984, which relates to a constable's general powers of seizure.

Once appropriate permission has been granted, a notice can be given, imposing a disclosure requirement. The effect of imposing a disclosure requirement is that the recipient shall be required, in accordance with the notice, to provide for the protected information in his or her possession to be put into an intelligible form. RIPA makes it an offence if the recipient knowingly fails, in accordance with the notice, to make the required disclosure, and if the recipient fails to keep the existence of such a notice secret.

Statistics on the investigation of protected electronic information

The annual report of the Chief Surveillance Commissioner includes details of the number of investigations into protected electronic information. The Commissioner's latest report covers the period from 1 April 2016 to 31 March 2017. The report outlines that during the reporting period, NTAC granted 159 approvals, out of 166 applications, to investigate electronic data protected by encryption.

6.10 – Bulk Personal Datasets

Bulk Personal Datasets (BPDs) are sets of personal information held by the security and intelligence agencies about a large number of individuals, the majority of whom will not be of any intelligence interest. The datasets are held on the agencies' electronic systems for the purposes of analysis.

BPDs are essential in helping the security and intelligence agencies identify subjects of interest or individuals who surface during the course of an investigation, to establish links between individuals and groups, to understand better a subject of interest's behaviour and connections and quickly to exclude the innocent. In short, they enable the agencies to join the dots in an investigation and to focus their attention on individuals or organisations that threaten our national security.

Regulation and Oversight

The security and intelligence agencies have powers under the Security Service Act 1989 and the Intelligence Services Act 1994 to acquire and use BPDs to help them fulfil their statutory functions, including protecting national security. BPDs may be acquired using investigatory powers, from other public sector bodies or commercially from the private sector. The use of BPD is subject to stringent internal handling arrangements and the regime is overseen by the Investigatory Powers Commissioner.

In his 2016 final annual oversight report, the Intelligence Services Commissioner, the Rt Hon Sir Mark Waller, recommended the agencies work proactively to prepare for the requirements under the Investigatory Powers Act, to ensure procedures are tried and tested before implementation. His assessment from his reviews of each agency's BPD holdings was that they each had safeguards in place, and he was confident in their record of use, and that paperwork contained good considerations of necessity and proportionality, although he would have liked a clearer demonstration of privacy considerations in some cases.

Of the concerns the Commissioner had identified in his 2015 annual report, he reported in 2016 that these had or were being addressed, and he was satisfied.

The Investigatory Powers Act 2016 will enhance the safeguards that apply to the retention and examination of BPDs acquired under the Security Service Act 1989 and the Intelligence Services Act 1994. The Secretary of State will have to approve warrants for the retention and examination of BPDs, if it is necessary and proportionate to do so. As is the case for interception and equipment interference authorisations, a Judicial Commissioner must also approve the decision to issue a warrant (following commencement for the security and intelligence agencies and Ministry of Defence).

7 – Oversight

7.1 – The Independent Reviewer of Terrorism Legislation

The current Independent Reviewer of Terrorism Legislation (IRTL), Max Hill QC, took up his appointment on 1 March 2017. Mr Hill took over from David Anderson QC, who was IRTL from 2011 to 2017. The IRTL is appointed by the Home Secretary through open competition in accordance with the Government Code on Public Appointments.

The role of the IRTL is to keep under review the operation of a range of UK counter-terrorism legislation to ensure that it is effective, fair and proportionate. This helps to inform public and political debate and provides independent and ongoing oversight of UK terrorism legislation as the legislative landscape and the threat from terrorism changes.

The IRTL is required by section 36 of the Terrorism Act 2000 (TACT) to report annually on the operation of the Act. He has discretion to set his work programme and can also review the following Acts depending on where he feels he should focus his attention:

- Part 1 of the Terrorism Act 2006;
- The Terrorism Prevention and Investigation Measures Act 2011;
- The Terrorist Asset-Freezing Act 2010;
- The Anti-Terrorism Crime and Security Act 2001;
- The Counter-Terrorism Act 2008 and;
- The Counter-Terrorism and Security Act 2015.

The annual review on the operation of the UK's core terrorism legislation is presented to the Secretary of State who is required to lay it before Parliament and publish it. To allow the IRTL to perform his duties he is security cleared and has access the most sensitive information and Government staff relating to counter-terrorism.

The IRTL's reports on TACT 2000 and part 1 of TACT 2006 may cover the following:

- The definition of terrorism;
- Proscribed organisations;
- Terrorist property;
- Terrorist investigations;
- Arrest and detention;
- Stop and search;
- Port and Border controls; and
- Terrorism offences

At the beginning of every year the IRTL is required to provide the Home Secretary with a work programme that specifies what reviews he intends to conduct in that 12 month period. The Secretary of State may also ask the IRTL to undertake other ad hoc or snapshot reviews. The previous IRTL, David Anderson QC, was asked by the Home Secretary to complete reviews on:

- The operation of Section 66 of the Immigration Act 2014 which provides the power to deprive a person of their British nationality where this may leave them stateless. This report was published in April 2016.

- The operation and regulation of investigatory powers following the implementation of the Data Retention and Investigatory Powers Act 2014. This report was published in June 2015 and titled 'A Question of Trust'. It helped to inform the development of, and debate during the Parliamentary passage of, the Investigatory Powers Act 2016; and
- The bulk powers in the Investigatory Powers Act 2016. This report examined the operational case for bulk interception, bulk equipment interference, bulk acquisitions of communications data, and bulk personal datasets. This report was published in August 2016.
- The operation and utility of Deportation with Assurances. This report was published in July 2017 and the Government will respond to it formally in due course.

The final report by Mr Anderson on the operation of the Terrorism Acts in 2015 was published in December 2016, and the Government response was published in July 2017.

Mr Hill's first report as the IRTL on the operation of the core Terrorism Acts in 2016 was published on 25 January 2018. His report on the use of terrorism legislation during Operation CLASSIFIC, the police investigation following the Westminster Bridge attack, was published on 28 March 2018. The Government responses to both reports will be published in due course.

7.2 – Investigatory Powers Commissioner

Lord Justice Sir Adrian Fulford was appointed as the first Investigatory Powers Commissioner (IPC) in February 2017 by the Prime Minister under section 227(1) of the Investigatory Powers Act 2016. Sir Adrian is currently supported in his role by 13 Judicial Commissioners, who were appointed by the Prime Minister on 1 September 2017.

Lord Justice Fulford has spent the majority of 2017 establishing the Investigatory Powers Commissioner's Office. The IPC took on statutory responsibility for oversight of the use of investigatory powers by public authorities on 1 September 2017. At this point, Sir Adrian took on the responsibilities of the Interception of Communications Commissioner, Intelligence Services Commissioner, and Chief Surveillance Commissioner. The IPC and Judicial Commissioners have oversight of all areas overseen by the previous Commissioners.

The IPC is responsible for keeping under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to:

- the interception of communications;
- the acquisition or retention of communications data;
- the acquisition of secondary data or related systems data; and
- equipment interference.

The IPC and Judicial Commissioners are supported by the Investigatory Powers Commissioner's Office. This includes a significantly expanded staff, including in-house legal and technical expertise, and a Technology Advisory Panel.

The IPC and Judicial Commissioners are also responsible for approving decisions to authorise warrants applied for under the Investigatory Powers Act. These warrants include:

- Targeted interception and bulk interception warrants
- Targeted equipment interference and bulk equipment interference warrants
- Bulk personal dataset warrants
- Bulk acquisition of communications data warrants
- Targeted examination warrants; and
- Mutual assistance warrants

7.3 – Interception of Communications Commissioner

The role of Interception of Communications Commissioner was abolished on 1 September 2017 under the Investigatory Powers Act 2016. All the responsibilities of the role have been taken on by the Investigatory Powers Commissioner.

The Interception of Communications Commissioner was previously appointed by the Prime Minister under section 57 of the Regulation of Investigatory Powers Act (RIPA). The Rt Hon Sir Stanley Burnton was appointed on 4 November 2015 and held the post until it was abolished.

The Interception of Communications Commissioner was independent of Government and was required to hold, or have held, high judicial office in order to be appointed to the role. The Commissioner's primary role was to oversee the use of two investigatory tools (interception and communications data) and to ensure that the Secretaries of State and public authorities operating under Part I of RIPA, which regulates the use of these powers, did so lawfully. Specifically, the Commissioner's statutory responsibilities under section 57(2) of RIPA were to keep under review:

- the exercise and performance by the Secretary of State of the powers and duties in sections 1 to 11 of RIPA, that is those relating to the granting and operation of interception warrants;
- the exercise and performance by the Scottish Minsters of the powers and duties conferred and imposed by sections 5, 9 and 10 of RIPA;
- the exercise and performance by the persons on whom they are conferred or imposed of the powers and duties under Chapter II Part I of RIPA, that is those relating to the acquisition and disclosure of communications data;
- the exercise and performance by the Secretary of State in relation to information under Part 1 of the powers and duties conferred or imposed by or under Part 3 of RIPA; and
- the adequacy of arrangements for safeguards relating to use that is made of interception material under section 15 of RIPA, which also embraces additional safeguards in section 16 of RIPA so far as applicable to Part I material, and those imposed by section 55.

Section 58(1) of RIPA imposed a statutory obligation on everyone concerned with the lawful interception of communications and the acquisition and disclosure of communications data under Part I of RIPA to disclose or provide to the Commissioner all such documents or information as they may require for the purpose of enabling the Commissioner to carry out his functions under section 57.

In addition to his statutory responsibilities under RIPA, the Commissioner also conducted oversight, by non-statutory agreement, of the lawful interception of prisoners' communications under section 47 of the Prison Act 1952 within prisons in England, Wales and Northern Ireland.

At the behest of the former Prime Minister David Cameron, the Commissioner also had responsibility for conducting non-statutory oversight of section 94 of the Telecommunications Act 1984. Specifically, this oversight covered the necessity and proportionality of any directions given

by the Secretary of State under Section 94, the use of any such directions and the safeguards that apply to them. Further information about directions given under this power, including those which enable the agencies to obtain communications data in bulk from telecommunications operators, may be found in Chapter 6 of this report.

The Commissioner did not have oversight of matters that were overseen by the Intelligence Services Commissioner or the Chief Surveillance Commissioner.

Under section 58(4) of RIPA, the Commissioner was required, as soon as practicable after the end of each calendar year and at the end of the period of six months beginning with the end of each calendar year, to report to the Prime Minister on the exercise of his functions. These reports were subsequently published and laid before Parliament.

The most recent annual report of the Commissioner, covering January to December 2016, was published on 20 December 2017 and contained detailed information and statistics in relation to the use of the investigatory powers that he oversaw. The report was published in full with no confidential annex. The statistics regarding the use of interception and communications data are set out in Chapter 6.1 to Chapter 6.6 of this report.

The Interception of Communications Commissioner's Office (IOCCO) also published a number of guidance documents, circulars, press statements and inquiry reports on its website in order to provide the public with as much information as possible about its functions. In addition, IOCCO has provided guidance to the Investigatory Powers Tribunal on a number of cases in 2017, and advice to public authorities in light of changes to existing Codes of Practice relating to powers overseen by the Commissioner.

Interception

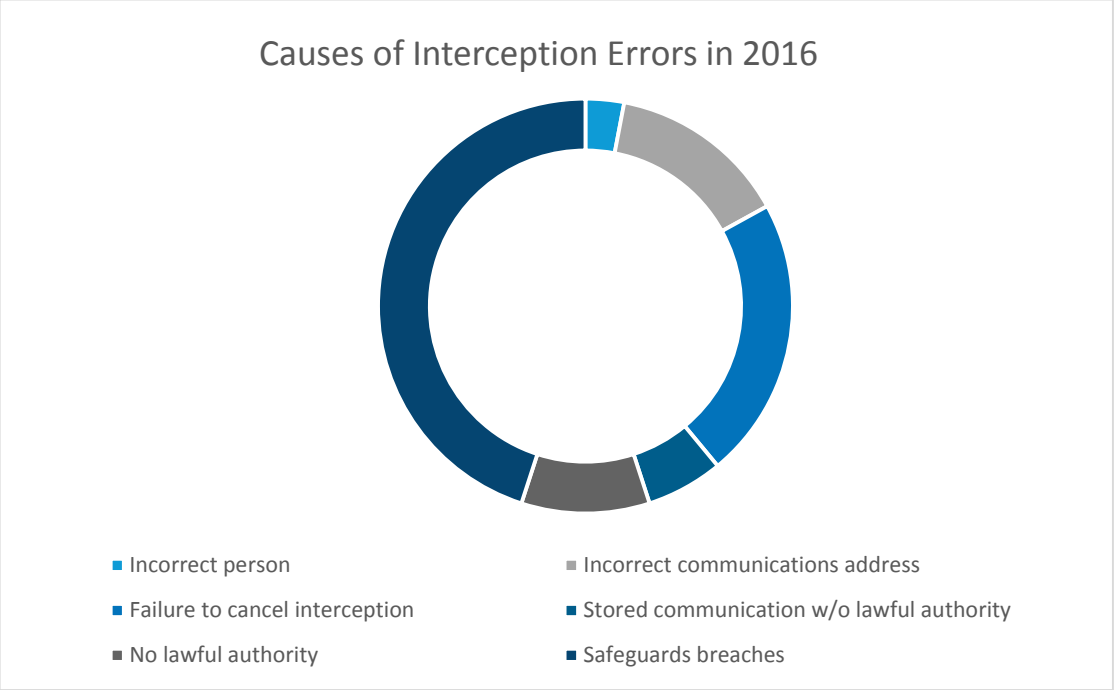
The Commissioner's 2016 Annual Report sets out details of the rigorous processes that his office, IOCCO, undertook to ensure that interception powers were being used lawfully and in accordance with RIPA. This includes inspections of the intercepting agencies and warrant granting departments. During 2016, IOCCO carried out 22 inspections of public authorities. There were three primary objectives during interception inspections, which were to ensure:

- that the systems in place for the interception of communications are sufficient for the purposes of Part I Chapter I and that all relevant records have been kept;
- that all interception has been carried out lawfully, and in accordance with Part I Chapter I of RIPA, and the associated Code of Practice; and
- that any errors are reported to the Commissioner and that the systems are reviewed and adapted where any weaknesses or faults are identified.

Over the course of these inspections, IOCCO examined 970 interception warrants, including associated paperwork. Following each inspection, IOCCO provided an inspection report to the head of the agency or department, outlining the formal recommendations. The relevant agency was required to report back to IOCCO within two months of this report, outlining the progress against these recommendations. The total number of recommendations made to the agencies and departments in 2016 was 28. During 2016, 108 errors were reported to IOCCO in relation to interception. This was an increase on the previous year's total of 68. The increase can be partly explained by the clearing of a backlog of previous errors by GCHQ. The breakdown of the causes of these errors is outlined below.

The largest category of errors was in relation to the “safeguards breaches”. These are instances where communications have been lawfully intercepted but where resultant actions do not comply with the safeguards in RIPA. An example of such an error would be an error in a technical system causing unwanted data to be selected for examination.

Figure 7: Summary of causes of errors reported to IOCCO in relation to interception in 2016



Communications Data

During 2016, IOCCO undertook 68 communications data inspections. Of these 68 inspections, 52 were of police forces and law enforcement agencies, three were of a security and intelligence agency, and 13 were of other public authorities and the National Anti-Fraud Network (NAFN). NAFN acts as the Single Point of Contact for all local authorities: since 1 December 2014, all local authority requests for communications data must be made through NAFN. As a consequence the Commissioner stopped inspecting individual local authorities but accessed those records at NAFN.

The primary objectives of the communications data inspections were to ensure:

- that the systems in place for acquiring communications data were sufficient for the purposes of RIPA and that all relevant records had been kept;
- that all acquisition of communications data had been carried out lawfully and in accordance with Part I Chapter II and its associated Code of Practice;
- that the data acquired was necessary and proportionate to the conduct authorised;
- that errors were being “reported” or “recorded” and that the systems were reviewed and adapted in light of any weaknesses or faults that were exposed; and
- that persons engaged in the acquisition of communications data were adequately trained and are aware of the relevant parts of the legislation.

As with interception inspections, IOCCO completed a report following each inspection, outlining recommendations, which the public authority was required to respond to within two months. From the 68 inspections in 2016, the total number of recommendations made was 235.

The Acquisition and Disclosure of Communications Data Code of Practice sets out two types of communications data error. A recordable error is one that does not result in communications data being wrongly acquired. Such errors must be recorded and made available to IOCCO during an inspection. A reportable error is one which results in data being wrongly acquired. Such errors must be reported to the Commissioner within five working days of the error being discovered.

In total, 1,101 communications data errors were reported to the Commissioner during 2016, a decrease of 8% on the 1,199 errors reported in 2015. A comparison with the 2015 figures reveals that the biggest causes of errors remain incorrect communications identifiers being submitted by applicants and single points of contact (SPoCs) within authorities, or data being acquired over the incorrect date or time period.

During 2016, 39.4% of errors identified were caused by the applicant and 43.5% by SPoCs by, for instance, including the incorrect communications address or date/time period on the application. 11.6% of errors were caused by communications service providers, for instance by disclosing the incorrect type of data or excess data, and 2.9% by designated persons.

At the end of each inspection, the public authority was given an overall compliance rating of good, satisfactory or poor. In 2016, 90% of public authorities achieved a good compliance rating, compared to 80% in 2015. In addition, 10% received a satisfactory rating, and no public authorities received a poor rating in 2015, compared to 4% in 2015.

Of the 1,101 errors in 2016, 29 serious errors were identified. IOCCO defines the following as serious errors:

- technical errors relating to communications service providers secure disclosure systems which resulted in a significant number of erroneous disclosures;
- errors where the public authority had, as a consequence of the data, initiated a course of action that impacted on persons not connected with the investigation or operation (for example, the sharing of information with another public authority stating a person was suspected of a crime, an individual being visited or the execution of a search warrant at premises unconnected with the investigation, the arrest of a person); and
- errors which resulted in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

Of the 29 serious errors, most were caused by human error.

Each of these errors is extremely regrettable. The Government welcomes the rigorous approach IOCCO took in their investigations to establish the causes of these errors, and to provide recommendations to mitigate the chances of recurrence.

The total of 1,101 errors in 2016, including the 29 serious errors, should be viewed in the context of the total number of items of communications data acquired: 754,559 for 2016 (0.015%).

Bulk Communications Data Acquisition

After commencing oversight of section 94 in February 2015, the Commissioner conducted formal inspections on an annual basis at any public authority in respect of which the Secretary of State had given a section 94 direction for the acquisition of bulk communications data.

As part of his investigations, the Commissioner reviewed any errors reported to him by the relevant security and intelligence agency, and the measures put in place by that agency to prevent any potential recurrence.

There is no statutory requirement to report an error when undertaking the acquisition of bulk communications data by means of a section 94 direction or when accessing data already retained as a consequence. However, the Security Service has implemented an internal policy process to report instances it considers to be errors when accessing communications data retained as a consequence of a section 94 direction.

In 2016 the Security Service reported 23 errors. The biggest cause of these was the applicant (i.e. the investigator/analyst) acquiring data on an incorrect communications address or identifier.

Whilst GCHQ has a mechanism for reporting errors to the Commissioner, it cannot easily differentiate the source from which the data is derived without compounding any potential intrusion (for example, by re-running the erroneous query) due to the fact that it commonly merges the communications data obtained under a section 94 direction with other datasets containing communications data (for example, related communications data obtained as a consequence of an interception warrant).

GCHQ has not reported any errors to the Commissioner that relate specifically to data obtained under a section 94 direction.

The Government welcomes the rigorous approach the Commissioner has taken in inspecting the use of data acquired under section 94 directions since he commenced oversight of this power in 2015.

7.4 – Intelligence Services Commissioner

The role of Intelligence Services Commissioner was abolished on 1 September 2017 under the Investigatory Powers Act 2016. All of the responsibilities of the role set out below have been taken on by the Investigatory Powers Commissioner.

The Intelligence Services Commissioner, the Rt Hon Sir John Goldring, was previously appointed by the Prime Minister under section 59 of the Regulation of Investigatory Powers Act 2000 (RIPA) on 1 January 2017, taking over from Sir Mark Waller. Sir John has now taken on the role of Deputy Investigatory Powers Commissioner.

The Intelligence Services Commissioner was independent of Government and was responsible for providing independent oversight of the use of investigatory powers by the security and intelligence agencies, the Ministry of Defence (MOD) and the armed forces. Section 59A of RIPA provided for the Prime Minister to direct the Intelligence Services Commissioner to keep under

review the carrying out of any aspect of the functions of the security and intelligence agencies, or the armed forces and MOD so far as engaging in intelligence activities. The Intelligence Services Commissioner did not have the function of overseeing anything kept under review by the Interception of Communications Commissioner.

The statutory functions of the Commissioner were set out in section 59 of RIPA. The Commissioner's statutory functions could be broken down into the following main areas:

- to keep under review the exercise by the Secretary of State and Scottish Ministers of their powers to issue warrants and authorisations to enable the security and intelligence agencies to carry out their functions. Such warrants and authorisations can relate to entering onto or interfering with property (or with wireless telegraphy), equipment interference, intrusive surveillance, and the investigation of electronic data protected by encryption; and
- to keep under review the exercise and performance of the powers and duties imposed on the intelligence services, MOD officials and members of the armed forces in relation to covert activities that are the subject of an internal authorisation procedure. Such activities include directed surveillance, the conduct and use of covert human intelligence sources (CHIS), and the investigation of electronic data protected by encryption.

The Commissioner also took on three additional oversight functions following Prime Ministerial directions issued under section 59A of RIPA:

- to keep under review compliance with 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;
- to provide oversight of the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets (BPD) by the intelligence services including misuse of data and how this can be prevented; and
- to keep under review the application of the Security Service guidelines on the use of agents who participate in criminality and the authorisations issued in accordance with them.

The Commissioner was also required to provide the Prime Minister with an annual report on the discharge of his functions, which the Prime Minister laid before Parliament. The Commissioner's final report covered 2016. As part of his continued drive for greater openness, the Commissioner restructured his report last year to address issues thematically – including, for example, sections on intrusive surveillance, directed surveillance, covert human intelligence sources and authorisations under section 7 of the Intelligence Services Act 1994 (ISA). This year the thematic sections were expanded to include additional information about bulk personal datasets and, for the first time, equipment interference. The Report provided greater statistical detail than previous iterations and also reported how the agencies and the Commissioner worked together to mitigate the risk of abuse of powers by any individual or group of individuals.

In order to acquire the information required to meet his statutory functions, the Commissioner scrutinised how the security and intelligence agencies, MOD officials and members of the armed forces carried out their activities. This scrutiny included formal inspections of MI5, SIS, GCHQ, the MOD and the armed forces. The Commissioner also conducted inspections of the Home Office, the Foreign Office and the Northern Ireland Office, the departments responsible for processing warrants for each Secretary of State.

The total number of warrants and authorisations extant across the security and intelligence agencies and MoD at the end of 2016 was 1,926. The Commissioner scrutinised 423 individual

warrants and authorisations, and the associated paperwork. Of the warrants and authorisations issued during 2016, as distinct from those extant at the end of the year, 33% were directed surveillance authorisations, 37% covert human intelligence source (CHIS) authorisations, 16% were authorisations under section 5 ISA, 11% combined property and intrusive surveillance warrants, 2% for Section 7 authorisations and 1% intrusive surveillance warrants.

An important aspect of the Commissioner's role was to examine errors that occurred during the process of the application and authorisation of warrants, or during their subsequent implementation. The Commissioner examined errors in two ways: firstly, through the scrutiny of individual warrants and authorisations as part of his inspection regime; secondly, the agencies were required to report to the Commissioner any error that resulted in any unauthorised activity where an authorisation should have been in place. Where the agencies were reporting errors to the Commissioner, he expected the reports to explain: when an error occurred; when it was discovered; the nature of the error; how it happened; and what, if any, unauthorised invasion of privacy resulted. The reports also included details of the steps taken to avoid errors happening again.

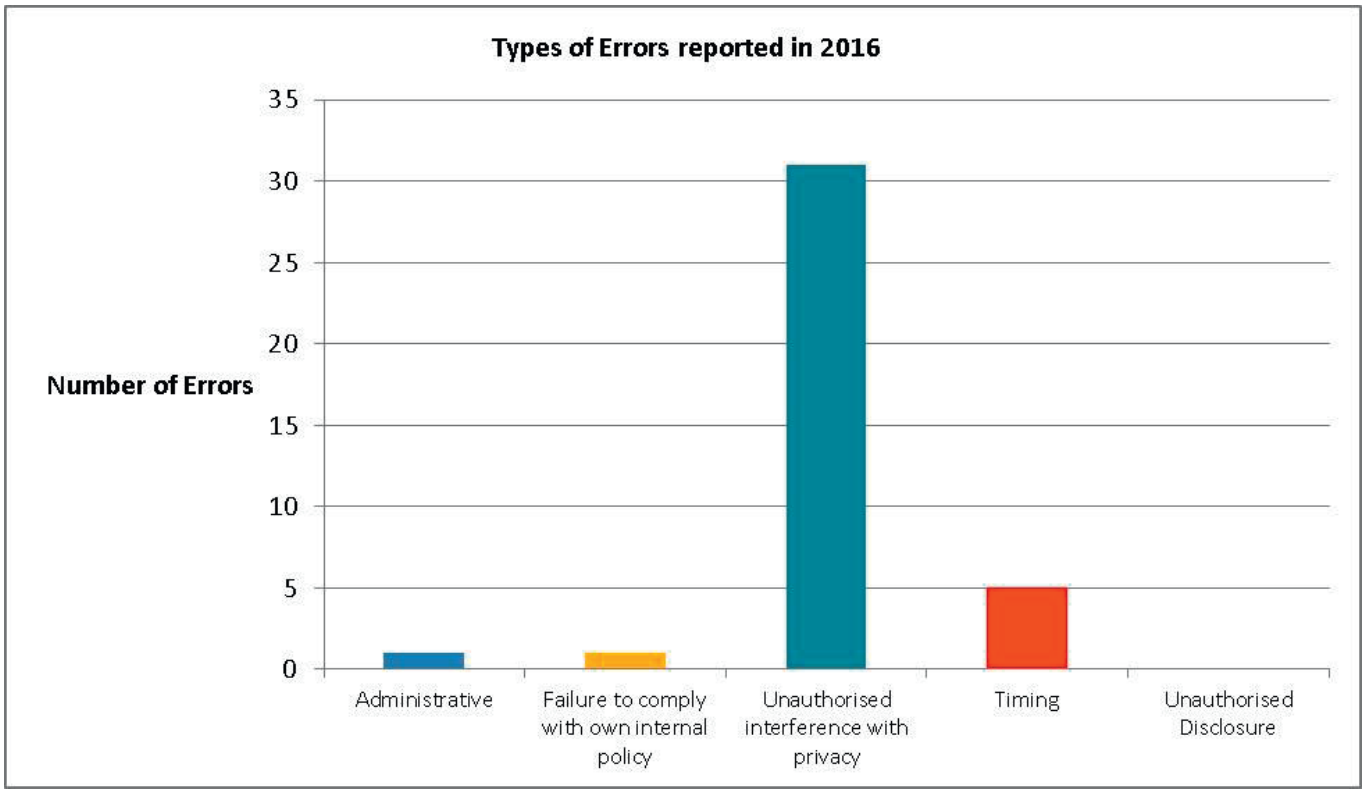
In his Annual Report for 2016, the Commissioner reviewed the categories of error reporting and clarified what is required from the security and intelligence agencies and the MOD. Category A errors are administrative errors; an obvious "slip" where no unauthorised intrusion into privacy had taken place as a result of the slip. These should have been reported to the Commissioner in writing bi-annually at inspection. Category B errors are those which are discovered to have occurred inadvertently during a warrant application, authorisation or during the operation of the warrant. These could be, for example, where an agency operated under a lapsed authorisation, or operated outside the parameters set out in the authorisation in the mistaken belief that it was authorised. These errors should have been reported to the Commissioner within three months of the date the error was discovered. Category C errors would be a deliberate decision taken to obtain information without proper authorisation or in any way to act irresponsibly. Such errors were expected to have been reported immediately to the Commissioner. If such a deliberate act were to have been committed, those involved would have been subject to disciplinary action and possible criminal charges.

During 2016, there were 38 errors, compared to 83 errors in 2015. Of this total, 37 were Category B errors or inadvertent errors and only one was a category A or administrative error. There were no Category C errors, as was the case in 2015.

Of the security and intelligence agencies, MI5 reported 28 errors to the Commissioner during 2016. The Commissioner noted that MI5 obtains a larger number of warrants and authorisations than the other agencies and that its error rate is low as a proportion of authorisations. SIS reported 6 errors to the Commissioner during 2015 and GCHQ reported 3. The Commissioner did not discover any additional errors during his inspections of these agencies.

In relation to warrant granting departments, one administrative error was brought to the Commissioner's attention when inspecting the Home Office, and the MOD reported one error to the Commissioner during an inspection.

Of the 38 errors reported the most common error was unauthorised interference with privacy. The breakdown of the causes of these errors is outlined below.



In 2016, the Commissioner made recommendations to the Security Service, SIS, GCHQ, MOD, Home Office, Foreign Office and the Northern Ireland Office relating to a range of processes, procedures and guidance available to staff. The Commissioner made a number of specific references to inadequacies in the way SIS record their decision-making in general, but noted improvements regarding the use of the Consolidated Guidance.

During 2016, the Consolidated Guidance was considered on 921 occasions by UKIC and the MOD. The Commissioner was satisfied that the agencies and the MOD took all steps they could to make their personnel aware of the terms of the guidance, and it was clear that careful consideration was given to its application in increasingly complex situations.

The Government welcomes the Commissioner's finding that "*the substantial compliance teams in each organisation and the relevant departments of state think deeply about the application of executive power and the intrusion into the privacy of its citizens. Everyone I inspect approaches the process in an open manner. Indeed, rather than hiding problems, they are often proactive in raising the most difficult issues with me*."

7.5 – Office of Surveillance Commissioners

The roles of Chief Surveillance Commissioner and Ordinary Surveillance Commissioners were abolished on 1 September 2017 under the Investigatory Powers Act 2016. All of their duties as set out below have been conferred on the Investigatory Powers Commissioner. The duties of the Chief Surveillance Commissioner have been conferred on the Investigatory Powers

Commissioner, and the duties of the Surveillance Commissioners have been conferred on the other Judicial Commissioners.

The Office of Surveillance Commissioners was responsible for providing robust, independent oversight of the use of covert surveillance powers by public authorities, excluding the security and intelligence agencies. The Chief Surveillance Commissioner, the Rt Hon the Lord Judge, and the Surveillance Commissioners, were appointed by the Prime Minister under section 91 of the Police Act 1997. All Commissioners were required to hold, or have held, high judicial office in order to be appointed to their roles.

The statutory responsibilities of the Chief Surveillance Commissioner were provided for in the Police Act 1997 RIPA and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). His specific responsibilities were to oversee:

- the performance of functions under Part III of the Police Act 1997;
- except in relation to the security and intelligence agencies, the exercise and performance of the powers and duties conferred by or under Parts II and III of RIPA; and
- the exercise and performance of the powers and duties conferred or imposed by or under RIPSA.

The Chief Surveillance Commissioner also acted as the Investigatory Powers Commissioner for the Sovereign Base Areas, Cyprus, under the Regulation of Investigatory Powers Ordinance 2012.

There were six Surveillance Commissioners working under the Chief Surveillance Commissioner. These six Commissioners had the following functions:

- granting prior approval for authorisations and renewals of any intrusive surveillance;
- granting prior approval for property interference where it involved a hotel bedroom, a dwelling, or office premises, or where it might have involved the acquisition of matters subject to legal privilege, confidential personal information or journalistic material;
- granting prior approval for any CHIS whose activities would have resulted in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege;
- granting prior approval for the long term authorisation of law enforcement relevant sources (commonly termed undercover officers);
- scrutinising notices of all other property interference authorisations, renewals and cancellations, and relevant source authorisations and cancellations;
- assisting the Chief Surveillance Commissioner in his oversight of functions exercised under Part III of RIPA, except where carried out with the permission off a judicial authority; and
- assisting the Chief Surveillance Commissioner in his duty to keep under review the use of Part II of RIPA by law enforcement agencies.

The Commissioners would only grant prior approval for any authorisation or renewal where the relevant action was necessary and proportionate. Where, at any time, a Commissioner was satisfied that there were not reasonable grounds for believing that an action was necessary and proportionate, he/she was able to quash an authorisation or renewal.

In addition to the six Commissioners, the Office of Surveillance Commissioners also included three Assistant Surveillance Commissioners and a number of Inspectors. The primary responsibility of the Assistant Commissioners was to oversee the activities of public authorities that are not law enforcement agencies, such as local authorities, in the exercise of their powers

under Part II of RIPA. To be appointed as an Assistant Surveillance Commissioner, an individual was required to hold, or have held, office as a judge of the Crown Court, a Circuit judge, a sheriff in Scotland, or a county court judge in Northern Ireland. The Surveillance Inspectors were responsible for assisting the Chief Surveillance Commissioner by undertaking detailed inspections of the public authorities whose activities he was tasked to oversee. The Surveillance Inspectors are continuing to assist the Investigatory Powers Commissioner. The Assistant Surveillance Commissioners are continuing in their roles, for a transitional period, until 30 April 2018.

The Chief Surveillance Commissioner reported annually to the Prime Minister and to Scottish Ministers on the matters for which the Commissioner was responsible under the Police Act 1997, RIPA and RIPSA. These reports were presented to Parliament and laid before the Scottish Parliament, and are publicly available. The Chief Surveillance Commissioner's most recent report was laid before Parliament on 20 December 2017 and covers the period 1 April 2016 to 31 March 2017.

The Commissioner's annual report includes statistics on the use of the powers of which he had oversight. Further details are included in Chapter 6 of this report.

The Commissioner's annual report includes details of the number of irregularities reported to him during the reporting period. For law enforcement agencies, there were 92 irregularities reported to the Commissioner and for other public authorities, there were three. This compared to 96 and four in 2015-16. The Commissioner outlines that the nature of irregularities varies very little from year to year. Sometimes there was a failure to be totally focused on what exactly has been authorised, and in precisely what terms, so that steps outside the authorised ambit were taken; sometimes there was a failure to ensure that what was sought had in fact been authorised; sometimes, equipment was allowed to continue to function after the expiry of the authorisation time, or after a direction to cease has been given; and sometimes supervising officers, more familiar with the legislation, recognised that an authorisation, which ought to have been procured in advance of an operation, was not.

Errors also occurred for technical reasons. For example, during this reporting period a law enforcement agency reported that a piece of equipment had captured more data than envisaged by the associated property interference and directed surveillance authorisation. This was because part of the equipment was automatically capturing more data than authorised. By the time the problem was identified the equipment had been used on a number of different operations. All were reported to the Commissioner and measures immediately put in place to prevent any repetition.

The Commissioner was clear that there is nothing to suggest wilful misconduct or bad faith in relation to any of these irregularities and that a total of 96 irregularities is an extremely small proportion of the total number of authorisations. The Commissioner reported that the overwhelming majority are the result of human error, which reinforces the need for regular training and continued robust oversight by senior officers and managers of the processes. The Commissioner further recommended that every public authority with the relevant statutory powers should have in place structures and training arrangements to ensure that the exercise of any such powers will be lawful.

7.6 – Investigatory Powers Tribunal

The Investigatory Powers Tribunal (IPT) was established in October 2000 under Part IV of RIPA. It is one part of a range of oversight provisions that ensure public authorities, including the security and intelligence agencies, act in a way that is compatible with the law, including the Human Rights Act 1998.

The Tribunal was established to consider, and if necessary, investigate and determine, any complaints made by members of the public (including non-governmental organisations) which fall into the following three categories.

First, the Tribunal can consider any complaint by a person who believes that they have been the victim of unlawful interference by public authorities, including the military, law enforcement and the security and intelligence agencies (MI5, SIS and GCHQ), using the investigatory powers regulated under RIPA. A complaint can be about any interference which the complainant believes has taken place against them, their property or communications, and can relate to interception, communications data acquisition, surveillance and property interference. In due course, the Tribunal will consider complaints relating to investigatory powers regulated under the Investigatory Powers Act 2016.

Second, the Tribunal can consider complaints by a person who is aggrieved by any conduct by or on behalf of the security and intelligence agencies.

Third, the Tribunal also considers claims where it is alleged that a human rights breach has been committed by the security and intelligence agencies.

Members of the public may be free to make the first two types of complaints (interference by public authorities and conduct of the security and intelligence agencies) to the ordinary courts instead of the Tribunal, but the Tribunal has additional powers of investigation which a court does not have. In cases of human rights breaches involving the security and intelligence agencies, the Tribunal is the only forum that can decide the complaint.

Members of the Tribunal must be senior members of the legal profession and both the President and Vice President must have held high judicial office.

There are currently eleven members of the Tribunal including the President, Sir Michael Burton. Sir Michael Burton is due to retire in September 2018. His successor is currently being recruited.

Recent Tribunal-related changes

The Investigatory Powers Act 2016 amends RIPA to provide for a new right of appeal from decisions and determinations of the Tribunal in circumstances where there is a point of law that raises an important point of principle or practice, or where there is some other compelling reason for allowing an appeal. The Home Office is taking forward work to implement this further safeguard.

The Home Office is also updating the Rules regulating the Tribunal. These rule changes will both reflect this new right of appeal and take into account other changes to Tribunal practice, which has evolved over the years since the current Rules came into force in 2000.

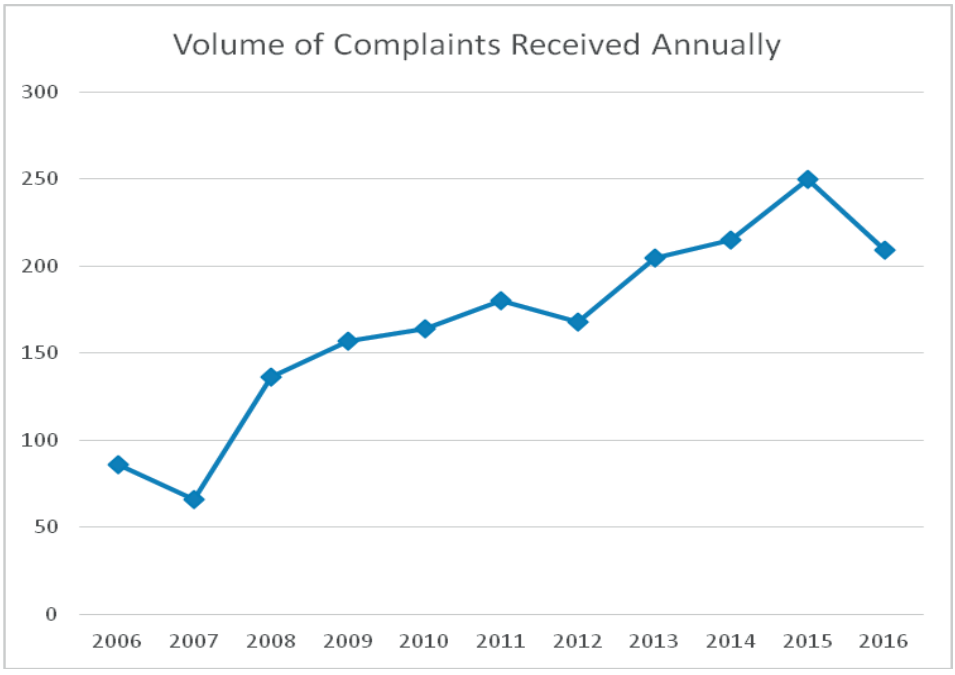
The Home Office consulted publicly on the draft Tribunal Rules in November 2017, and is preparing to lay the new Rules before Parliament.

Tribunal Statistics

In 2016, the Tribunal sat on eleven occasions in open court.

In 2016, the Tribunal received 209 new cases[35] and decided 230 cases. In 2015, the Tribunal received 251 new cases.

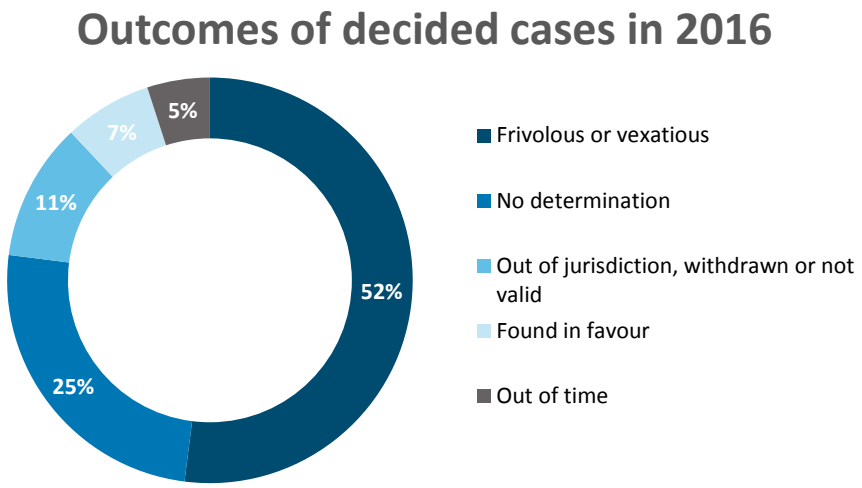
Volume of cases over the last ten years



Of the 230 decided cases in 2016, 120 (52%) were ruled to be frivolous or vexatious. These cases are ones where the allegation or belief is so fanciful that it is considered not to be sustainable. The decision to assess a case as frivolous or vexatious is currently taken by at least two Tribunal Members. In 58 (25%) of the cases, there was a "no determination outcome".

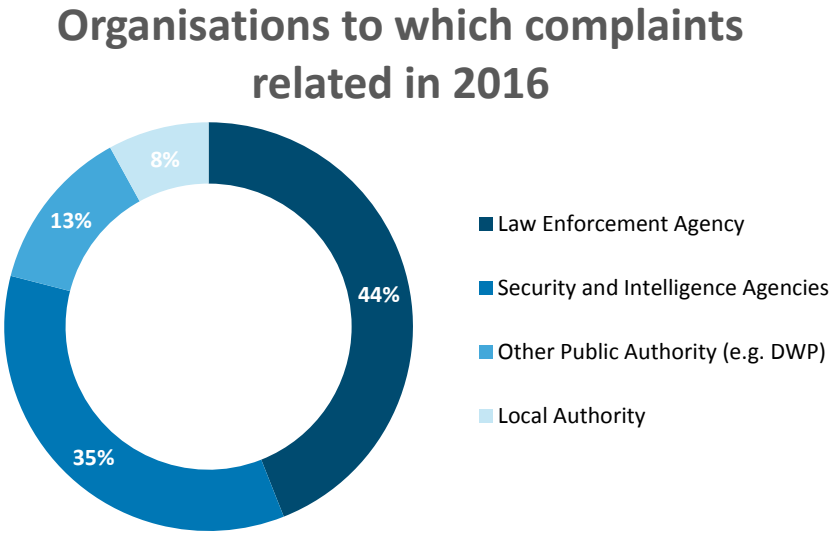
[35] The figure of 209 new complaints in 2016 does not include complaints that are the direct result of the online Privacy International campaign that followed the Tribunal's judgement in *Liberty/Privacy International (No 1 and No 2)* [2014] UKIP Trib 13/77-H [2015] 3 All ER 142 and [2015] 3 AER 212. That campaign has led to 665 individual complaints in all against the security and intelligence agencies. The Tribunal held an OPEN public hearing on 15 April 2016 to consider those complaints and the judgement that followed (dated 16 May 2016) can be found here: http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

This means that the Tribunal ruled there was no unlawful or unreasonable activity involving the complainant. 26 (11%) cases were ruled to be out of the Tribunal's jurisdiction, or were either withdrawn or invalid. Eleven (5%) cases were ruled to be out of time and in fifteen (7%) cases, the Tribunal found in favour of the complainant.



Details of all of the cases received and decided by the Tribunal between 2011 and 2016 are at **Annex C**[36].

44% of complaints were related to law enforcement agencies (such as the National Crime Agency, or a police force). 35% of complaints were related to the security and intelligence agencies whilst 8% of complaints were related to a local authority. Finally, 13% of complaints were related to other public authorities (for example, the Department for Work and Pensions).



Full copies of the Tribunal's judgments are available on the Tribunal website at www.ipt-uk.com

[36] All of the Tribunal judgements arising from oral hearings are published on the Tribunal website at www.ipt-uk.com and BAILII (The British and Irish Legal Information Institute)

8 – Recommended Reading List

Legislation

- Anti-social Behaviour, Crime and Policing Act 2014 – www.legislation.gov.uk/ukpga/2014/12/contents
- Anti-Terrorism, Crime and Security Act 2001 http://www.legislation.gov.uk/ukpga/2001/24/contents
- Counter-Terrorism Act 2008 http://www.legislation.gov.uk/ukpga/2008/28
- Counter-Terrorism and Security Act 2015 - www.legislation.gov.uk/ukpga/2015/6/contents
- Data Protection Act 2018 – www.legislation.gov.uk/ukpga/2018/12/contents
- Data Retention and Investigatory Powers Act 2014 - www.legislation.gov.uk/ukpga/1998/29/contents
- Digital Economy Bill 2016-2017 - https://services.parliament.uk/bills/2016-17/digitaleconomy.html
- Freedom of Information Act 2000 – www.legislation.gov.uk/ukpga/2000/36/contents
- Human Rights Act 1998 – www.legislation.gov.uk/ukpga/1998/42/contents
- Immigration (European Economic Area) Regulations 2016 - http://www.legislation.gov.uk/uksi/2016/1052/made
- Intelligence Services Act 1994 – www.legislation.gov.uk/ukpga/1994/13/contents
- Investigatory Powers Act 2016 - http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
- Justice and Security Act 2013 – www.legislation.gov.uk/ukpga/2013/18/contents
- Police Act 1997 – www.legislation.gov.uk/ukpga/1997/50/contents
- Policing and Crime Act 2017 http://www.legislation.gov.uk/ukpga/2017/3/contents/enacted (the section in the report currently has it down as a Bill
- Privacy and Electronic Communications (EC Directive) Regulations 2003 – www.legislation.gov.uk/uksi/2003/2426/contents/made
- Proscribed Organisations (Applications for Deproscription etc) Regulations 2006 (SI 2006/2299) – www.legislation.gov.uk/uksi/2006/2299/made
- Protection of Freedoms Act 2012 – www.legislation.gov.uk/ukpga/2012/9/contents
- Regulation of Investigatory Powers Act 2000 – www.legislation.gov.uk/ukpga/2000/23/contents
- Terrorism Act 2000 – www.legislation.gov.uk/ukpga/2000/11/contents
- Terrorism Act 2006 – www.legislation.gov.uk/ukpga/2006/11/contents
- Terrorist Asset-Freezing etc Act 2010 – www.legislation.gov.uk/ukpga/2010/38/contents
- Terrorism Prevention and Investigation Measures Act 2011 – www.legislation.gov.uk/ukpga/2011/23

Government Publications

- Acquisition and Disclosure of Communications Data Code of Practice under the Regulation of Investigatory Powers Act 2000 - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf
- CONTEST: The United Kingdom's Strategy for Countering Terrorism – www.gov.uk/government/collections/contest
- CONTEST Annual Report for 2015 – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/539683/55469_Cm_9310_Web_Accessible_v0.11.pdf
- Counter-Terrorism Statistics, Operation of Police Powers under the Terrorism Act 2000 – https://www.gov.uk/government/collections/counter-terrorism-statistics
- Exclusion Decisions and Exclusion Orders - https://www.gov.uk/government/publications/exclusion-decisions-and-exclusion-orders
- HM Government Modern Crime Prevention Strategy - https://www.gov.uk/government/publications/modern-crime-prevention-strategy
- National Crime Agency annual report and accounts 2015 to 2016 – https://www.gov.uk/government/publications/national-crime-agency-annual-report-and-accounts-2015-to-2016
- Police and Border Officials on Seizing Travel Documents Code of Practice - https://www.gov.uk/government/publications/code-of-practice-for-police-and-border-officials-on-seizing-travel-documents
- Retention of Communications Data Code of Practice under the Regulation of Investigatory Powers Act 2000 - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426249/Retention_of_Communications_Data_Code_of_Practice_March_2015.pdf
- Royal Prerogative - https://www.gov.uk/government/publications/royal-prerogative
- Statistics on Closed Material Procedure – https://www.gov.uk/government/publications/use-of-closed-material-procedure-report-25-june-2015-to-24-june-2016
- Statistics on Terrorist Asset-Freezing – https://www.gov.uk/government/collections/operation-of-the-uks-counter-terrorist-asset-freezing-regime-quarterly-report-to-parliament
- Investigatory Powers Act 2016 Codes of Practice (minus the Draft Communications Data Code of Practice- https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice
- Investigatory Powers Act, Draft Communications Data Code of Practice - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724392/CCS207_CCS0618947544-001_Home_Office_Publication_of_Codes_WEB_V2.pdf

Independent Publications

- Attacks in London and Manchester between March and June 2017; Independent Assessment of MI5 and Internal Reviews, David Anderson QC - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf
- Bulk Powers Review by the former Independent Reviewer of Terrorism Legislation, David Anderson QC - https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review-report/
- A Question of Trust: Report of the Investigatory Powers Review by the former Independent Reviewer of Terrorism Legislation, David Anderson QC – https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/
- Independent Reviewer of Terrorism Legislation, Annual Reports (Terrorism Acts, TPIMs, Asset-Freezing) – https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2018/01/Terrorism-Acts-in-2016.pdf
- Intelligence and Security Committee, Report on Privacy and Security – http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf
- Investigatory Powers Commissioner's Office – www.ipco.org.uk
- Investigatory Powers Tribunal, Case Statistics and Judgments – www.ipt-uk.com
- Office of Surveillance Commissioner's Report 2016 – 2017 – www.ipco.org.uk (publications page)
- Report of the Intelligence Services Commissioner for 2016 – www.ipco.org.uk (publications page)
- Report of the Interception of Communications Commissioner for 2016 – www.ipco.org.uk (publications page)
- Royal United Services Institute, Independent Surveillance Review – www.rusi.org

9 – ANNEXES

ANNEX A – Proscribed Terrorist Organisations

List of Proscribed International Terrorist Groups

- 74 international terrorist organisations are proscribed under the Terrorism Act 2000.
- 14 organisations in Northern Ireland that were proscribed under previous legislation.

The information about the groups' aims was given to Parliament when they were proscribed.

Users should bear in mind that there is no universal standard for transliterating Arabic and other languages into Latin characters. Therefore, the spelling of the names of proscribed organisations appearing in other publications may differ slightly from that given in this list.

17 November Revolutionary Organisation (N17) - *Proscribed March 2001*
Aims to highlight and protest at what it deems to be imperialist and corrupt actions, using violence. Formed in 1974 to oppose the Greek military Junta, its stance was initially anti-Junta and anti-US, which it blamed for supporting the Junta.

Abdallah Azzam Brigades, including the Ziyad al-Jarrah Battalions (AAB) - *Proscribed June 2014*
AAB is an Islamist militant group aligned with Al Qa'ida and the global jihad movement, currently fighting in Syria and Lebanon. The group began operating in Pakistan in 2009. The Lebanese branch uses the name the Ziyad al Jarrah Battalion, and is named after Lebanese 9/11 hijacker Ziyad al Jarrah who participated in the hijacking and crash of United Flight 93.

AAB has increased its operational pace since the onset of the Syrian insurgency, claiming responsibility for a rocket attack launched from Lebanon into northern Israel in August 2013. On 19 November 2013, AAB claimed responsibility for a double suicide bombing outside the Iranian embassy in Beirut, which killed at least 22 people and wounded over 140.

On 19 February 2014, the group's media wing, the Al-Awzaey Media Foundation, announced on Twitter and YouTube that the group claimed responsibility for two suicide bombings near the Iranian cultural centre in Beirut killing 11 and wounding 130, in revenge for actions by Iran and Hizballah, in Lebanon and Syria.

The group has threatened to launch further terrorist attacks and has demanded that the Lebanese Government free imprisoned jihadists. It has also threatened attacks on Western targets in the Middle East.

Abu Nidal Organisation (ANO) - *Proscribed March 2001*
ANO's principal aim is the destruction of the state of Israel. It is also hostile to 'reactionary' Arab regimes and states supporting Israel.

Abu Sayyaf Group (ASG) - *Proscribed March 2001*
The precise aims of the ASG are unclear, but its objectives appear to include the establishment of an autonomous Islamic state in the Southern Philippine island of Mindanao.

Ajnad Misr (Soldiers of Egypt) - *Proscribed November 2014*
The group is a jihadist group based in Egypt and is believed to be a splinter group of Ansar Bayt al Maqdis (ABM), which was proscribed on 4 April. Ajnad Misr has stated that it seeks to protect Egyptian Muslims and avenge alleged abuse against them by the Egyptian security services.

Ajnad Misr is believed to have been active since 20 November 2013, when it attacked an Egyptian checkpoint. It announced its establishment on 23 January 2014 and has claimed responsibility a number of attacks on Egyptian security forces in a military campaign. The claims were made in three communiqués posted on its Facebook and Twitter accounts on 23 January, 24 January, and 31 January. On the jihadi forum al-Fida', Ansar Bayt al Maqdis, referred to Ajnad Misr in a communiqué issued on January 28, expressing support for the group and identifying it as being responsible for two attacks in Greater Cairo in January. Ajnad Misr has claimed responsibility for the bombing at Cairo University on 2 April that resulted in the death of a policeman and injuries to three others.

al-Ashtar Brigades including Saraya al-Ashtar, Wa'ad Allah Brigades, Islamic Allah Brigades, Imam al-Mahdi Brigades and al-Haydariyah Brigades - *Proscribed December 2017*
The group is a Shia militant extremist organisation that was established during 2013. Its aim is to overthrow the Bahraini al-Khalifa ruling family through violent militant operations. It lists the ruling al-Khalifa family, Bahrain security forces and Saudi Arabia as targets for attacks. The group has been responsible for numerous attacks since being established, which it has claimed responsibility for, including:

- On 1 January 2017 – 10 inmates (all convicted of terrorism offences in Bahrain) were broken out of Jaw Reformation and Rehabilitation Centre, which led to the death of a police officer.
- An IED attack in a bus station in Sitrah, which was claimed by the group under the name Wa'ad Allah Brigades on 7 February 2017.
- An attack on a police vehicle near the village of al Qadeem on 7 July 2017.

The group has promoted violent activity against the Bahraini Government, as well as the British, American and Saudi Arabian Governments on social media.

Al-Gama'at al-Islamiya (GI) - *Proscribed March 2001*
The main aim of GI is to overthrow the Egyptian government and replace it with an Islamic state through all means, including the use of violence. Some members also want the removal of Western influence from the Arab world.

Al Ghurabaa - *Proscribed July 2006*
Al Ghurabaa / The Saved Sect is an Islamist group which seeks to establish an Islamic Caliphate ruled by Shariah law. The group first emerged as Al Muhajiroun in the UK in 1996, led by Omar Bakri Muhammed, who then publicly disbanded the organisation in 2004. The organisation reformed in 2004 under the names Al Ghurabaa and the Saved Sect. While the Group has some links to groups overseas, it is based and operates within the UK.

Note: The Government laid Orders in January 2010 and November 2011, which provide that **"Al Muhajiroun", "Islam4UK", "Call to Submission", "Islamic Path", "London School of Sharia"** and **"Muslims Against Crusades"** should be treated as alternative names for the organisation which is already proscribed under the names **Al Ghurabaa** and **The Saved Sect**. The Government laid an Order, in June 2014 recognising **"Need4Khilafah"**, the **"Shariah Project"** and the **"Islamic Dawah Association"** as the same as the organisation proscribed as Al Ghurabaa and **The Saved Sect**, which is also known as **"Al Muhajiroun"**.

Al Ittihad Al Islamia (AIAI) - *Proscribed October 2005*
The main aims of AIAI are to establish a radical Sunni Islamic state in Somalia, and to regain the Ogaden region of Ethiopia as Somali territory via an insurgent campaign. Militant elements within AIAI are suspected of having aligned themselves with the 'global jihad' ideology of Al Qa'ida, and to have operated in support of Al Qa'ida in the East Africa region.

Al Murabitun - *Proscribed April 2014*
Al Murabitun resulted from a merger of two Al Qa'ida in the Maghreb (AQ-M) splinter groups that are active in Mali and Algeria, the Movement for the Unity and Jihad in West Africa (MUJWA) and Mokhtar Belmokhtar's group, the Al Mulathamine Battalion which included the commando element 'Those Who Sign in Blood'. The merger was announced in a public statement in August 2013.

Al Murabitun aspires to unite Muslims from "the Nile to the Atlantic" and has affirmed its loyalty to al-Qaida leader Ayman al-Zawahiri and the emir of the Afghan Taleban, Mullah Omar.
As at 3 April 2014, the group has not claimed responsibility for any terrorist attacks since the merger but both precursor groups have participated in a number of terrorist attacks and kidnapping for ransom during the past 13 months. Belmokhtar's group was responsible for the attack against the In Amenas gas facility in January 2013 that resulted in the death of over thirty people including Britons. In May 2013 the two groups targeted a military barracks in Agadez, Niger and a uranium mine in Arlit which supplies French nuclear reactors. The suicide attack in Agadez resulted in the deaths of at least twenty people.

Despite previously separating themselves from AQM, citing leadership issues and the desire to expand their control, both precursor groups continued to cooperate and fight alongside AQM fighters in Mali and other regions of West Africa. This activity has continued since the merger.

al-Mukhtar Brigades including Saraya al-Mukhtar - *Proscribed December 2017*
The group is a Shia militant organisation that was established during 2013. It lists the al-Khalifa ruling family, Bahrain security forces and Saudi Arabia as targets for attacks. The group's activities include the continued promotion and glorification of terrorism via social media throughout 2017.

Al Qa'ida (AQ) - *Proscribed March 2001*
Inspired and led by Usama Bin Laden, its aims are the expulsion of Western forces from Saudi Arabia, the destruction of Israel and the end of Western influence in the Muslim world.

Note: The Government laid Orders in July 2013 December 2016 and May 2017, which provided that the **"al-Nusrah Front (ANF)", "Jabhat al-Nusrah li-ahl al Sham", "Jabhat Fatah al-Sham"** and **"Hay'at Tahrir al-Sham"** should be treated as alternative names for the organisation which is already proscribed under the name Al Qa'ida.

Al Shabaab - *Proscribed March 2010*
Al Shabaab is an organisation based in Somalia which has waged a violent campaign against the Somali Transitional Federal Government and African Union peacekeeping forces since 2007, employing a range of terrorist tactics including suicide bombings, indiscriminate attacks and assassinations. Its principal aim is the establishment of a fundamentalist Islamic state in Somalia, but the organisation has publicly pledged its allegiance to Usama Bin Laden and has announced an intention to combine its campaign in the Horn of Africa with Al Qa'ida's aims of global jihad.

Ansar Al Islam (AI) - *Proscribed October 2005*
AI is a radical Sunni Salafi group from northeast Iraq around Halabja. The group is anti-Western, and opposes the influence of the US in Iraqi Kurdistan and the relationship of the KDP and PUK to Washington. AI has been involved in operations against Multi-National Forces-Iraq (MNF-I).

Ansar al-Sharia-Benghazi (AAS-B) which translates as the Partisans of Islamic Law - *Proscribed November 2014*
AAS-B is a Sunni Islamist militia group that has an anti-Western rhetoric and advocates the implementation of strict Sharia law. AAS-B came into being in 2011, after the fall of the Gaddafi regime. The group was led by Mohammed Ali al-Zahawi and Ahmed Abu Khattalah is an AAS-B senior leader.

AAS-B is involved in terrorist attacks against civilian targets, frequent assassinations, and attempted assassinations of security officials and political actors in eastern Libya. On 11 September, 2012 members of AAS-B took part in the attack against the U.S. Special Mission and Annex in Benghazi, Libya, killing the US ambassador and three other Americans. In September 2012, Mohammed Ali al-Zahawi, in an interview openly stated his support for Al Qa'ida's strategy but denied any links to the organisation. He also confirmed AAS-B had demolished and desecrated Sufi shrines in Benghazi, which the group regard as idolatrous.

AAS-B used its online presence to denounce the 2013 capture and removal from Libya of al Qa'ida operative Abu Anas al-Libi, by American military forces. In August 2013, Ahmed Abu Khattala, a senior leader of the group, was charged with playing a significant role in last year's attack on the U.S. diplomatic compound in Benghazi.

AAS-B continues to pose a threat to Libya and Western interests and is alleged to have links to proscribed organisation Ansar al-Sharia-Tunisia and Al Qa'ida.

The US designated AAS-B as a terrorist organisation in January 2014 and the UN listed AAS-B on 19 November

Ansar Al Sharia-Tunisia (AAS-T) - *Proscribed April 2014*
Ansar Al Sharia-Tunisia (AAS-T) is a radical Islamist group founded in April 2011. The group aims to establish Sharia law in Tunisia and eliminate Western influence. The group is ideologically aligned to Al Qa'ida (AQ) and has links to AQ affiliated groups. It is reported that the group announced its loyalty to AQM in September 2013.
AAS-T's leader, Seif Allah Ibn Hussein also known as Abu Ayadh al-Tunis, is a former AQ veteran combatant in Afghanistan. He has been hiding following issue of a warrant for his arrest relating to an allegation of inciting the attack on the US Embassy in Tunis that killed four people in September 2012.

Extremists believed to have links with AAS-T are assessed to be responsible for the attacks in October 2011 on a television station and, in June 2012, an attack on an art exhibit. AAS-T is assessed to be responsible for the attacks on the US Embassy and American school in Tunis in September 2012. The Tunisian government believe AAS-T was responsible for the assassination of two National Coalition Assembly members; Chokri Belaid in February 2013 and Mohamed Brahmi in July 2013.

Additionally, elements of the group are believed to have been involved in the attempted suicide attack, in October 2013, at a hotel in a tourist resort in Sousse where a significant number of British tourists were staying.

Ansar Al Sunna (AS) - *Proscribed October 2005*
AS is a fundamentalist Sunni Islamist extremist group based in central Iraq and what was the Kurdish Autonomous Zone (KAZ) of Northern Iraq. The group aims to expel all foreign influences from Iraq and create a fundamentalist Islamic state.

Ansar Bayt al-Maqdis (ABM) - *Proscribed April 2014*
ABM is an Al Qa'ida inspired militant Islamist group based in the northern Sinai region of Egypt. The group is said to recruit within Egypt and abroad and aims to create an Egyptian state ruled by Sharia law.

ABM is assessed to be responsible for a number of attacks on security forces in Egypt since 2011. The attacks appear to have increased since the overthrow of the Morsi government in July 2013. The group's reach goes beyond the Sinai, with the group claiming responsibility for a number of attacks in Cairo and cross-border attacks against Israel. ABM has undertaken attacks using vehicle borne improvised explosive devices and surface-to-air missiles. Examples of attacks that the group has claimed responsibility for include:

- in September 2013 an attack on the Egyptian Interior Minister in which a UK national was seriously injured;
- the attack on a police compound in Mansoura on 24 December 2013, killing at least 16 people, including 14 police officers; and
- an attack on a tourist bus in which three South Koreans and their Egyptian driver died on 16 January 2014.

Ansarul Muslimina Fi Biladis Sudan (Vanguard for the protection of Muslims in Black Africa) (Ansaru) - *Proscribed November 2012*
Ansaru is an Islamist terrorist organisation based in Nigeria. They emerged in 2012 and are motivated by an anti-Nigerian Government and anti-Western agenda. They are broadly aligned with Al Qa'ida.

Armed Islamic Group (Groupe Islamique Armée) (GIA) - *Proscribed March 2001*
The aim of the GIA is to create an Islamic state in Algeria using all necessary means, including violence.

Asbat Al-Ansar (League of Partisans or Band of Helpers) - *Proscribed November 2002*
Sometimes going by the aliases of 'The Abu Muhjin' group/faction or the 'Jama'at Nour', this group aims to enforce its extremist interpretation of Islamic law within Lebanon and increasingly, further afield.

Babbar Khalsa (BK) - *Proscribed March 2001*
BK is a Sikh movement that aims to establish an independent Khalistan within the Punjab region of India.

Basque Homeland and Liberty (Euskadi ta Askatasuna) (ETA) - *Proscribed March 2001*
ETA seeks the creation of an independent state comprising the Basque regions of both Spain and France**.**

Baluchistan Liberation Army (BLA) - *Proscribed July 2006*
BLA are comprised of tribal groups based in the Baluchistan area of Eastern Pakistan, which aims to establish an independent nation encompassing the Baluch dominated areas of Pakistan, Afghanistan and Iran.

Boko Haram (Jama'atu Ahli Sunna Lidda Awati Wal Jihad) (BH) - *Proscribed July 2013*
Boko Haram is a terrorist organisation, based in Nigeria that aspires to establish Islamic law in Nigeria and has carried out a number of terrorist attacks that have targeted all sections of Nigerian society.

Egyptian Islamic Jihad (EIJ) - *Proscribed March 2001*
The main aim of the EIJ is to overthrow the Egyptian government and replace it with an Islamic state. However, since September 1998, the leadership of the group has also allied itself to the 'global Jihad' ideology expounded by Usama Bin Laden and has threatened Western interests.

Global Islamic Media Front (GIMF) including GIMF Banlga Team also known as Ansarullah Bangla Team (ABT) and Ansar-al Islam – *Proscribed July 2016*
GIMF is an Islamist extremist propaganda organisation associated with Al Qa'ida (AQ) and other extremist groups around the world. Its activities include propagating a jihadist ideology, producing and disseminating training manuals to guide terror attacks and publishing jihadi news casts. GIMF releases products in a number of languages including Arabic, Urdu, Bengali, English, German and French.

On 31 December 2015, the GIMF announced the merger of ABT into its ranks, renaming it GIMF Bangla Team. Prior to the merger, using the names ABT and Ansar-al Islam, the group claimed responsibility for the prominent murders and attacks of secular bloggers from 2013 to 2015: including Bangladeshi-American Avijit Roy; Niladri Chatterji Niloy; Ahmed Rajib Haider; Asif Mohiuddin; Oyasiqur Rahman; Ananta Bijoy; Das and AKM Shafiul Islam. The group have been linked to a number of hit lists of bloggers, writers and activists around the world (including nine individuals based in Britain, seven in Germany and two in America, one in Canada and one in Sweden) in 2015.

On 7 January 2016 GIMF Bangla Team published an infographic chronicling attacks carried out against "blasphemers in Bangladesh" from January 2013 to October 2015. The graphic contained names and locations of 13 attacks, eight of which were celebrated as successful assassinations. Bangladesh banned ABT in May 2015.

Groupe Islamique Combattant Marocain (GICM) - *Proscribed October 2005*
The traditional primary objective of the GICM has been the installation of a governing system of the caliphate to replace the governing Moroccan monarchy. The group also has an Al Qa'ida-inspired global extremist agenda.

Hamas Izz al-Din al-Qassem Brigades - *Proscribed March 2001*
Hamas aims to end Israeli occupation in Palestine and establish an Islamic state.

Harakat-Ul-Jihad-Ul-Islami (HUJI) - *Proscribed October 2005*
The aim of HUJI is to achieve though violent means accession of Kashmir to Pakistan, and to spread terror throughout India. HUJI has targeted Indian security positions in Kashmir and conducted operations in India proper.

Harakat-Ul-Jihad-Ul-Islami (Bangladesh) (HUJI-B) - *Proscribed October 2005*
The main aim of HUJI-B is the creation of an Islamic regime in Bangladesh modelled on the former Taliban regime in Afghanistan.

Harakat-Ul-Mujahideen/Alami (HuM/A) and Jundallah - *Proscribed October 2005*
The aim of both HuM/A and Jundallah is the rejection of democracy of even the most Islamic-oriented style, and to establish a caliphate based on Sharia law, in addition to achieving accession of all Kashmir to Pakistan. HuM/A has a broad anti-Western and anti-President Musharraf agenda.

Harakat Mujahideen (HM) - *Proscribed March 2001*
HM, previously known as Harakat Ul Ansar (HuA) seeks independence for Indian-administered Kashmir. The HM leadership was also a signatory to Usama Bin Laden's 1998 fatwa, which called for worldwide attacks against US and Western interests.

Haqqani Network (HQN) - *Proscribed March 2015*
The Haqqani Network (HQN) is an Islamist, nationalist group seeking to establish Sharia law and control territory in Afghanistan. It is ideologically aligned with the Taleban, and aims to eradicate Western influence, disrupt the Western military and political efforts in Afghanistan. The group is demanding that US and Coalition Forces withdraw from Afghanistan. The group is led by Jalaluddin Haqqani and his son, Sirajuddin.

HQN has links with a number of terrorist groups in the region including proscribed Central Asian group Islamic Jihad Union (IJU). HQN also have long established links with Al Qa'ida (AQ) that were strengthened after the removal of the Taleban by the US when AQ leader Osama bin Laden was probably sheltered by Jalaluddin in North Waziristan (NWA).

HQN continues to play an active and influential role in the Afghan insurgency in the East of the country and is seeking to expand its influence in to other areas of Afghanistan. While it can be difficult to identify specific HQN responsibility for attacks, given the Taleban practice of claiming attacks on behalf of the insurgency as a whole, the group believed to have been responsible for the recent attack against the British Embassy vehicle in November 2014 which killed six people including a UK national and an Afghan member of UK Embassy staff and injuring more than 30 people.

It is likely that HQN will continue to view Kabul as a key target location due to the concentration of UK and Western interests in the capital.

HQN has been banned as a terrorist group by the USA since September 2012, Canada since May 2013 and the UN since November 2012.

Hasam including Harakat Sawa'd Misr, Harakat Hasm and Hasm - *Proscribed December 2017*
The group is an extremist group using violent tactics against the Egyptian security forces, and the Egyptian regime. The group announced its creation on 16 July 2016 following an attack in Fayoum Governate, Egypt. In September 2016 the group claimed responsibility for the attempted assassination of Assistant Prosecutor General Zakaria Abdel-Aziz. On 5 August 2016 the group also claimed responsibility for the attempted assassination of the former Grand Mufti of Egypt Ali Gomaa.

The group have claimed responsibility for over 15 attacks including:

- 8 March 2017 - Small arms fire in Cairo;
- 26 March 2017 - IED attack in Cairo;
- 1 May 2017 - Small arms fire in Cairo;
- 18 June 2017 – IED attack in Cairo;
- 7 July 2017 - Small arms fire in Cairo;
- 20 July 2017 - Small arms fire in Fayoum Governate; and
- 30 September 2017 – IED explosion close to the Myanmar Embassy Cairo.

Hizballah Military Wing – *Hizballah's External Security Organisation was proscribed March 2001 and in 2008 the proscription was extended to Hizballah's Military apparatus including the Jihad Council.*
Hizballah is committed to armed resistance to the state of Israel and aims to seize all Palestinian territories and Jerusalem from Israel. Its military wing supports terrorism in Iraq and the Palestinian territories.

Imarat Kavkaz (IK) also known as the Caucasus Emirate - *Proscribed December 2013*
Imarat Kavkaz seeks a Sharia-based Caliphate across the North Caucasus. It regularly uses terrorist tactics and has carried out attacks against both Russian state and civilian targets. The organisation claimed responsibility for the attack on Domedodevo airport in Moscow in January 2011, that killed 35 including one British national and a suicide attack on the Moscow Metro in March 2010 that killed 39. Since then there has been continued activity by Imarat Kavkaz, including renewed threats of terrorist activity in Russia.

Indian Mujahideen (IM) - *Proscribed July 2012*
IM aims to establish an Islamic state and implement Sharia law in India using violent means.

Islamic Army of Aden (IAA) - *Proscribed March 2001*
The IAA's aims are the overthrow of the current Yemeni government and the establishment of an Islamic State following Sharia Law.

Islamic Jihad Union (IJU) - *Proscribed July 2005*
The primary strategic goal of the IJU is the elimination of the current Uzbek regime. The IJU would expect that following the removal of President Karimov, elections would occur in which Islamic-democratic political candidates would pursue goals shared by the IJU leadership.

Islamic Movement of Uzbekistan (IMU) - *Proscribed November 2002*
The primary aim of IMU is to establish an Islamic state in the model of the Taleban in Uzbekistan. However, the IMU is reported to also seek to establish a broader state over the entire Turkestan area.

Islamic State of Iraq and the Levant (ISIL) also known as Dawlat al-'Iraq al-Islamiyya, Islamic State of Iraq (ISI), Islamic State of Iraq and Syria (ISIS) and Dawlat al Islamiya fi Iraq wa al Sham (DAISh) and the Islamic State in Iraq and Sham - *Proscribed June 2014*
ISIL is a brutal Sunni Islamist terrorist group active in Iraq and Syria. The group adheres to a global jihadist ideology, following an extreme interpretation of Islam, which is anti-Western and promotes sectarian violence. ISIL aims to establish an Islamic State governed by Sharia law in the region and impose their rule on people using violence and extortion.

ISIL was previously proscribed as part of Al Qa'ida (AQ). However on 2 February 2014, AQ senior leadership issued a statement officially severing ties with ISIL. This prompted consideration of the case to proscribe ISIL in its own right.

ISIL not only poses a threat from within Syria but has made significant advances in Iraq. The threat from ISIL in Iraq and Syria is very serious and shows clearly the importance of taking a strong stand against the extremists.

We are aware that a number of British nationals have travelled to Syria and some of these will inevitably be fighting with ISIL. It appears that ISIL is treating Iraq and Syria as one theatre of conflict and its potential ability to operate across the border must be a cause of concern for the whole international community.

In April 2014, ISIL claimed responsibility for a series of blasts targeting a Shia election rally in Baghdad. These attacks are reported to have killed at least 31 people. Thousands of Iraqi civilians lost their lives to sectarian violence in 2013, and attacks carried out by ISIL will have accounted for a large proportion of these deaths.

ISIL has reportedly detained dozens of foreign journalists and aid workers. In September 2013, members of the group kidnapped and killed the commander of Ahrar ash-Sham after he intervened to protect members of a Malaysian Islamic charity.

In January 2014, ISIL captured the Al-Anbar cities of Ramadi and Fallujah, and is engaged in ongoing fighting with the Iraqi security forces. The group also claimed responsibility for a car bomb attack that killed four people and wounded dozens in the southern Beirut suburb of Haret Hreik.

ISIL has a strong presence in northern and eastern Syria where it has instituted strict Sharia law in the towns under its control. The group is responsible for numerous attacks and a vast number of deaths. The group is believed to attract foreign fighters, including Westerners, to the region. The group has maintained control of various towns on the Syrian/Turkish border allowing the group to control who crosses and ISIL's presence there has interfered with the free flow of humanitarian aid.

Note: The Government laid an Order in August 2014 which provides that **"Islamic State (Dawlat al Islamiya)"** should be treated as another name for the organisation which is already proscribed as ISIL. The UK does not recognise ISIL's claims of a 'restored' Caliphate or a new Islamic State.

Jaish e Mohammed (JeM) and splinter group Khuddam Ul-Islam (KuI) – *JeM, proscribed March 2001 and KuI, proscribed October 2005*
JeM and KuI seek the 'liberation' of Kashmir from Indian control as well as the 'destruction' of America and India. JeM has a stated objective of unifying the various Kashmiri militant groups.

Jamaah Anshorut Daulah - *Proscribed July 2016*

JAD was established in March 2015 following the merger of several Indonesian extremist and terrorist groups aligned to Daesh. JAD has extensive links to Daesh and actively recruits fighters in Syria.

The group is led by the imprisoned extremist cleric Aman Abdurrahman and has close ties to other terrorist groups including Daesh. Its membership includes several former Jemaah Islamiyah (JI) members. JI were responsible for the 2002 and 2005 Bali attacks.

JAD was responsible for the attack near Sarinah Mall in Jakarta in January 2016, which was claimed by Daesh and resulted in the deaths of seven people (including the five attackers) and 20 people (including five police officers) being injured.

Jamaat ul-Ahrar (JuA) - *Proscribed March 2015*

JuA is a militant Islamist group that split away from Tehrik-e-Taliban Pakistan (TTP) in August 2014. JuA aims to establish an Islamic caliphate in Pakistan and aspires to extend global jihad into the Indian subcontinent.

The group have claimed responsibility for a number of recent attacks, including on 21 November 2014, a grenade attack on the Muttahida Qaumi Movement (MQM) in Orangi Town area of Karachi that killed three members of the Sindh Assembly and injured 50 workers; on 7 November 2014, twin bombings targeting peace committee volunteers in Chinari village of Safi Tehsil in the Mohmand Agency killed at least six people. JuA's spokesman, Ehsanullah Ehsan, claimed responsibility and vowed to continue attacking tribal peace committees; and on 2 November 2014, the suicide bomber attack on the Pakistan side of Wagah border crossing, shortly after the famous flag-lowering ceremony had concluded, that killed over 60 people.

In September 2014, Ehsanullah Ehsan released a statement criticising the British Government for arresting Al Muhajiroun (ALM) associates and made a threat, stating that "your future security depends upon how nicely you treat the Muslims in Britain".

In March 2015 the group claimed responsibility for fatal attacks on Christian sites in Lahore.

Jammat-ul Mujahideen Bangladesh (JMB) - *Proscribed July 2007*
JMB first came to prominence on 20 May 2002 when eight of its members were arrested in possession of petrol bombs. The group has claimed responsibility for numerous fatal bomb attacks across Bangladesh in recent years, including suicide bomb attacks in 2005.

Jamaat Ul-Furquan (JuF) - *Proscribed October 2005*
The aim of JuF is to unite Indian administered Kashmir with Pakistan; to establish a radical Islamist state in Pakistan; the 'destruction' of India and the USA; to recruit new jihadis; and the release of imprisoned Kashmiri militants.

Jaysh al Khalifatu Islamiya (JKI) which translates as the Army of the Islamic Caliphate – *proscribed November 2014*
JKI is an Islamist jihadist group, consisting predominately of Chechen fighters. JKI is an opposition group active in Syria.

JKI splintered from Jaysh al-Muhajireen Wal Ansar (JAMWA) in 2013. At that point a number of members went with Umar Shishani (aka Umar the Chechen) to join the Islamic State of Iraq and the Levant (ISIL) and, the rest of the group stayed distinct and renamed itself Majahideen of the Caucasus and the Levant (MCL) and more recently renamed itself JKI.

Before his death in 2014, JKI was led by Seyfullah Shishani, who had pledged allegiance to the leader of the Al Nusrah Front, Mohammed Al-Jawlani. JKI has assisted ANF and ISIL in conducting attacks.

In February 2014 a British individual linked to the group carried out a suicide attack on a prison in Aleppo, resulting in prisoner escapes.

Jeemah Islamiyah (JI) - *Proscribed November 2002*
JI's aim is the creation of a unified Islamic state in Singapore, Malaysia, Indonesia and the Southern Philippines.

Jund al-Aqsa (JAA) which translates as Soldiers of al-Aqsa - *Proscribed January 2015*
JAA is a splinter group of Al Nusrah Front (ANF), active in Syria against the Syrian Government since September 2013. JAA is a foreign fighter battalion of a variety of nationalities, as well as a native Syrian contingent. The group is primarily operating in Idlib and Hama.

JAA is believed to be responsible for the attack on 9 February 2014 in Maan village killing 40 people of which 21 were civilians. JAA and Ahrar al-Sham are reported to have uploaded YouTube footage of their joint offensive against the village, although neither group has claimed responsibility.

JAA has supported the Islamic Front in an operation to seize Hama military airport during July 2014. ANF released a document summarising its operations in August 2014, which included details of an attack that targeted a resort hotel conducted in collaboration with JAA.

Jund al Khalifa-Algeria (JaK-A) which translates as Soldiers of the Caliphate - *Proscribed January 2015*
JaK-A is an Islamist militant group believed to be made up of members of dormant Al Qa'ida (AQ) cells. JaK-A announced its allegiance to the Islamic State of Iraq and Levant (ISIL) in a communiqué released on 13 September 2014.

In April 2014, JaK-A claimed responsibility for an ambush on a convoy, that killed 11 members of the Algerian army. On 24 September 2014, the group beheaded a mountaineering guide, Hervé Gourdel, a French national. The abduction was announced on the same day that a spokesman for ISIL warned that it would target Americans and other Western citizens, especially the French, after French jets joined the US in carrying out strikes in Iraq on ISIL targets.

Kateeba al-Kawthar (KaK) also known as Ajnad al-sham and Junud ar-Rahman al Muhajireen - *Proscribed June 2014*
KaK describes itself as a group of mujahideen from more than 20 countries seeking a 'just' Islamic nation.

KaK is an armed terrorist group fighting to establish an Islamic state in Syria. The group is aligned to the most extreme groups operating in Syria and has links to Al Qa'ida. The group's leader is described as a Western Mujaadid commander. KaK is believed to attract a number of Western foreign fighters and has released YouTube footage encouraging travel to Syria and asking Muslims to support the fighters.

Partiya Karkeren Kurdistani (PKK) which translates as the Kurdistan Worker's Party - *Proscribed March 2001*
PKK/KADEK/KG is primarily a separatist movement that seeks an independent Kurdish state in southeast Turkey. The PKK changed its name to KADEK and then to Kongra Gele Kurdistan, although the PKK acronym is still used by parts of the movement.

Note: The Government laid an Order in 2006 which provides that **"KADEK"** and **"Kongra Gele Kurdistan"** should be treated as alternative names for the organisation which is already proscribed as PKK.

Lashkar e Tayyaba (LT) - *Proscribed March 2001*
LT seeks independence for Kashmir and the creation of an Islamic state using violent means.

Note: The Government laid an Order in March 2009 which provides that **"Jama'at' ud Da'wa (JuD)"** should be treated as another name for the organisation which is already proscribed as Lashkar e Tayyaba.

Liberation Tigers of Tamil Eelam (LTTE) - *Proscribed March 2001*
The LTTE is a terrorist group fighting for a separate Tamil state in the North and East of Sri Lanka.

Libyan Islamic Fighting Group (LIFG) - *Proscribed October 2005*
The LIFG seeks to replace the current Libyan regime with a hard-line Islamic state. The group is also part of the wider global Islamist extremist movement, as inspired by Al Qa'ida. The group has mounted several operations inside Libya, including a 1996 attempt to assassinate Mu'ammar Qadhafi.

Liwa al-Thawra - *Proscribed December 2017*
Liwa al-Thawra is an extremist group using violent tactics against Egyptian security forces, to fight for political reform and an end to the Egyptian regime. It announced its creation on 21 August 2016 following an attack in Monofeya, Egypt. The group is responsible for assassination attempts against Egyptian officials. The group have claimed responsibility for attacks including:

- 21 August 2016 the group claimed responsibility for the attack in Monofeya, Egypt;
- 22 October 2016 the group claimed responsibility for the assassination of Egyptian Brigadier General Adel Regali; and
- On 1 April 2017 the group claimed responsibility for the bombing of the Egyptian police training centre in Tanta, Egypt.

Minbar Ansar Deen also known as Ansar al-Sharia UK - *Proscribed July 2013*
Minbar Ansar Deen is a Salafist group based in the UK that promotes and encourages terrorism. Minbar Ansar Deen distributes content through its online forum which promotes terrorism by encouraging individuals to travel overseas to engage in extremist activity, specifically fighting. The group is not related to Ansar al-Sharia groups in other countries.

Mujahidin Indonesia Timur (MIT) which translates as Mujahideen of Eastern Indonesia - *Proscribed July 2016*
MIT is Indonesia's most active terrorist group based in the mountainous jungle of Poso, in Central Sulawesi. Its leader Abu Warda, also known as Santoso, is one of Indonesia's most wanted terrorist. The group's modus operandi is to attack the police and the army which includes the use of explosives (including the use of IEDs), and shootings. MIT have been responsible for deaths of more than a dozen police officers in Poso in the last three years. They have also used kidnappings and beheadings of Christian farmers in Poso to dissuade the local populace from assisting the police.

MIT pledged its allegiance to Daesh in July 2014 and are assessed to have links to other Daesh affiliated terrorist groups in the region. MIT has claimed responsibility for a number of recent attacks and has threatened attacks on targets across the country including the capital (specifically the Jakarta police headquarters and the presidential palace in a video uploaded on 22 November 2015).

In September 2015 MIT was banned as a terrorist group by the USA and the UN.

National Action - *Proscribed December 2016*
National Action is a racist neo-Nazi group that was established in 2013. It has a number of branches across the UK, which conduct provocative street demonstrations and stunts aimed at intimidating local communities. Its activities and propaganda materials are particularly aimed at recruiting young people.

The group is virulently racist, anti-Semitic and homophobic. Its ideology promotes the idea that Britain will inevitably see a violent 'race war', which the group claims it will be an active part of. The group rejects democracy, is hostile to the British state and seeks to divide society by implicitly endorsing violence against ethnic minorities and perceived 'race traitors'.

National Action's online propaganda material, disseminated via social media, frequently features extremely violent imagery and language. It condones and glorifies those who have used extreme violence for political or ideological ends. This includes tweets posted by the group in 2016, in connection with the murder of Jo Cox (which the prosecutor described as a terrorist act), stating "only 649 MPs to go" and a photo of Thomas Mair with the caption "don't let this man's sacrifice go in vain" and "Jo Cox would have filled Yorkshire with more subhumans!", as well as an image condoning and celebrating the terrorist attack on the Pulse nightclub in Orlando and another depicting a police officer's throat being slit. The images can reasonably be taken as inferring that these acts should be emulated and therefore amount to the unlawful glorification of terrorism.

Note: The Government laid an Order in September 2017 which provides that **"Scottish Dawn"** and **"NS131 (National Socialist Anti-Capitalist Action)"** should be treated as alternative names for the organisation which is already proscribed as National Action.

Palestinian Islamic Jihad - Shaqaqi (PIJ) - *Proscribed March 2001*
PIJ aims to end the Israeli occupation of Palestine and to create an Islamic state. It opposes the existence of the state of Israel, the Middle East Peace Process and the Palestinian Authority, and has carried out suicide bombings against Israeli targets.

Popular Front for the Liberation of Palestine-General Command (PFLP-GC) - *Proscribed June 2014*
PFLP-GC is a left wing nationalist Palestinian militant organisation formed in 1968. It is based in Syria and was involved in the Palestine intifada during the 1970s and 1980s. The group is separate from the similarly named Popular Front for the Liberation of Palestine (PFLP).

From its outset, the group has been a Syrian proxy. PFLP-GC has been fighting in the Syrian war in support of Assad, including in Yarmouk Refugee Camp in July 2013. The group also issued statements in support of the Syrian government, Hizballah, and Iran.

Revolutionary Peoples' Liberation Party - Front (Devrimci Halk Kurtulus Partisi - Cephesi) (DHKP-C) - *Proscribed March 2001*
DHKP-C aims to establish a Marxist-Leninist regime in Turkey by means of armed revolutionary struggle.

Salafist Group for Call and Combat (Groupe Salafiste pour la Predication et le Combat) (GSPC) - *Proscribed March 2001*
Its aim is to create an Islamic state in Algeria using all necessary means, including violence.

Saved Sect or Saviour Sect - *Proscribed July 2006*
The Saved Sect /Al Ghurabaa is an Islamist group which seeks to establish an Islamic Caliphate ruled by Shariah law. The group first emerged as Al Muhajiroun in the UK, in 1996,

led by Omar Bakri Muhammed, who then publicly disbanded the organisation in 2004. The organisation reformed in 2004 under the names Al Ghurabaa and the Saved Sect. While the Group has some links to groups overseas, it is based and operates within the UK.

Note: The Government laid Orders, in January 2010 and November 2011, which provide that **"Al Muhajiroun", "Islam4UK", "Call to Submission", "Islamic Path", "London School of Sharia"** and **"Muslims Against Crusades"** should be treated as alternative names for the organisation which is already proscribed under the names **Al Ghurabaa** and **The Saved Sect**. The Government laid an Order, in June 2014 recognising **"Need4Khilafah"**, the **"Shariah Project"** and the **"Islamic Dawah Association"** as the same as the organisation proscribed as **Al Ghurabaa** and **The Saved Sect**, which is also known as **"Al Muhajiroun"**.

Sipah-e Sahaba Pakistan (SSP) (Aka Millat-e Islami Pakistan (MIP) - SSP was renamed MIP in April 2003 but is still referred to as SSP) and splinter group Lashkar-e Jhangvi (LeJ) - *Proscribed March 2001*
The aim of both SSP and LeJ is to transform Pakistan by violent means into a Sunni state under the total control of Sharia law. Another objective is to have all Shia declared Kafirs and to participate in the destruction of other religions, notably Judaism, Christianity and Hinduism.

Kafirs means non-believers: literally, one who refused to see the truth. LeJ does not consider members of the Shia sect to be Muslim, so concludes they can be considered a 'legitimate' target.

Note: The Government laid an Order in October 2013 which provides that **"Ahle Sunnat wal Jamaat (ASWJ)"** should be treated as another name for the organisation which is already proscribed as Sipah-e Sahaba Pakistan (SSP) and Lashkar-e Jhangvi (LeJ).

Tehrik Nefaz-e Shari'at Muhammadi (TNSM) - *Proscribed July 2007*
TNSM regularly attacks coalition and Afghan government forces in Afghanistan and provides direct support to Al Qa'ida and the Taliban. One faction of the group claimed responsibility for a suicide attack on an army training compound on 8 November 2007 in Dargai, Pakistan, in which 42 soldiers were killed.

Tehrik-e Taliban Pakistan (TTP) - *Proscribed January 2011*
Tehrik-e Taliban Pakistan has carried out a high number of mass casualty attacks in Pakistan and Afghanistan since 2007. The group have announced various objectives and demands, such as the enforcement of Sharia, resistance against the Pakistani army and the removal of NATO forces from Afghanistan. The organisation has also been involved in attacks in the West, such as the attempted Times Square car-bomb attack in May 2010.

Teyre Azadiye Kurdistan (TAK) - *Proscribed July 2006*
TAK is a Kurdish terrorist group currently operating in Turkey.

Turkestan Islamic Party (TIP) also known as East Turkestan Islamic Party (ETIP), East Turkestan Islamic Movement (ETIM) and Hizb al-Islami al-Turkistani (HAAT) - *Proscribed July 2016*
TIP is an Islamic terrorist and separatist organisation founded in 1989 by Uighur militants in western China. It aims to establish an independent caliphate in the Uighur state of Xinjiang Uighur Autonomous Region of North-western China and to name it East Turkestan. TIP is based in the Federally Administered Tribal Areas (FATA) of Pakistan, and operates in China, Central and South Asia and Syria. The group has claimed responsibility for a number of attacks

in China, the latest of these being in April 2014. TIP has links to a number of terrorist groups including Al Qa'ida (AQ).

In November 2015, TIP released the 18th issue of its magazine 'Islamic Turkestan' through the Global Islamic Media Front (GIMF), detailing TIP's jihad against the Chinese authorities. Video footage from September 2015 shows TIP hosting training camps in areas controlled by the Pakistani Taliban in North Waziristan.

More recently TIP has maintained an active and visible presence in the Syrian war and has published a number of video clips of its activities. Examples of this from March to April 2016 include:

- TIP claiming a joint attack with Jund al Aqsa in Sahl al Ghab and published a video of a suicide bomb attack in April 2016;
- a video published in March 2016 which promotes the victories of TIP in Syria and calls for Muslims to join jihad; and
- a video slide show published in April 2016 which shows fighters and children in training.

TIP has been banned by the UN and is also sanctioned by the USA under the Terrorist Exclusion list.

Turkiye Halk Kurtulus Partisi-Cephesi (THKP-C) is also known as the Peoples' Liberation Party/Front of Turkey, THKP-C Acilciler and the Hasty Ones - *Proscribed June 2014*
THKP-C is a left wing organisation formed in 1994. The group grew out of the Turkish extreme left Revolutionary Youth Movements which formed in the 1960s and 70s.

THKP-C now also operates as a pro-Assad militia group fighting in Syria and has developed increased capability since the Syrian insurgency. THKP-C is assessed to have been involved in an attack in Reyhanli, Turkey, in May 2013, killing over 50 people and injuring over 100.

The organisation has always been most prominent in the southern province of Hatay. A number of other groups have been formed under the THKP-C umbrella including 'Mukavament Suriye' (Syrian Resistance), which is reported to have been responsible for the recent Banias Massacre killing at least 145 people.

LIST OF PROSCRIBED GROUPS LINKED TO NORTHERN IRELAND RELATED TERRORISM

Continuity Army Council
Cumann na mBan
Fianna na hEireann
Irish National Liberation Army
Irish People's Liberation Organisation
Irish Republican Army
Loyalist Volunteer Force
Orange Volunteers
Red Hand Commando
Red Hand Defenders
Saor Eire
Ulster Defence Association
Ulster Freedom Fighters
Ulster Volunteer Force

ANNEX B – Items of Communications Data by Public Authority

The Intelligence Agencies

GCHQ	4156
MI5 - Non S.94	39364
SIS	453

Police Forces and Law Enforcement Agencies

Avon & Somerset Constabulary	13160
British Transport Police	2404
Cambridgeshire & Bedfordshire Constabulary	9433
Cheshire Constabulary	10761
City of London Police	4472
Cleveland Police	6861
Cumbria Constabulary	3625
Derbyshire Constabulary	5588
Devon & Cornwall Police	18300
Dorset Police	4186
Durham Constabulary	6378
Dyfed Powys Police	3386
Gloucestershire Constabulary	3387
Greater Manchester Police	40857
Gwent Police	5453
Hampshire Constabulary	10979
Hertfordshire Constabulary	12825
HMRC	12731
Humberside Police	5360
Kent & Essex SCD*	18149
Lancashire Constabulary	18517
Leicestershire Police	10126
Lincolnshire Police	3994
Ministry of Defence Police	145
Merseyside Police	25356

Metropolitan Police Directorate of Professional Standards	750
Metropolitan Police Communications Intelligence Unit	103602
Metropolitan Police Counter Terrorism Command	3360
Norfolk Constabulary & Suffolk Constabulary	6654
North Wales Police	5573
North Yorkshire Police	4560
Northamptonshire Police	7872
Northumbria Police	8744
Nottinghamshire Police	13293
Police Scotland	44158
PSNI	8228
Royal Air Force Police	49
Royal Military Police	275
Royal Navy Police	62
National Crime Agency	65212
South Wales Police	10159
South Yorkshire Police	13121
Staffordshire Police	9279
Surrey Police	9558
Sussex Police	5332
Thames Valley Police	11281
The Home Office (Immigration Enforcement)	6736
Warwickshire Police and West Mercia Police*	20933
West Midlands Police	55250
West Yorkshire Police	30054
Wiltshire Police	5412

Other Public Authorities

Total items of data	
Competition and Markets Authority	87
Criminal Cases Review Commission	6
Department of Enterprise, Trade and Investment (Based in NI) - Northern Ireland Trading Standards Service	201
Department of Health - MHRA	329
Department of Work & Pensions - Child Maintenance Group (CMG)	36
Financial Conduct Authority	2347
Gambling Commission	19
Gangmasters Licensing Authority	68
Health & Safety Executive	5
HMPS NOMS	120
Information Commissioner's Office	89
IPCC	55
Maritime & Coastguard Agency	15
NHS Protect	10
Ofcom	3
Police Ombudsman for Northern Ireland	6
Serious Fraud Office	526
National Anti-Fraud Network	724

The following "other" public authorities reported that they did not acquire any communications data during 2016:

- Department for Transport - Air Accident Investigation Branch
- Department for Transport - Marine Accident Investigation Branch
- Department for Transport - Rail Accident Investigation Branch
- NHS Scotland
- NI Health & Social Services Central Services Agency (Was Central Services Agency)
- Northern Ireland Office (NIPS)
- Police Investigations Review Commissioner
- Prudential Regulation Authority
- Scottish Criminal Cases Review Commission
- No Fire Authority
- No Ambulance Service or Trust

Local Authorities, through the National Anti-Fraud Network

Local Authority	Total items of data
Bath & North East Somerset Council	10
Bedford Borough Council	3
Birmingham City Council	43
Bracknell Forest Borough Council	23
Bristol City Council	22
Buckinghamshire County Council	4
Bury Metropolitan Borough Council	3
Caerphilly County Borough Council	13
Cambridgeshire County Council	37
Cardiff Council	9
Cheshire West & Chester Council	22
Cornwall Council	1
Derbyshire County Council	6
Devon County Council	5
Doncaster Metropolitan Council	8
Dover District Council	21
Durham County Council	6
East Riding of Yorkshire Council	3
Flintshire County Council	2
Gateshead Metropolitan Borough Council	9
Halton Borough Council	2
Hampshire County Council	16
Hertfordshire County Council	4
Kent County Council	50
Lancashire County Council	24
Leicestershire County Council	12
Lincolnshire County Council	2

London Borough of Brent Council	4
London Borough of Bromley Council	21
London Borough of Camden Council	4
London Borough of Croydon Council	3
London Borough of Enfield Council	57
London Borough of Islington Council	11
London Borough of Lambeth Council	9
London Borough of Newham Council	4
London Borough of Wandsworth Council	11
Newport City Council	11
Norfolk County Council	2
North Kesteven District Council	5
North Lanarkshire Council	3
North Lincolnshire Council	12
North Yorkshire County Council	20
Northumberland County Council	3
Nottinghamshire County Council	20
Oldham Metropolitan Borough Council	1
Plymouth City Council	5
Preston City Council	2
Redcar & Cleveland Borough Council	16
Rhondda Cynon Taff County Borough Council	12
Slough Borough Council	2
South Gloucestershire Council	2
Staffordshire County Council	11
Stockton On Tees Borough Council	6
Stoke on Trent City Council	32
Suffolk County Council	6
Surrey County Council	17
Thurrock Borough Council	7

Torbay Borough Council	4
Warrington Borough Council	8
West Berkshire Council	2
West Sussex County Council	3
Worcestershire County Council	3
York City Council	25

The following local authorities made applications but acquired no data:

- Barnsley Metropolitan Council
- City of London Corporation
- Cumbria County Council
- East Sussex County Council
- Elmbridge Borough Council
- Gloucestershire County Council
- London Borough of Barking & Dagenham Council
- London Borough of Merton Council
- Mole Valley District Council
- Oxfordshire County Council
- Sheffield City Council
- St. Helens Metropolitan Borough Council
- Tewkesbury Borough Council
- Wakefield Metropolitan District Council
- Warwickshire County Council
- Watford Borough Council
- Wiltshire Council

ANNEX C – Decisions made in cases at the Investigatory Powers Tribunal, 2011-2016

Year	New Cases Received	Cases Decided	Decision Breakdown
2011	180	196	86 (44%) were ruled as 'frivolous or vexatious'
			72 (36%) received a 'no determination' outcome
			20 (10%) were ruled out of jurisdiction
			11 (6%) were ruled out of time
			3 (2%) were withdrawn
			2 (1%) were judged to be not a valid complaint
			2 (1%) were found in favour
2012	168	191	100 (52.5%) were ruled as 'frivolous or vexatious'
			62 (32.5%) received a 'no determination' outcome
			14 (7%) were ruled out of jurisdiction
			9 (5%) were ruled out of time
			5 (2.5%) were withdrawn
			1 (0.5%) were judged to be not a valid complaint
2013	205	161	85 (53%) were ruled as frivolous or vexatious
			50 (31%) received a 'no determination' outcome
			17 (10%) were ruled out of jurisdiction, withdrawn or not valid
			9 (6%) were ruled out of time
2014	215	201	104 (52%) were ruled as frivolous or vexatious
			53 (26%) received a 'no determination' outcome
			36 (18%) were ruled out of jurisdiction, withdrawn or not valid
			8 (4%) were ruled out of time
2015	251[37]	219	101 (47%) were ruled as frivolous or vexatious
			65 (30%) received a 'no determination' outcome
			38 (17%) were ruled out of jurisdiction, withdrawn or not valid
			7 (3%) were ruled out of time
			8 (4%) were found in favour
2016	209[38]	230	120 (52%) were ruled as frivolous or vexatious
			58 (25%) received a 'no determination' outcome
			26 (11%) were ruled out of jurisdiction, withdrawn or not valid
			11 (5%) were ruled out of time
			15 (7%) were found in favour

[37] Plus 367 from the Privacy International worldwide campaign; 618 in total

[38] Plus 297 from the Privacy International worldwide campaign; 506 in total

HM Government

ISBN 978-1-5286-0719-3
CCS0418538240