HM Government

HM Government Transparency Report 2015: Disruptive and Investigatory Powers

Cm 9151

HM Government Transparency Report 2015: Disruptive and Investigatory Powers

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

November 2015

Cm 9151

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

Print ISBN 9781474125611
Web ISBN 9781474125628

ID 27101501 11/15 51973 19585

Printed on paper containing 75% recycled fibre content minimum

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

Foreword

The Government is committed to increasing the transparency of the work of our intelligence, security and law enforcement agencies. But it is essential that this is done without damaging national security or effective law enforcement and, as a result, public safety.

The Government has a strong track record of enhancing transparency in this area. We have supported the strengthening of a number of powerful independent oversight bodies. This includes the giving of greater powers to the Intelligence and Security Committee. The report of that Committee into the murder of Fusilier Lee Rigby, published in November 2014, and their Privacy and Security Report, published in March, provide powerful examples of the rigorous scrutiny that is applied to the activities of our intelligence agencies, and the extent to which the details of this scrutiny are made public. As the Prime Minister said in his statement to the House of Commons on 25 November 2014 "few countries in the world would publish this degree of detail about the activities of their security services".

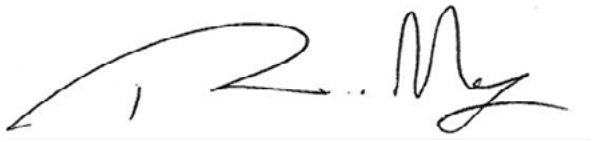
In addition, in 2014 the Government asked the Independent Reviewer of Terrorism Legislation, David Anderson QC, to conduct a review of the operation and regulation of law enforcement and intelligence agency investigatory powers, with specific reference to the interception of communications and the separate issue of communications data. David Anderson's report was published on 11 June. This report set out a comprehensive assessment of the intelligence agencies' capabilities and the legal and privacy frameworks that govern their use.

The Government has been clear about the need for legislation in order for law enforcement and the intelligence agencies to keep pace with an evolving threat and a changing communications environment, and has today brought forward a draft Bill for pre-legislative scrutiny. We have carefully considered the findings of David Anderson and the Intelligence and Security Committee, as well as the recent report of the Royal United Services Institute into the UK's surveillance programmes, which together form a firm basis for consultation on legislation.

Additional resources have also been given to the Intelligence Services Commissioner so that he is better able to engage with the public. And we have worked with the Interception of Communications Commissioner's Office to enhance what statistics will be collected in the future, and published, in relation to public authorities' use of communications data.

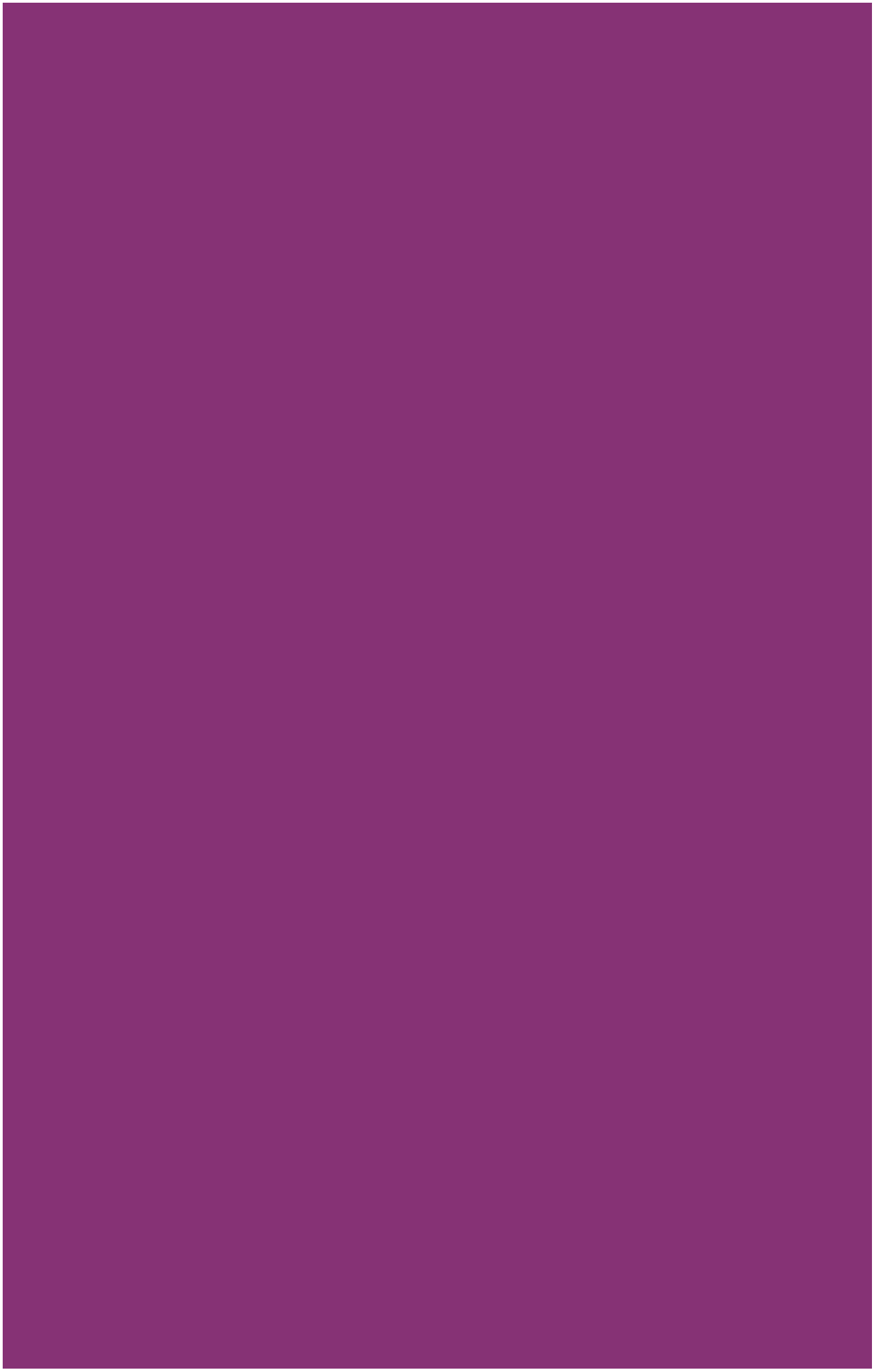
All of this activity and more shows that where we can give the public more information, we do. However, we are not complacent and recognise that more can be done. In particular, we need to ensure that we reach out and explain to the public information that has already been made available, both in relation to the threats that we face and what we do to counter them. The latest annual report of the Interception of Communications Commissioner, published in March, provides a great example of this, ensuring information is understandable and dealing directly with public concerns. Equally, the most recent report by the current Intelligence Services Commissioner, Sir Mark Waller, provided greater openness than ever before.

Our commitment to doing more to enhance transparency in this way is why we committed to produce this report. It includes, for the first time, a consolidated picture of the use, regulation and oversight of a wide range of disruptive and investigatory techniques that are crucial to keeping the public safe.



Theresa May MP
Home Secretary

Contents



2 – Introduction

The latest Annual Report on the United Kingdom's strategy for countering terrorism, CONTEST, was published on 23 March 2015. That report makes clear that 2014 was an exceptionally challenging period for counter-terrorism in the UK. It was also a period in which terrorist tactics changed. Some groups continued to aspire to large scale attacks. However, others now advocate simple attacks that can be conducted by individuals acting alone, which is fuelled by unprecedented levels of terrorist propaganda. The changing threat stems from the conflict in Syria and Iraq and is connected to groups such as the Islamic State of Iraq and the Levant (ISIL). These developments prompted the Joint Terrorism Analysis Centre (JTAC) to raise the threat level from SUBSTANTIAL to SEVERE on 29 August 2014. This means that a terrorist attack in the UK is now judged to be highly likely.

Equally, serious and organised crime continues to constitute a threat to our national security and the 2014 Annual Report on the Government's Serious and Organised Crime Strategy was also published on 23 March 2015. Serious and organised crime costs the United Kingdom at least £24 billion each year, leads to loss of life and can deprive people of their security and prosperity. Organised crime is wide ranging and includes drugs trafficking, human trafficking, high value fraud, other financial crime and cyber crime. These crimes damage communities, destabilise financial markets, threaten the security of our borders and undermine confidence in communications technology and the online economy.

Espionage also continues to pose a threat to British interests. Cyber espionage in particular has posed an increasing threat over recent years, with new technologies enabling espionage to take place on an almost industrial scale in some cases. In light of the threats that we face, it is crucial that we have the powers we need to counter them and that they are used in an appropriate and proportionate way.

This is a new report, which will be published on an annual basis, explaining tools the Government and the intelligence and law enforcement agencies use to counter the threat from terrorism and serious and organised crime, as well as other threats to our national security.

The report is split into two main sections. The first includes figures on the use of disruptive and investigatory powers, explains their utility and outlines the legal frameworks that ensure they can only be used when necessary and proportionate. The second section explains the roles of the Commissioners, and other bodies, that provide independent oversight and scrutiny of the use of these tools.

There remain limits to what can be said publically about the use of certain sensitive techniques, and particularly the work of the intelligence agencies, because to do so could aid criminals and terrorists to change their behaviour in order to evade detection. We have seen significant evidence of this following the allegations made by Edward Snowden.

As Sir Iain Lobban, former Director of GCHQ, told the Intelligence and Security Committee on 7 November 2013 "We have actually seen chat around specific terrorist groups, including close to home, discussing how to avoid what they now perceive to be vulnerable communications methods or how to select communications which they now perceive not to be exploitable."[1]

However, it is vital the public have both the confidence that the intelligence and law enforcement agencies have the powers needed and that those powers are used proportionately. These agencies rely on many members of the public to provide support in their work. If the public do not trust the police and intelligence agencies, then that will have a real operational impact.

This report therefore ensures that the public are able to access, in one place, a guide to a range of 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 guard against their abuse.

1 Transcript of Evidence, Open Evidence Session, Intelligence and Security Committee, 7 November 2013, page 17, http://isc.independent.gov.uk/news-archive/7november2013-1

3 – The Counter-Terrorism and Security Act 2015

The Counter-Terrorism and Security Act received Royal Assent on 12 February 2015.[2] This legislation created new powers that are urgently needed by our intelligence and law enforcement agencies, in order to counter the terrorist threat we face from organisations such as ISIL.

The powers in the Act will ensure that we can better disrupt the ability of individuals to travel abroad to fight for terrorist organisations or engage in terrorism-related activity, as well as to control their ability to return to the United Kingdom. These powers also enhance capabilities to monitor and control the actions of those in the UK who pose a threat to national security; and to prevent individuals from being radicalised in the first instance. The Act includes discrete measures in a number of areas:

In relation to disrupting travel:

- Providing the police with a power to seize a passport at the border temporarily, during which time they will be able to investigate the individual concerned.
- Creating Temporary Exclusion Orders that can temporarily disrupt the return to the UK of a British citizen suspected of involvement in terrorist activity abroad – ensuring that when individuals do return, it is done in a manner which we control.
- Enhancing our border security arrangements for aviation, maritime and rail travel, with provisions relating to passenger data, 'no fly' lists, and security and screening measures. These will help us to enforce our stringent requirements effectively with carriers that provide transport to and from the UK.

To deal with those returning to or already in the UK:

- Enhancing existing Terrorism Prevention and Investigation Measures, including the ability to relocate a TPIM subject, and a power to require them to attend meetings as part of their ongoing management e.g. with the probation service or JobCentre Plus staff.

To support those at serious risk of succumbing to radicalisation:

- Creating a general duty on a range of specified authorities to have due regard to preventing people from being drawn into terrorism.
- Putting Channel – the voluntary programme for people at risk of radicalisation – on a statutory basis (and allowing us to do likewise for its equivalent programme in Scotland through secondary legislation).

---

2 The Counter-Terrorism and Security Act is available at http://services.parliament.uk/bills/2014-15/counterterrorismandsecurity/documents.html

And to help disrupt the wider activities of these terrorist organisations:

- Enabling the retention of additional information by communications service providers in order to attribute an Internet Protocol address to a specific individual, enhancing vital investigative capabilities.
- Amending existing law to ensure that UK-based insurance firms cannot inadvertently provide cover for the payment of terrorist ransoms, which subsequently fund further terrorist activity, by third parties.

The Act also clarifies the law relating to where goods may be examined and the examination of goods comprising postal items under Schedule 7 to the Terrorism Act 2000.

This report focuses on the exercise of pre-existing powers. As the Counter-Terrorism and Security Act only completed its Parliamentary passage in this calendar year this report does not, therefore, include a detailed explanation of the exercise of its provisions. We expect that the Government's 2016 Transparency Report will include details of the operation of the powers the legislation has created, as well as an explanation of how the use of these powers is safeguarded and overseen.

4 – Terrorism Arrests and Outcomes

Conviction in a court is the most effective tool we have to stop terrorists. 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 2015,[3] there were 299 persons arrested for terrorism-related offences, an increase of 31% from the 229 arrests the previous year. The recent rise was driven by an increase in the number of arrests across all age groups (except 25-29 year olds), most notably 18-20 year olds, which more than doubled from 20 to 43. There was also an increase of 35% in the number of persons arrested for international-related terrorism.

Of the 299 arrests, 118 (39%) resulted in a charge and 85% of these charges, relating to 100 individuals, were considered to be terrorism-related. Many of these cases will be ongoing. Therefore, the number of charges from the 299 arrests in 2014/15 can be expected to rise over time.

Of the 100 people charged with terrorism-related offences, 35 have been prosecuted and 62 are awaiting prosecution. Of the 35 prosecution cases, 33 individuals have been convicted of an offence: 31 for terrorism-related offences and 2 for non-terrorism-related offences.

As at 31 March 2015, there were 192 persons in custody in Great Britain for terrorism-related offences and domestic extremism/separatism. This total comprised of 122 persons in custody for terrorism-related offences and 70 persons in custody for domestic extremism/separatism.

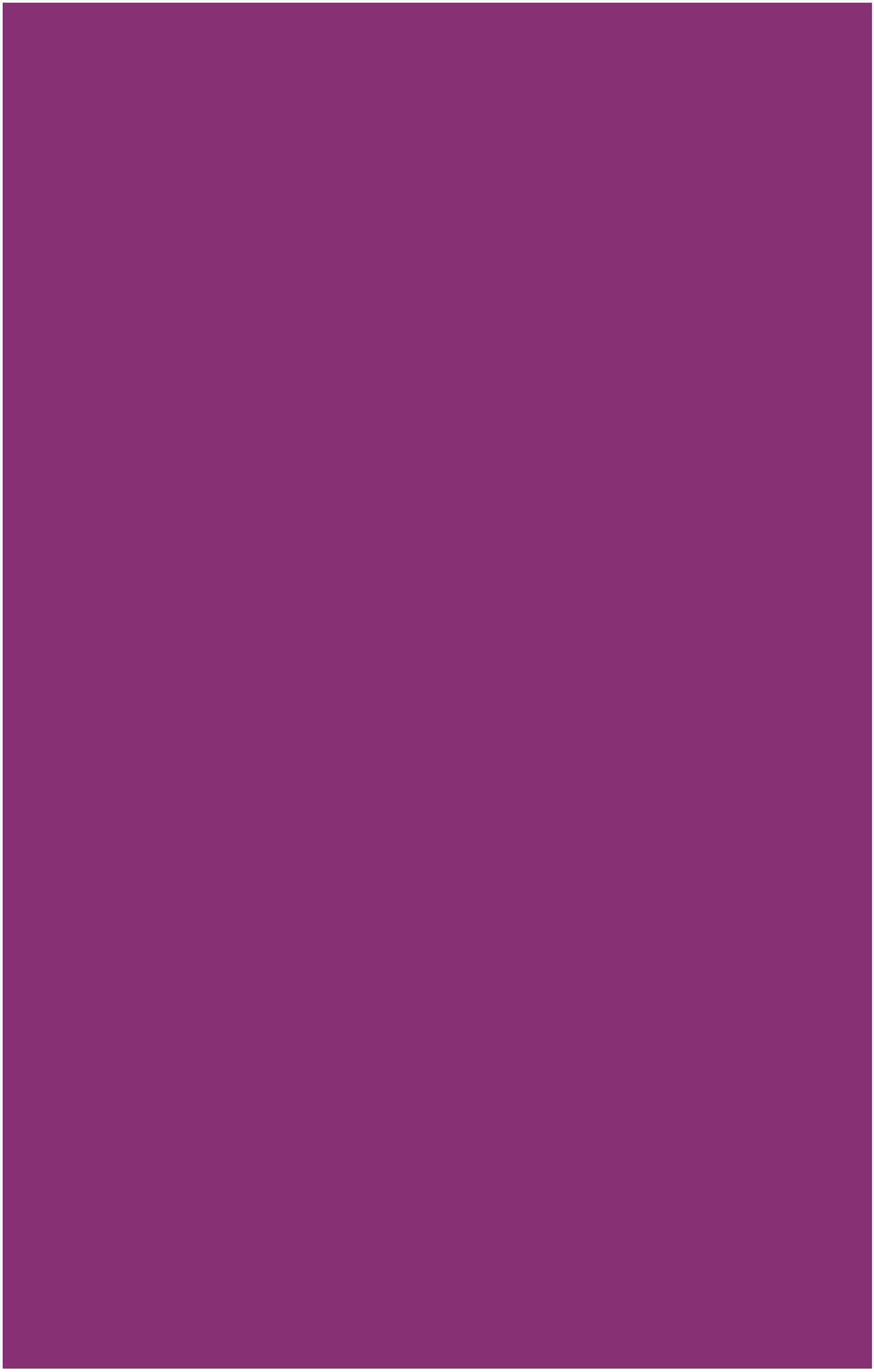
This was an increase of 38 persons compared with the situation as at 31 March 2014. This rise was driven by an increase in the number of domestic extremist prisoners (following the convictions of a number of individuals following English Defence League (EDL) rallies) and, to a lesser extent, an increase in the number of terrorism-related prisoners.[4] Terrorism arrests and outcomes are often highly reliant on the investigatory powers and tools outlined in this report.

Figure 1: summary of key activity in relation to those arrested in connection with terrorism-related offences in the year ending 31 March 2015

Terrorism-related arrests	Terrorism-related charges	Convicted (following a terrorism-related charge)	Convicted: terrorism-related	Convicted: non-terrorism-related
299	100	33	31	2

[3] All figures in this section are correct as at 8 July 2015.

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



5 – Serious and Organised Crime Arrests and Outcomes

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

The NCA published its second Annual Report in July 2015.[5] This report explained the NCA's response to the threat we face from serious and organised crime. Some key measurable outcomes from this activity are below.

It should be noted that these figures only provide an indication of the response to serious and organised crime by UK law enforcement and intelligence agencies. The National Crime Agency was established to lead the UK's overall effort to tackle serious and organised criminality. However, this effort also involves the work of a wide range of other public authorities, including the Police, 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 and prosecute those responsible. In the period from April 2014 to March 2015, 2,171 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 475 UK convictions in relation to NCA casework and 907 disruptions. NCA activity also contributed to 1,219 arrests overseas.

Interdictions

Between April 2014 and March 2015, activity by the NCA resulted in the interdiction of dangerous drugs, including 148.9 tonnes of cannabis, 70.8 tonnes of cocaine, 13.6 tonnes of opium and 4 tonnes of heroin. In addition, during this period NCA activity resulted in the seizure of 138 guns and 765 other firearms.

Criminal Finances

In the period from April 2014 to March 2015 the NCA recovered assets worth £24.4 million. In addition, they denied assets of £43.3 million. Asset denial activity included cash seizures, restrained assets, frozen assets, and the value of confiscation and civil recovery orders.

Child Protection

In the period from April 2014 to March 2015, NCA activity led to 211 children being protected and a further 1,570 children being 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

[5] See www.nationalcrimeagency.gov.uk/publications

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.

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

6 – Disruptive Powers

It is not always possible to prosecute or deport terrorists and other individuals who threaten our national security. For example, where there is not enough evidence to advance a prosecution, or where there are concerns about an individual's treatment were they to be deported back to their home country.

It is therefore vital that the Government has the tools it needs to ensure the activities of individuals who pose a threat to our national security can be effectively disrupted.

This section of the report explains key disruptive powers the Government uses to keep the public safe, including details of their use and how this is limited by stringent safeguards.

6.1 – 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 a powerful disruptive tool in the prevention of terrorism.

Section 47(a) of the Terrorism Act 2000 (TACT) enables a senior police officer to authorise searches in specified areas or places, where they reasonably suspect that an act of terrorism is going to take place. Any authorisation must be considered necessary to prevent such an act and must only cover the area and time period considered necessary to do so.

An authorisation under section 47(a) enables any constable in uniform to stop and search a vehicle (and any person in that vehicle), or a pedestrian, for the purpose of discovering whether there is anything that might constitute evidence that the vehicle concerned is being used for the purpose of terrorism, or that a relevant person is or has been concerned in the commission, preparation or instigation of acts of terrorism. This power may be exercised whether or not the constable reasonably suspects that such evidence exists.

Since coming into force, no searches have been made in Great Britain under section 47(a). This reflects the fact that these powers may only be used where it is reasonably suspected that an act of terrorism is going to take place.

Under section 43 of TACT, police officers have further powers to stop and search a suspect. A police officer may only exercise their power under this section where they reasonably suspect that a person is involved in activity related to terrorism.

In the year ending 31 March 2015, 411 persons were stopped and searched by the Metropolitan Police Service under section 43 of TACT. This represents a 9% decrease from

the previous year's total of 450. In the year ending 31 March 2015, the arrest rate of those stopped and searched under section 43 was 7%, which is the same as the previous year.[6]

6.2 – 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 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.

Examinations are not simply about the police talking to individuals who are already known or suspected of being involved in terrorism. They 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 use of Schedule 7 is based on the current terrorist threat to the UK, meaning certain routes are given greater focus. Self-defined members of ethnic minority communities do comprise a majority of those examined under Schedule 7. 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 his report[7] published in July 2014 the Independent Reviewer of Terrorism Legislation, David Anderson QC, stated:

"As in previous years, I have no reason to believe that Schedule 7 powers are exercised in a racially discriminatory way."

The statutory Code of Practice for examining officers provides guidance on the selection of individuals for examination. Selection should be based on the threat posed by the various terrorist groups active in and outside the UK, on the basis of informed considerations. Selection can be informed by 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.

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 Schedule 7, obligations under Schedule 7, key points of the Code of Practice including an individual's rights and relevant contact details (including those needed to provide feedback or make a complaint).

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

7 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2014/07/Independent-Review-of-Terrorism-Report-2014-print2.pdf

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 Terrorism Act 2000.

The Anti-social Behaviour, Crime and Policing (ASBCP) Act 2014 made amendments to Schedule 7 to reduce the potential for the power to be operated in a way that might interfere with individuals' rights unnecessarily or disproportionately, whilst still retaining the operational effectiveness of the provisions to protect the public from terrorism.[8] The changes made to Schedule 7 by the ASBCP Act 2014 were:

- reducing the maximum period of examination from nine to six hours;
- extending to individuals detained at a port the statutory rights to have a person informed of their detention and to consult a solicitor privately;
- ensuring access to legal advice for all individuals examined for more than one hour;
- clarifying that the right to consult a solicitor includes consultation in person;
- introducing statutory review of the need for continued detention;
- introducing a statutory requirement for training of examining and reviewing officers;
- establishing a statutory basis for undertaking strip searches to require suspicion that the person is concealing something which may be evidence that the person is involved in terrorism and a supervising officer's authority;
- repealing the power to seek intimate samples (e.g. blood, semen); and
- providing expressly that an examining officer may make and retain a copy of information obtained or found in the course of an examination.

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. This is an important tool, as those engaged in terrorist-related activity can use goods to plan, finance, train, and commit their attacks. The Counter-Terrorism and Security Act 2015 (CTSA) clarified the legal position in relation to:

- the examination of goods in remote storage outside the immediate boundary of a port; and
- the examination of goods comprising items of post.

To reflect the changes made by both the ASBCP and CTSA, the Schedule 7 Code of Practice was updated. The most up to date version of the Code came into effect on 25 March 2015.[9]

Statistics on the operation of Schedule 7 powers are published by the Home Office on a quarterly basis.[10] In the year ending 31 March 2015, a total of 31,769 individuals were examined at ports under Schedule 7, a fall of 28% on the previous year.

---

8 The Anti-social Behaviour, Crime and Policing Act 2014 is available at www.legislation.gov.uk/ukpga/2014/12/contents/enacted

9 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

10 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

In total, in the year ending 31 March 2015, 1,311 persons were detained during a Schedule 7 examination. This figure is higher than the 517 persons who were detained in the previous year. The increase in the number of detentions follows the introduction of the ASBCP Act, which amended Schedule 7 to ensure that mandatory detention takes place where an examination lasts for more than one hour. This requirement ensures examinees' detention is safeguarded; the statutory review of detention process begins after one hour, and detainees have the right to legal advice for examinations which take longer than one hour. Introducing mandatory detention ensures examinees receive that which they are entitled to.

Of those individuals that were detained, 35% categorised themselves as Asian or Asian British. The next most predominant ethnicity groups were Chinese or Other at 27% and Black or Black British at 12%. The proportion of those that categorised their ethnicity as White or Mixed made up 11% and 6% respectively. 9% chose not to define their ethnicity.

The total number of Schedule 7 examinations should be viewed in the context of approximately 118.7 million arrivals in the UK in the year ending 31 March 2015. This means that during this reporting period, approximately 3 persons were examined out of every 10,000 persons passing through UK ports.

6.3 – Terrorist Asset-Freezing

The UK terrorist asset-freezing regime 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 can be exercised in cases where a criminal prosecution is not possible and to prevent asset flight when suspects are arrested, provided the statutory test is met.

The UK asset-freezing regime meets obligations placed on the UK by Resolutions of the UN Security Council and associated EC Regulations. It is implemented by the Terrorist Asset-Freezing etc Act 2010 (TAFA).[11]

TAFA gives the Treasury the power to impose financial restrictions on individuals and groups believed to be involved in terrorism, whether in the UK or abroad. These restrictions have the effect of freezing any funds or assets in the UK belonging to the designated person or entity and making it an offence for any person to make funds, financial services or economic resources available 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 overseas agencies to identify possible targets, although this is unusual.

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 or acting on behalf of someone who is, or has been, involved

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

in terrorist activity. Under section 2(1)(b), a designation may only be made where the Treasury considers it necessary for purposes connected with protecting members of the public 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, 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 freeze, ensuring that human rights are taken account of, whilst also ensuring that funds are not diverted to terrorist purposes;
- designations expire after a year unless reviewed and renewed. The Treasury may only renew a designation where the requirements under section 2(1)(a) and (b) of the Act 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 of TAFA is met. Conditions are that either: the individual is under 18; or it is in the interests of national security or justice for only certain people to be informed of the designation; or for reasons connected with the prevention or detection of serious crime;
- 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 the Act (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, David Anderson QC may conduct a review of the operation of the Terrorist Asset Freezing etc. Act 2010; and
- 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.

In addition to the UK's domestic terrorist asset-freezing regime under TAFA, the Government is also responsible for the UK's operation of the UN Al-Qaida and EU terrorist asset-freezing regimes. The UN terrorist asset-freezing regime specifically targets Al-Qaida. UN Al-Qaida asset freezes are approved by all Security Council members and are listed centrally by the UN. These freezes apply in all UN Member States and a travel ban is also applied to those listed. Under the UN Al-Qaida asset-freezing regime, the Treasury has responsibility for licensing and compliance with the regime in the UK under the Al-Qaida (Asset-Freezing) Regulations 2011.

EU terrorist asset freezes relate to external terrorist threats to the EU. Under EU Common Position 931 (EU CP931), such asset freezes can only be applied to persons who are external to the EU; home-grown terrorists not linked to groups outside the EU cannot have their assets frozen under this regime. Under this regime, the EU has responsibility for designations and the Treasury has responsibility for licensing and compliance with the regime in the UK under Part 1 of TAFA. UK operation of this regime takes place under EU Regulations (EC) 2580/2001.

The most recent quarterly publication by the Treasury on the operation of the UK's asset-freezing regime covers the period from 1 April 2015 to 30 June 2015. Under TAFA, as at 30 June 2015, there was £39,000 of assets frozen, covering 49 accounts in the UK. This includes 11 accounts that were frozen during this reporting period. At the end of the reporting period, there were a total of 30 extant designations. There were no new designations during this reporting period.

In addition, as at 30 June 2015, under the EU asset-freezing regime, there were £11,000 of assets frozen, covering 10 accounts. This figure does not duplicate funds frozen under TAFA. Under the EU regime, no new accounts were frozen or unfrozen during this reporting period.

Under the UN asset-freezing regime, there was £53,000 of assets frozen as at 30 June 2015, across 21 accounts. No new accounts were frozen during this reporting period and four accounts were unfrozen.

Other key figures from this reporting period are at **ANNEX A**.[12]

Over the course of the full year from 1 July 2014 to 30 June 2015, and covering the UN, EU and UK terrorist asset-freezing regimes, there were 36 new accounts frozen and 35 accounts that were unfrozen. In addition, over the course of the year, there were 45 new designations and 24 delistings.

6.4 – 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. These measures can include: overnight residence requirements, including relocation to another part of the UK; daily 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.

[12] 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

The use of TPIMs is subject to stringent safeguards in existing legislation. Before the Secretary of State decides to impose a TPIM notice on an individual, she 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).[13] 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");
- some or all of the relevant activity is new terrorism-related activity;
- 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.

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) 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 has also published factors she considers appropriate to take into account when considering whether to relocate a subject under the travel measure.[14] These are: the need to prevent or

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

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

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 Independent Reviewer of Terrorism Legislation, David Anderson QC, has a statutory duty to review the Terrorism Prevention and Investigation Measures Act 2011. He has, to date, published an annual report setting out an assessment of the use of the power and any recommendations to improve its use, though changes made to the Independent Reviewer's remit through the Counter-Terrorism and Security Act 2015 allow for a more flexible arrangement in respect of the frequency of this review.[15]

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 her TPIM powers.

The most recent report covers the period from 1 June 2015 to 31 August 2015. As at 31 August 2015, there were three TPIM notices in force, two of which related to a British citizen. There were no extensions, revocations or revivals of TPIM notices between 1 June 2015 and 31 August 2015. There were 10 variations made to measures specified in TPIM notices during the reporting period and no applications to vary measures were refused. Two TPIM subjects were relocated during this period.[16]

6.5 – Royal Prerogative

The Royal Prerogative is an important tool used to disrupt individuals who seek to travel abroad 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.

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.

On 25 April 2013, the Government redefined the public interest criteria to refuse or withdraw a passport in a Written Ministerial Statement to Parliament.[17] The Statement provides that:

"There is no entitlement to a passport and no statutory right to have access to a passport. The decision to issue, withdraw or refuse a British passport is at the discretion of the Secretary of State for the Home Department (the Home Secretary) under the Royal Prerogative.

15 David Anderson's latest annual report on the operation of TPIMs in 2014 is available at https://terrorismlegislationreviewer.independent.gov.uk/category/reports/

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

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

This Written Ministerial Statement updates previous statements made to Parliament from time to time on the exercise of the Royal Prerogative and sets out the circumstances under which a passport can be issued, withdrawn, or refused. It redefines the public interest criteria to refuse or withdraw a passport.

A decision to refuse or withdraw a passport must be necessary and proportionate. The decision to withdraw or refuse a passport and the reason for that decision will be conveyed to the applicant or passport holder. The disclosure of information used to determine such a decision will be subject to the individual circumstances of the case.

The decision to refuse or withdraw a passport under the public interest criteria will be used only sparingly. The exercise of these criteria will be subject to careful consideration of a person's past, present or proposed activities. For example, passport facilities may be refused to or withdrawn from British nationals who may seek to harm the UK or its allies by travelling on a British passport to, for example, engage in terrorism-related activity.

These may include individuals who seek to engage in fighting, extremist activity or terrorist training outside the United Kingdom, for example, and then return to the UK with enhanced capabilities that they then use to conduct an attack on UK soil. The need to disrupt people who travel for these purposes has become increasingly apparent with developments in various parts of the world."

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:

"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."

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 abroad.

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.

Following the Secretary of State's statement in April 2013, the Royal Prerogative was used six times in 2013 and 24 times in 2014. These figures refer to occasions where an individual's passport was either revoked or their application for a passport was withdrawn on public interest grounds.

6.6 – National Security Exclusions

The Secretary of State (normally the Home Secretary) may decide to exclude an individual who is not a British Citizen if she considers their presence in the UK is not conducive to the public good. The Government condemns all those whose behaviours and views run counter to our shared values and will not stand for extremism in any form.

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.

Between 11 May 2010 and 31 December 2014, the Government has excluded 155 people from the United Kingdom, including 61 exclusions on National Security grounds. There were 41 exclusions made between 1 January 2014 and 31 December 2014.[18]

The Secretary of State will use exclusion powers when justified and based on all available evidence. In all matters the Secretary of State must act reasonably, proportionately and consistently. Its use must be consistent with the Human Rights Act 1998. Exclusion powers are very serious and the Government does not use them lightly.

6.7 – 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.

The Secretary of State may deprive 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.

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);
- war crimes; and
- serious and organised crime.

Last year, by means of the Immigration Act 2014, the Government introduced a power whereby in a small subset of 'conducive' cases – where the individual has naturalised as a British citizen and conducted themselves 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. 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.

18 Figures derived from internal Home Office information.

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 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 May 2010 and the end of December 2014, 28 people were deprived of British citizenship on the basis that to do so was 'conducive to the public good'. Four of those people were deprived of British citizenship between 1 January 2014 and 31 December 2014.[19]

6.8 – 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 terrorist-related activities. Where there are concerns for an individual's safety on return, government-to-government assurances are used to achieve deportation in accordance with the UK's human rights obligations.

Deportation 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, including 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.

However, the Government believes that it is absurd that the deportation of foreign nationals can take so many years and cost the taxpayer so much money. In particular, cases where we and the Courts agree that they pose a significant threat to national security. We are taking steps, including through the Immigration Act 2014,[20] to put this right. We have also asked the Independent Reviewer of Terrorism Legislation, David Anderson QC, to review the legal framework of DWA to examine whether the process can be improved, including by learning from the experiences of other countries.

The UK currently has functioning DWA arrangements with Algeria, Jordan, Lebanon, Ethiopia and Morocco.

A total of 12 people have been removed from the UK under DWA arrangements.[21]

19 Figures derived from internal Home Office information

20 The Immigration Act 2014 is available at www.legislation.gov.uk/ukpga/2014/22/contents

21 Figures derived from internal Home Office information.

6.9 – Proscription

Proscription is an important tool that enables 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 she 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 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 to interfere seriously with or to disrupt seriously 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 the Secretary of State will take into account when deciding whether or not to exercise the discretion to proscribe. These discretionary factors are:

- 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
- 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)); and

- wear clothing or carry or display articles in public in such a way or in such circumstances as to 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 consideration 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).[22]

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 the appeal is allowed, 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.

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.

There are currently 67[23] international terrorist organisations proscribed under the Terrorism Act 2000. In addition, there are 14 organisations in Northern Ireland that were proscribed under previous legislation.

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 B**.

---

22 The Proscribed Organisations (Applications for Deproscription etc) Regulations 2006 (SI 2006/2299) are available at www.legislation.gov.uk/uksi/2006/2299/made

23 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'.

6.10 – Tackling Online Extremism

Terrorist groups make extensive use of the internet to spread their messages, through a growing social media presence and compelling propaganda designed to reach a wide audience. This material can directly influence people who are vulnerable to radicalisation and tip them into acceptance of undertaking violent acts.

This Government takes the threat from online terrorist and extremist propaganda very seriously. In order to tackle this challenge, we are working to restrict access to such content. We have a robust yet balanced approach that involves working with industry, law enforcement and the public. This is in line with the recommendations of the Prime Minister's Extremism Task Force, which published a report on tackling radicalisation and extremism in December 2013.[24] The Task Force was established in the wake of the murder of Fusilier Lee Rigby, in order to agree practical steps the Government can take to fight against all forms of extremism.

The police Counter Terrorism Internet Referral Unit (CTIRU) is responsible for referring content, which breaches UK Terrorism legislation, to industry. Since the CTIRU was established in February 2010, they have secured the removal of more than 110,000 pieces of unlawful terrorist-related content, which encourages or glorifies acts of terrorism. 75% of these have been removed since the Extremism Task Force reported in December 2013.

The majority of this content is hosted overseas on social media platforms. There is a clear role for the internet industry and responsible social media companies are working with us to take down extremist material and safeguard their users. This approach limits the circulation of this material and is working well.

In recent months, we have seen an increase in the scale and pace of terrorist communications by groups like ISIL, encouraging vulnerable people to travel to conflict zones like Syria and Iraq. Approximately 70% of CTIRU's current caseload is ISIL, Syria or Iraq related.

We launched the newly updated CTIRU reporting tool in March 2014. Public referrals have tripled since this was introduced. Members of the public can report content of concern to the police at www.gov.uk/report-terrorism. We also encourage the public and civil society organisations to refer terrorist and extremist content directly to social media companies and Internet Service Providers (ISPs) through existing flagging mechanisms.

6.11 – Closed Material Procedure

The Justice and Security Act 2013 introduced a new statutory closed material procedure (CMP), which allows for sensitive material which would be damaging to national security to be examined in civil court proceedings.[25] CMPs ensure Government Departments, the Security and Intelligence Agencies, law enforcement and indeed any other party to proceedings have the opportunity properly to defend themselves, or bring proceedings, in the civil court, where

[24] The full report of the Extremism Task Force, "Tackling Extremism in the UK, Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism", which was published on 4 December 2013, is available at www.gov.uk/government/publications/tackling-extremism-in-the-uk-report-by-the-extremism-taskforce

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

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 interest 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. 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, if necessary, the CMP may be revoked by a judge at any stage of proceedings.

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.

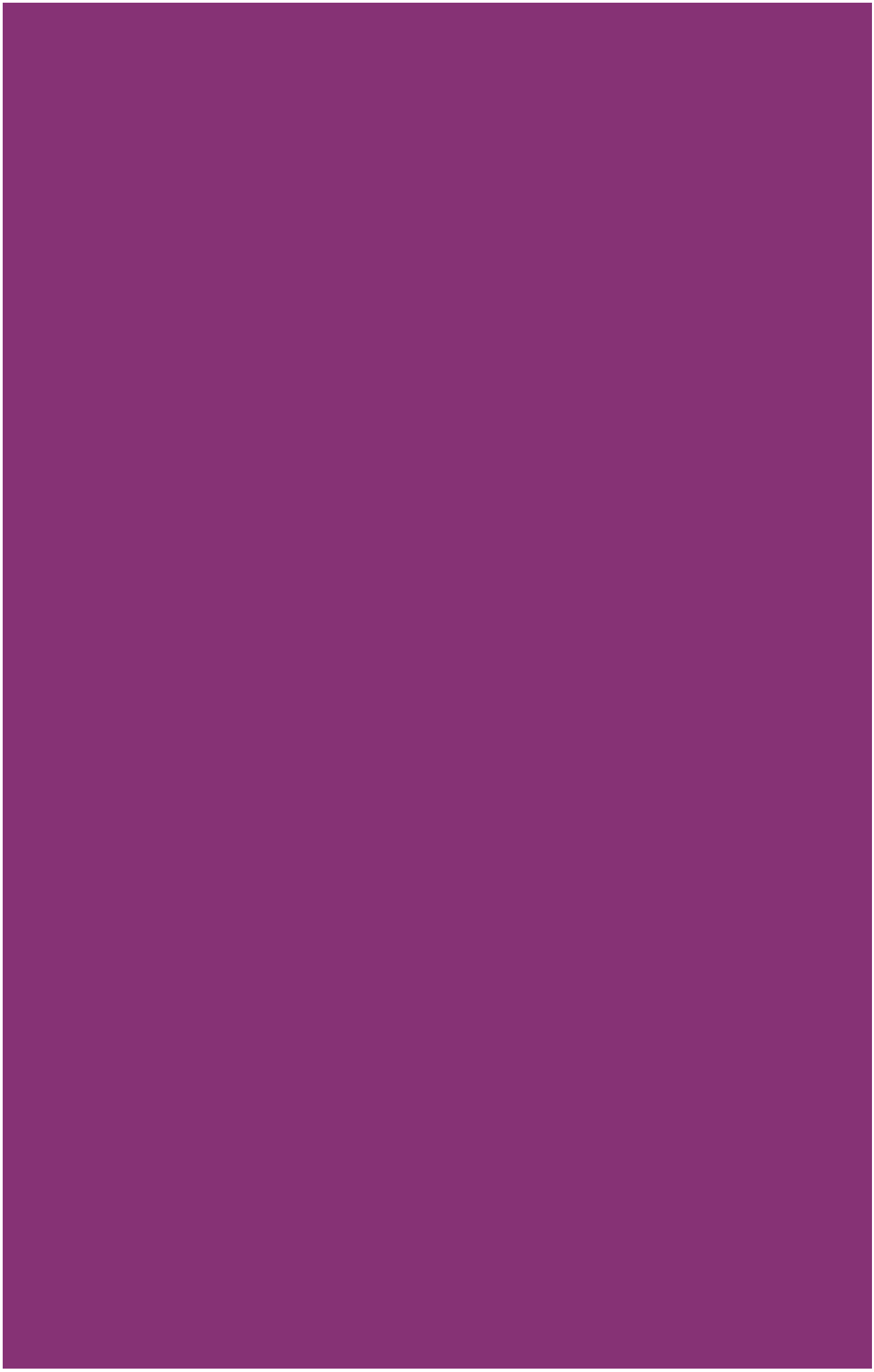
The Justice and Security Act requires the Secretary of State to prepare (and lay before Parliament) a report on CMP applications and subsequent proceedings under section 6 of the Act. Under section 12(4) of the Act, the report must be prepared and laid before Parliament as soon as reasonably practicable after the end of the twelve month period to which the report relates. The first report covered the period from 25 June 2013 (when the Act came into force) to 24 June 2014.[26] The most recent report, relating to the period 25 June 2014 to 24 June 2015, was published on 15 October 2015[27].

In the latest reporting period from 2014 to 2015, there were 11 applications for a declaration that a CMP be made (9 of them by the Secretary of State, and 2 by the Chief Constable of the Police Service of Northern Ireland). There were 5 declarations made in proceedings (3 in response to applications during the reporting period, and 2 in response to applications during previous reporting periods). None of the declarations were revoked.

There were 7 final judgments during this period (2 of them were partly closed judgments).

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

[27] https://www.gov.uk/government/publications/use-of-closed-material-procedure-report-25-june-2014-to-24-june-2015



7 – Investigatory Powers

The use of a range of covert investigatory techniques is critical to the intelligence and law enforcement agencies' ability to counter the threats we face from terrorism and serious and organised crime. The powers outlined in this chapter, subject to robust safeguards, are vital in the investigation of crime, including terrorism, and to preserve national security.

These powers are primarily regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), which ensures that they can only be used where it is necessary and proportionate to do so.[28] RIPA sets strict limits on the exercise of these powers, including the purposes for which they can be used, the authorities that can use them, authorisation procedures and how the material obtained can be used.

In addition, it is this Government's intention to bring forward legislation relating to the security, intelligence and law enforcement agencies' use of investigatory powers and to have that legislation enacted before the sunset provision in the Data Retention and Investigatory Powers Act 2014 takes effect on 31 December 2016.

The Government published a draft Bill for pre-legislative scrutiny by a Joint Committee of Parliament on 4 November, with the intention of introducing a Bill early in the New Year.

This section explains key investigatory powers, sets out their use, and describes the stringent safeguards that regulate them.

7.1 – Interception

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. 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. The majority of MI5's top priority UK counter-terrorism investigations have used intercept capabilities in some form to identify, understand or disrupt plots seeking to harm the UK and its citizens.

There are only a very limited number of intercepting agencies. These are: MI5, the Secret Intelligence Service, the Government Communications Headquarters (GCHQ), the National Crime Agency, the Metropolitan Police Service, the Police Service of Northern Ireland, the Police Service of Scotland, HM Revenue and Customs and the Ministry of Defence.

[28] The Regulation of Investigatory Powers Act is available at www.legislation.gov.uk/ukpga/2000/23/contents

RIPA, and the associated Code of Practice, sets out a comprehensive legal framework, approved by Parliament, for the regulation of the interception of communications. RIPA contains a range of robust safeguards and any interception warrant must be authorised by a Secretary of State (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). Authorisation takes place on a case by case basis, for limited and specified purposes, and only when the Secretary of State considers that it is both necessary and proportionate.

Interception warrants have a limited duration. Where they have been authorised in relation to national security or the economic well-being of the UK (directly linked to national security), an interception warrant lasts for six months. Where a warrant has been issued in relation to serious crime, this duration is three months. Whilst an interception warrant may be renewed at the end of such a period, this can only be done by a Secretary of State, and where it is still considered to be necessary and proportionate. In addition, the interception warrant must be cancelled if it is no longer necessary or proportionate.

The use of interception is subject to independent oversight by the Interception of Communications Commissioner and the Interception of Communications Commissioner's Office (IOCCO). The Commissioner reports to the Prime Minister and his reports are published and laid before Parliament (see also **Chapter 8.2**). Under measures in the Data Retention and Investigatory Powers Act 2014, the Commissioner is now required to report on a twice yearly basis. His latest annual report, covering 2014, was published on 12 March 2015 and his first half-yearly report was published on 16 July 2015.[29] The Security and Intelligence Agencies are also subject to oversight by the Intelligence and Security Committee (ISC) of Parliament. On 12 March 2015 the ISC, whose powers were significantly strengthened as a result of the Justice and Security Act 2013, published its report following its review into the balance between individual rights to privacy and our collective right to security, which included detailed consideration of the use of interception powers.

There are two types of interception warrant. Warrants issued under section 8(1) of RIPA may be issued in respect of the interception of communications to or from a specified person or premises carried on any postal service or telecommunications system. A section 8(1) warrant must name or describe either a person as the interception subject, or a single set of premises to which the interception warrant relates.

An application for a section 8(1) warrant will contain a consideration of necessity and proportionality, including:

- the background of the operation and a summary of the threat to national security or the serious crime being investigated;
- the relevant person or premises the warrant relates to, including an outline of the subject's relevance to the investigation;
- why the intelligence sought is not available by other, less intrusive means;

[29] The Data Retention and Investigatory Powers Act 2014 is available at www.legislation.gov.uk/ukpga/2014/27/contents/enacted

- the communications address to be intercepted, how that address was identified, how it is known that it relates to the subject of the warrant and confirmation that the interception is feasible;
- the information that is expected to be obtained from the warrant and why such information is necessary to achieve the objective of the investigation;
- the likely extent of interference with the privacy of the subject of the warrant;
- the likely extent of interference with the privacy of individuals who are not the subject of the warrant, for example, any recipients of legitimate social or business calls and messages from the communications address;
- an assurance that the intercepted material will be handled in accordance with the safeguards in RIPA; and
- where it is anticipated that confidential material may be accessed, such as matters subject to legal privilege, confidential journalistic material or other confidential personal information, this must be highlighted on the application form and an additional degree of consideration must be applied.

Interception warrants may also be issued under section 8(4) of RIPA in respect of external communications. External communications are defined in RIPA 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 transit. 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 transit, such as a domestic email that is transmitted via a server in another country.

Conduct authorised under a section 8(4) warrant may sometimes result in the incidental interception of communications that were both sent and received in the British Islands; RIPA permits this only if it is necessary to intercept the external communications that are the target of the warrant. In his 2014 Annual Report, the Interception of Communications Commissioner provided a further summary of internal and external interception.[30]

As with an application for a section 8(1) warrant, an application for a section 8(4) warrant must contain a consideration of necessity and proportionality. Specifically, this will include:

- the background to the relevant operational requirement;
- a description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data;
- a description of the communications to be intercepted, including details of the communications service provider(s) and an assessment of the feasibility of the operation where relevant;

[30] The 2014 annual report of the Interception of Communications Commissioner can be found at www.iocco-uk.info

- a consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- an assurance that the intercepted material will be handled in accordance with the safeguards in RIPA; and
- an assurance that intercepted material will be read, looked at or listened to only so far as it is covered by the terms of a certificate issued by the Secretary of State describing the material which may be examined. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971).

Responsibility for authorising any interception warrant, either under section 8(1) or section 8(4), lies with a Secretary of State.

Before material intercepted under a section 8(4) warrant may be examined, it is subject to a further consideration of necessity and proportionality. If an analyst wishes to examine a communication sent by or intended for an individual believed to be located in the British Islands, he or she must apply to the Secretary of State for an authorisation under section 16(3) of RIPA. This process is similar to the application for a warrant under section 8(1).

Interception authorised under sections 8(1) and 8(4) plays a vital role in safeguarding national security and detecting and preventing serious crime.

A draft updated Interception of Communications Code of Practice was published for public consultation on 6 February 2015. The consultation closed on 20 March 2015. The updated Code includes new details about the operation of the regime for the interception under RIPA of communications sent or received from outside the UK. It also includes further information about the safeguards for the interception of legally privileged communications and minor changes to reflect developments in the law since the Code was first introduced in 2002. Responses to the consultation have been analysed and the Code will be debated in Parliament in due course.

Interception Statistics

There are limits in statute relating to the extent to which information can be published in relation to interception. Section 19 of RIPA requires that the existence of an interception warrant and steps taken to implement it, as well as any intercepted material, are kept secret. This reflects the importance of protecting the sensitive operational capabilities of our intelligence and law enforcement agencies. Publishing such details would assist those who seek to do us harm, including terrorists, to evade detection.

However, the Interception of Communications Commissioner does publish figures in relation to the use of interception, including the total number of interception warrants authorised (see also **Chapter 8.2**). For 2014, this figure was 2,795. In 2013 it was 2,760, and in 2012, 3,372. For the first time, the Commissioner's report for 2014 also published the breakdown of the total number of warrants issued by statutory purpose. In 2014, 68% of warrants were issued for the purpose of the prevention and detection of serious crime, 31% were issued in the interest of national security and 1% were issued in relation to a combination of statutory purposes.

The 2014 annual report of the Interception of Communications Commissioner highlights that the total number of extant interception warrants as at 31 December 2014 was 1605. Given that 2795 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 1605 warrants that were extant at 31 December 2014, 20 were issued under section 8(4) of RIPA.

7.2 – Communications Data

Communications data (CD) is information about who was communicating, when, from where, how and with whom; the context but not the content of a communication. For example, CD for mobile phones might be billing and location information and for online communications, the internet protocol (IP) addresses identifying the individual, or at least the device, that sent an email or posted a message on the internet.

CD is used in the investigation and prosecution of a broad range of crimes, including terrorism. It enables the police, and other public authorities, to build a picture of the activities, contacts and whereabouts of suspects and victims. It can also be used to identify and locate vulnerable people. CD 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.[31] A number of case studies outlining the use of communications data are set out at **ANNEX C**.

The acquisition of CD is stringently regulated, primarily by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA ensures that CD can only be acquired by certain public authorities, and for a statutory purpose, approved by Parliament. For example, the police can acquire CD in an emergency to help locate someone whose life is at risk but where no crime is suspected. Requests 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. In the case of local authorities, since 1 December 2014, requests must be made centrally through the National Anti-Fraud Network and, under provisions in the Protection of Freedoms Act 2012, also require judicial approval.

The Data Retention and Investigatory Powers Act 2014 (DRIPA) was passed in response to a European Court of Justice judgment that threatened the Government's ability to require communications service providers to retain CD. DRIPA ensures that certain categories of CD continue to be available to public authorities when needed. DRIPA, and the Data Retention Regulations 2014 made under it,[32] also introduced additional safeguards, enhancing our data retention notice regime and formalising the requirements placed on communications service providers to safeguard this data.

DRIPA was an emergency measure that did not introduce any new powers, rights of access, or obligations on communications service providers that did not already exist. In addition to DRIPA, the Counter-Terrorism and Security Act 2015 (CTSA) received Royal Assent on 12 February. CTSA has amended DRIPA to include a provision for domestic communications

31 Information provided by the Crown Prosecution Service Organised Crime Division.

32 The Data Retention Regulations 2014 are available at www.legislation.gov.uk/uksi/2014/2042/contents/made

companies, that are under a data retention notice, to retain additional information to help identify who was using an internet protocol (IP) address at a specific point in time.

The CTSA provides important new capabilities to our law enforcement agencies. It will ensure that they are better able to identify suspects, victims, and those at risk of harm, from their communications online.

However, the CTSA does not address all of the capability gaps that the Draft Communications Data Bill in 2012 was intended to close. This means that as technology changes, and more and more communications take place over the internet, our law enforcement and intelligence agencies' capability to acquire CD will continue to degrade. The Government has been clear that legislation is needed on investigatory powers, including communications data, to ensure that we have a legal framework that is modern, fit for purpose and gives our law enforcement and intelligence agencies the capabilities they need. A draft Bill was published on 4 November for pre-legislative scrutiny.

The Interception of Communications Commissioner and the Interception of Communications Commissioner's Office (IOCCO) provide independent oversight of the acquisition of communications data by public authorities, including through inspections of these authorities. The Commissioner provides reports to the Prime Minister, which are subsequently published. Under provisions in DRIPA, the Commissioner is now required to report on a half-yearly basis, further enhancing transparency. The latest annual report of the Commissioner was published on 12 March 2015 and his first half-yearly report was published on 16 July.

The processing of personal information, including communications data, is regulated by the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, which is overseen by the Information Commissioner. The Information Commissioner is also under a duty to audit compliance by communications service providers with the provisions of the Data Retention Regulations 2014 with respect to the security, integrity and deletion of retained data.

In March, two new communications data Codes of Practice were presented to Parliament and brought into force. The revised Acquisition and Disclosure of Communications Data Code of Practice introduces a requirement that law enforcement acquisition of communications data to determine journalistic sources be carried out under the Police and Criminal Evidence Act 1984 (or equivalent legislation in Northern Ireland and Scotland), which provides for judicial authorisation. The code also contains enhanced record-keeping requirements on public authorities that are able to acquire communications data. These requirements include the collection of statistics relating to the number of individual items of CD acquired by public authorities, the type of data acquired, the crime types they relate to, the age of the data and the number of days of data being sought. The changes in the code will lead to the publication of significantly more detailed statistics on the use of communications data in the future.

In addition to the revised acquisition code, a new Data Retention Code of Practice has also been brought into force. This code sets out how the Government implements the requirements in DRIPA and the Data Retention Regulations and covers: the issue, review, variation and revocation of data retention notices; the communications service providers' ability to recover their costs; data security; oversight by the Information Commissioner; and safeguards on the disclosure and use of retained data by communications service providers.

Communications Data Statistics

The latest annual report of the Interception of Communications Commissioner, covering 2014, contains more detail than ever before on the use of communications data by public authorities, as outlined below (see also **Chapter 8.2**).

There were 517,236 notices and authorisations for communications data under Chapter II of Part I of RIPA in 2014, compared to 514,608 in 2013. Authorisations and notices are the two methods for acquiring communications data. An authorisation, under section 22(3) of RIPA, is effected by a person in the relevant public authority engaging in conduct to acquire the CD, primarily through the use of secure, auditable CD disclosure systems. A notice, under section 22(4) of RIPA, requires a communications service provider to disclose the data to the relevant public authority.

In addition to publishing the total number of notices and authorisations under Chapter II of Part I of RIPA, the Commissioner's latest report also includes, for the first time, the total number of applications for communications data. For 2014, this was 267,373. An authorisation will only be granted, or a notice given, once a designated person in a public authority has approved an application for communications data. The number of applications is a significantly lower figure than the number of notices and authorisations. This is because one application may result in more than one notice or authorisation, such as where the CD required is held by more than one communications service provider.

In certain circumstances, and where there is no time to complete the normal written process for requesting CD, a public authority may make an urgent oral request. Circumstances where an urgent oral request may be made include a situation where there is an imminent threat to life, or where there is a credible threat to national security. During 2014 there were 55,346 notices and authorisations given orally. 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, but 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 2014 report of the Interception of Communications Commissioner includes details of the total number of notices and authorisations, 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 in place a divert on 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 2014, almost half (49%) of notices and authorisations were for subscriber data; 33% were for traffic data; and 2% were for service use data. In addition, 16% of notices and authorisations were for a combination of different data types.

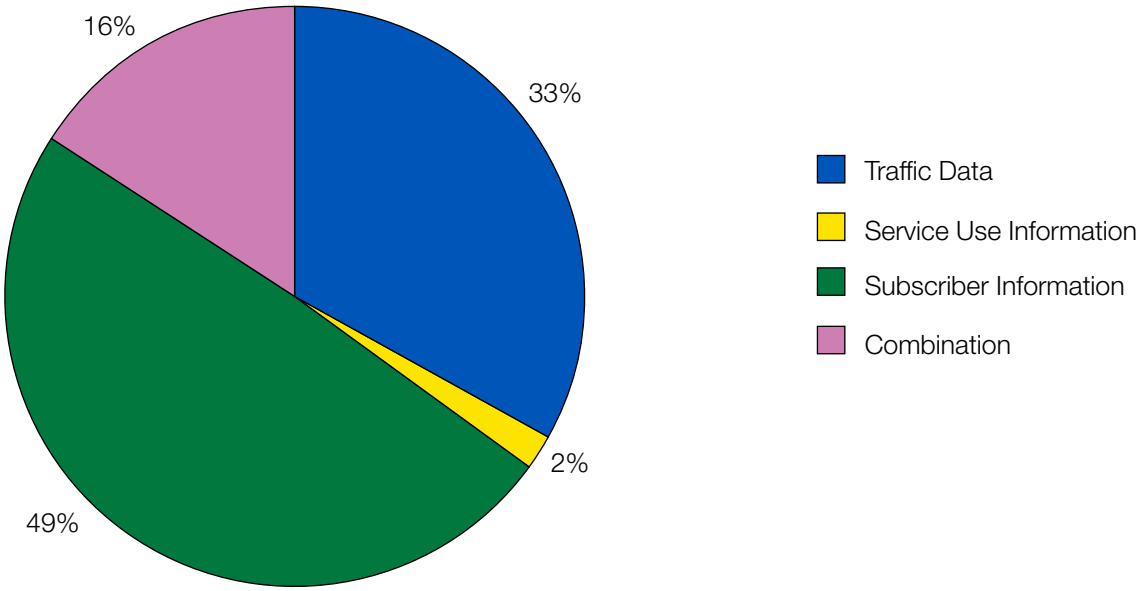


Figure 2: Communications data authorisations and notices by data type, 2014

The Commissioner's report also breaks down the total number of notices and authorisations, except those granted on an urgent oral basis, by the type of public authority requesting the data. This shows that the large majority of CD requests made in 2014 were from the police and law enforcement agencies, comprising 88.9% of notices and authorisations in total. The security and intelligence agencies accounted for 9.8% of the total, and less than 2% were made up by local authorities (0.4%) and other public authorities (0.9%).

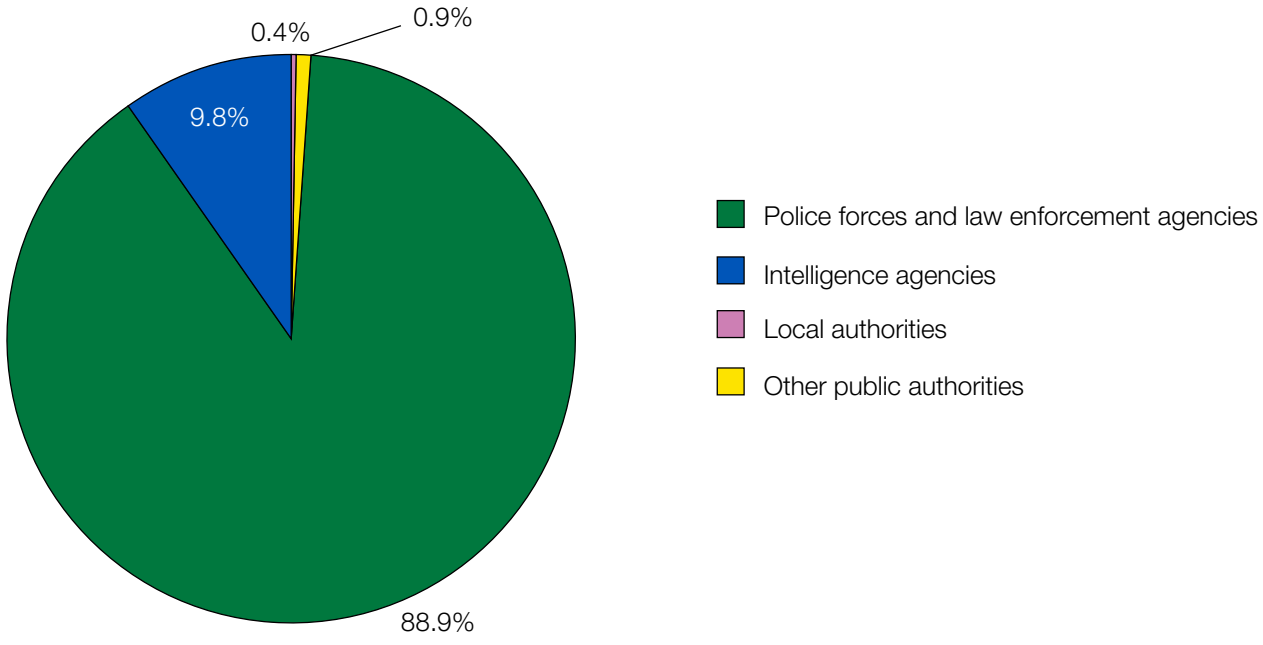


Figure 3: Communications data authorisations and notices by public authority type, 2014

The report also breaks this category down further, and includes the total number of notices, authorisations and applications, made by each public authority. The full list is included at **ANNEX D**.

The Commissioner's report also breaks down the total number of applications by the statutory purpose for which the data was required. During 2014, the prevention and detection of crime was the most predominant statutory purpose for which CD was acquired, accounting for 78.5% of notices and authorisations. The next most common statutory purposes were national security (15%) and preventing death or injury in an emergency situation (6%). The combined total for all other statutory purposes accounted for less than 1% of all applications.

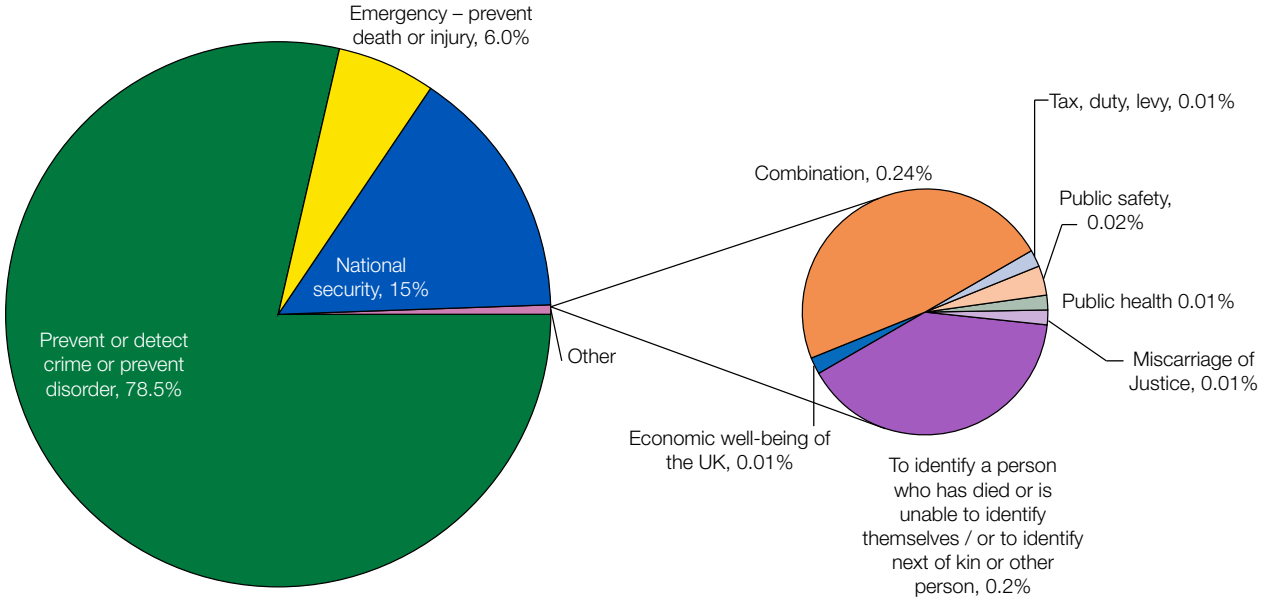


Figure 4: Communications data applications by statutory purpose, 2014

The Commissioner's report does not include statistics on the number of individuals to whom communications data notices and authorisations relate. This is because requests are normally made in relation to phones, or other devices and accounts. Investigators in public authorities then need to establish which individual was using the device. In addition, individuals usually have more than one device or account, such as landline phones, mobiles, broadband and so on. Different requests may also relate to the same device in different locations and at different times. For these reasons, developing accurate statistics on the number of individuals whose CD has been acquired, in relation to the total number of notices and authorisations, is likely to be impossible.

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

The use of covert techniques is an important weapon in the fight against terrorism and serious and organised crime, including the trafficking of drugs and firearms, and child abuse. Covert surveillance (both intrusive and directed surveillance) and the use of covert human intelligence sources (CHIS) are stringently regulated by Part II of the Regulation of Investigatory Powers Act 2000 (RIPA). Additionally, the Police Act 1997[33], and the Intelligence Services Act 1994,[34] provide for property interference to be undertaken by the law enforcement 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. The exercise of these powers by the intelligence agencies and the Ministry of Defence is overseen by the Intelligence Services Commissioner (see also **Chapter 8.3**). The use of these powers by the police and other public authorities is overseen by the Office of Surveillance Commissioners (see also **Chapter 8.4**).

Intrusive Surveillance

Intrusive surveillance is surveillance 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 intelligence agencies, the Ministry of Defence and HM Armed Forces requires authorisation by the Secretary of State. Applications by the police and other public authorities are authorised internally. However, these applications additionally require the prior approval of an independent Surveillance Commissioner (working for the Office of Surveillance Commissioners).

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.

---

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

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

Local authorities in England, Wales and Northern Ireland[35] must also obtain judicial approval for the use of directed surveillance, under measures in the Protection of Freedoms Act 2012.[36] In addition to the requirement for judicial oversight, 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 where necessary and proportionate for a statutory purpose approved by Parliament. 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 source, and for the source's security and welfare.

The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 increased the authorisation levels required for the use of undercover officers and enhanced oversight by the Office of Surveillance Commissioners. Specifically, any deployment of an undercover law enforcement officer must be authorised by an Assistant Chief Constable, or equivalent, and notified to the Office of Surveillance Commissioners. Any deployment lasting more than 12 months must be authorised directly by the Chief Constable, or equivalent, and receive prior approval by an independent Surveillance Commissioner. This level of authorisation and approval must be obtained for any authorisation lasting more than three months, in circumstances where the authorisation involves matters subject to legal privilege.

Property Interference

Property interference may be authorised for law enforcement agencies under Part III of the Police Act 1997, in order for them to enter or interfere with property, or wireless telegraphy, for the purpose of preventing or detecting serious crime. Similar powers are contained in section 5 of the Intelligence Services Act 1994 for the purpose of enabling the intelligence agencies to exercise their functions.

Property interference is subject to a stringent authorisation regime, ensuring it can only be used where 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 gives authorisation for property interference, he or she must, as soon as reasonably practical, give notice of it to a Surveillance Commissioner. In addition, prior approval for a property interference authorisation must be sought from a Surveillance Commissioner where the property in question is used wholly or mainly as a dwelling or is a hotel bedroom or office

[35] 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.

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

premises. Approval is also required where the interference might involve acquiring knowledge of matters subject to legal privilege, journalistic material or confidential personal information.

The 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 they are satisfied that it is necessary and proportionate, and they must also give consideration as to 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.

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 have recently been updated to reflect, among other things, the enhanced authorisation procedures for law enforcement agencies' use of CHIS and for local authorities' use of directed surveillance. Also, the revised CHIS Code stipulates 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, laid before Parliament on 15 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. The revised Codes of Practice came into force on 10 December 2014.

Statistics for covert techniques

Intelligence Agencies

The annual report of the Intelligence Services Commissioner includes statistics on the total number of warrants and authorisations approved across the intelligence agencies and Ministry of Defence (see also **Chapter 8.3**).

For the 2014 calendar year, the total number of warrants and authorisations approved was 2032, compared to 1887 in 2013.

Law Enforcement Agencies and Other Public Authorities

The annual report of the Chief Surveillance Commissioner includes statistics on the use of intrusive surveillance, directed surveillance, CHIS and property interference by law enforcement agencies and other public authorities (see also **Chapter 8.4**). The Commissioner's latest report covers the period from 1 April 2014 to 31 March 2015. There were 321 authorisations for intrusive surveillance, compared to 392 in the previous period. In addition, two authorisations for intrusive surveillance in this reporting period were quashed by Commissioners.

Law enforcement agencies authorised the use of directed surveillance on 8,333 occasions, with 1,173 extant at the end of March 2015. These figures were lower than in the previous reporting period, where the Commissioner reported that 9,664 authorisations were given, with 1,484 extant at the end of the year. The total number of authorisations for directed surveillance by other public authorities was 2,207, compared to 4,412 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) traditionally accounts for the majority of authorisations within this category. The DWP reported a 72% reduction in the number of authorisations granted in this reporting period, from 3,225 the previous year down to 894. The reduction in DWP figures largely accounts for the total decrease in the number of authorisations in this category.

During the reporting period 2,998 CHIS were authorised by law enforcement agencies and as at 31 March 2015, there remained 2,812 authorised. Over the course of the year, 2,823 CHIS were cancelled, although this figure includes CHIS that were authorised in previous years. At the end of the reporting period, there were 90 active CHIS in other public authorities. Only a very small proportion of these public authorities (2.5%) use CHIS. This will often be for matters such as trading standards investigations.

During the reporting period, and excluding renewals, property interference authorisations were granted on 2,091 occasions. This was a decrease of 598 on the previous year. None of these authorisations were quashed by Commissioners.

Following the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 coming into force, the Commissioner's annual report includes statistics on the number of authorisations of relevant sources. In this context "relevant sources" refers to undercover officers employed by law enforcement agencies who have been authorised for longer than twelve months, either continuously or cumulatively in respect of a particular operation. During the reporting period 1,095 relevant sources were notified to the Office of Surveillance Commissioners, 770 were cancelled and 46 were submitted for the prior approval renewal process.

Figure 5: Summary of key activity in relation to the use of covert techniques in the year ending 31 March 2015

	Intrusive surveillance authorisations	Property interference authorisations	Relevant sources notified	Directed surveillance authorisations	Authorised CHIS at 31/03/2015
Law Enforcement	321	2,091	1,095	8,333	2,812
Other Public Authorities				2,207	90

7.4 – Investigation of Protected Electronic Information

The investigation of electronic information protected by encryption is an important tool to ensure that public authorities' ability to protect the public is not undermined by technologies used to protect electronic information. 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 utilise the same technologies in order to conceal their unlawful conduct and to evade detection.

Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) provides a transparent statutory framework enabling public authorities to give a notice to holders of protected information requiring protected electronic information which the authority has obtained lawfully, or is likely to obtain lawfully, to be put into an intelligible form.

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, or in the interests of the economic well-being of the UK. In addition, these powers must not be used where the person with the appropriate permission can 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 permission to serve a notice requiring protected information to be put into an intelligible form. 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 of RIPA.

The National Technical Assistance Centre (NTAC), which provides technical assistance to public authorities, particularly law enforcement agencies and intelligence agencies, includes a facility for the processing of lawfully obtained protected electronic information.

NTAC is the lead national authority for all matters relating to the processing of protected information into an intelligible form, and acts as a guardian and gatekeeper to public authorities that have powers to exercise this function. All public authorities are required to consult with NTAC at the earliest opportunity when considering the exercise of the powers in Part III of RIPA. No public authority may serve any notice or seek to obtain appropriate permission without the prior approval of NTAC to do so.

A public authority may seek appropriate permission for giving a notice from an appropriate authority. Public authorities may obtain appropriate permission from a person holding judicial office where protected information is likely to be, or has been, obtained under a warrant issued by 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 under section 8 of RIPA), 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 in consequence of 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 requirement for permission to be granted by 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, which relates to a constable's general powers of seizure.

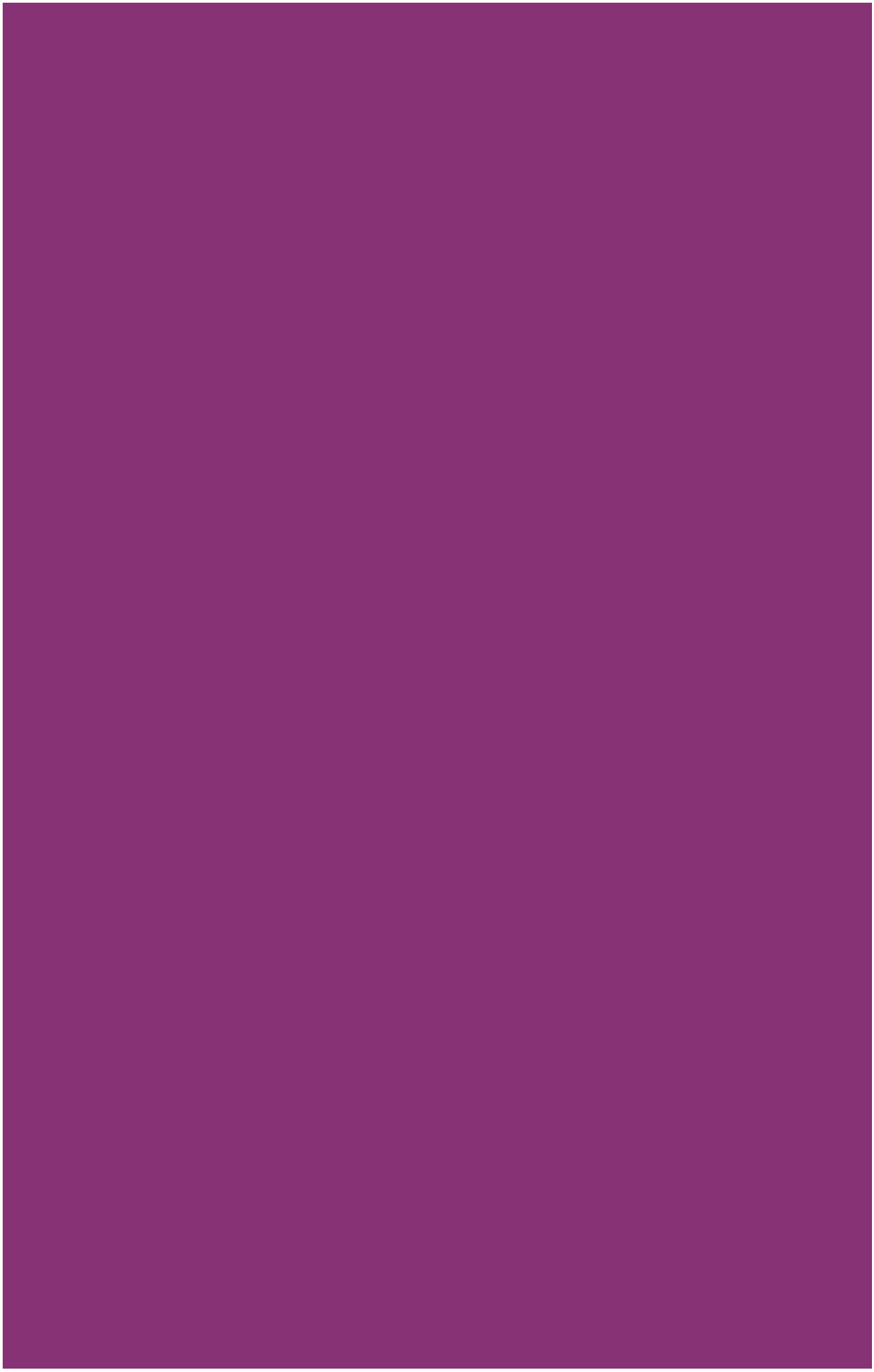
Once appropriate permission has been given, a disclosure requirement can be placed on a number of parties, including the company that developed or provided the service protecting the relevant information. Such a notice should not be served without first having consulted the relevant company about the technical and practical implications for their business of the proposed disclosure requirement. The effect of imposing a disclosure requirement is that the recipient shall be required, in accordance with the notice, to make a disclosure of any key to the protected information to make the material intelligible that is in his/her possession. 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 of protected electronic information. The Commissioner's latest report covers the period from 1 April 2014 to 31 March 2015. The report outlines that during the reporting period, NTAC granted 88 approvals, out of 89 applications, to investigate electronic data protected by encryption. Permission was not sought in ten cases after NTAC approval. From the remainder, permission was granted to progress 38 of these approvals and 37 were subsequently served. Of these 37 cases, nine were complied with, 22 were not, and the remainder are still being processed. The Annual Report of the Interception of Communications Commissioner confirms that there were no notices given in 2014 for the investigation of protected electronic information, in relation to information obtained from an interception warrant.

Covering the reporting period, NTAC were informed that three convictions were secured as a result of these approvals. One conviction related to the charge of possession of indecent images of children, one to threats to kill and one to murder.

Other offences for which a disclosure Notice was sought include: firearms, domestic extremism, possession of indecent images of children, kidnapping of children, human trafficking, insider dealing, fraud, evasion of excise duty, money laundering, perverting the course of justice, drug trafficking and drug possession with intent to supply.



8 – Oversight

As well as being stringently regulated by the robust safeguards set out in existing legislation, the use of disruptive and investigatory powers is subject to rigorous, independent oversight. The operation of terrorism legislation, including the exercise of various disruptive powers set out in this report, is subject to review by the Independent Reviewer of Terrorism Legislation.

The use of the investigatory powers explained in this report is primarily overseen by three independent Commissioners: the Interception of Communications Commissioner and the Interception of Communications Commissioner's Office (IOCCO); the Intelligence Services Commissioner; and the Chief Surveillance Commissioner, as well as Surveillance Commissioners in the Office of Surveillance Commissioners.

In addition to the oversight of the Commissioners, the Investigatory Powers Tribunal provides an independent right of redress to any individual who believes that investigatory powers have been used unlawfully against them.

The following section explains the roles and functions of each of the Commissioners, as well as the Independent Reviewer of Terrorism Legislation and the Investigatory Powers Tribunal, setting out their inspection and reporting regimes, and outlining the findings of their most recent annual reports.

Further to the oversight bodies that are explained in the following section, the intelligence agencies are also overseen by the Intelligence and Security Committee of Parliament (ISC). The ISC was established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the Security Service, Secret Intelligence Service and GCHQ. The Justice and Security Act 2013 provided the Committee with additional powers, increasing its remit to include retrospective oversight of operational activity and the wider intelligence and security activities of Government. The ISC is committed to ensuring oversight of the intelligence agencies becomes more transparent and accordingly held its first open evidence session with the heads of the intelligence agencies on 7 November 2013.

8.1 – Independent Reviewer of Terrorism Legislation

The role of the Independent Reviewer of Terrorism Legislation ("The Independent Reviewer"), David Anderson QC, is to ensure that the operation of UK counter-terrorism legislation is fair, effective and proportionate. As part of this role, the Independent Reviewer regularly writes reports which are prepared for Secretaries of State and subsequently laid before Parliament, thereby informing the public and political debate. He is independent of Government and cleared to consider sensitive information relating to national security to inform his role.

The Independent Reviewer's statutory functions are set out at section 36 of the Terrorism Act 2006, which requires him to review the operation of terrorism legislation relating to the exercise of a broad range of powers, including a number of the disruptive powers explained in this report. The operation of Part I of that Act, which relates to terrorism offences, as well as the Terrorism Act 2000, fall within his remit and, specifically, his reports on these cover the following areas:

- definition of terrorism;
- proscribed organisations;
- terrorist property;
- terrorist investigations;
- arrest and detention;
- stop and search;
- port and border controls; and
- terrorist offences.

Since August 2012, the Independent Reviewer has also had a specific power to monitor the conditions of individuals detained for terrorism offences for more than 48 hours to ensure they are compliant with the provisions within Schedule 8 of the Terrorism Act 2000.

Separately, the Independent Reviewer also reviews the operation of the Terrorism Prevention and Investigation Measures Act 2011, and the Terrorist Asset-Freezing Etc. Act 2010.[37]

The Counter-Terrorism and Security Act 2015 made changes to the Independent Reviewer's remit and reporting requirements. It additionally allows him to review the following counter-terrorism statutes: Part 1 of the Anti-Terrorism, Crime and Security Act 2001 and Part 2 of that Act in so far as it relates to terrorism; the Counter-Terrorism Act 2008; and Part 1 of the Counter-Terrorism and Security Act 2015. The Act also made changes to provide the Independent Reviewer with flexibility in the way in which he reports. From 2016, he must set out a work programme at the beginning of each calendar year, to include what he will report on in that 12 month period, but has a greater discretion to determine the areas on which he will report, which he must notify to the Secretary of State. The exception to this is the Terrorism Act 2000, which remains subject to the existing annual reporting requirement.

The Government publishes responses to all of the Independent Reviewer's reports and his recommendations. The most recent response to his Annual Report on the operation of the Terrorism Acts was published on the GOV.UK website on 12 March 2015.

The Independent Reviewer has a number of other statutory functions. By virtue of section 7 of the Data Retention and Investigatory Powers Act 2014, he was required to undertake a review of the operation and regulation of investigatory powers, with specific reference to

[37] The Independent Reviewer's full reports on the operation of the Terrorism Acts, terrorist asset-freezing and terrorism prevention and investigation measures, as well as ad hoc "snap shot reports" on wider issues, can be found on his website at www.terrorismlegislationreviewer.independent.gov.uk

communications data and interception, and report his findings to the Prime Minister. The review gave specific consideration to the issues below:

- current and future threats, capability requirements and the challenges of current and future technologies;
- the safeguards to protect privacy;
- the implications for the legal framework of the changing global nature of technology;
- the case for amending or replacing legislation;
- the statistical and transparency requirements that should apply; and
- the effectiveness of current statutory oversight arrangements.

David Anderson's report, following his review, was published on 11 June.

8.2 – Interception of Communications Commissioner

The Interception of Communications Commissioner is appointed by the Prime Minister under section 57 of the Regulation of Investigatory Powers Act (RIPA). The Rt Hon Sir Anthony May stepped down as Commissioner on 31 July and a successor has not yet been appointed. In the interim, the Interception of Communications Commissioner's Office (IOCCO) are continuing to undertake their audits of public authorities' use of interception and communications data.

The Interception of Communications Commissioner is independent of Government and must hold, or have held, high judicial office in order to be appointed to the role. The Commissioner's primary role is to oversee the use of two investigatory tools, interception and communications data (see also **Chapter 7.1** and **Chapter 7.2**), and to ensure that the Secretaries of State and public authorities operating under Part I of RIPA, which regulates the use of these powers, do so lawfully. Specifically, the Commissioner's statutory responsibilities under section 57(2) of RIPA are to keep under review:

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

Section 58 (1) of RIPA imposes a statutory obligation on everyone concerned with the lawful interception of communications and the acquisition and disclosure of communications data under RIPA Part I to disclose or provide to the Commissioner all such documents or

information as he 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 conducts 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.

The Commissioner has also now been asked by the Prime Minister to conduct non-statutory oversight of Section 94 of the Telecommunications Act 1984. Section 94 provides that the Secretary of State may, after consultation with a person to whom that section applies, give to that person such directions as appear to the Secretary of State to be necessary in the interest of national security or relations with the government of a country or territory outside the United Kingdom. Specifically, this oversight will cover 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.

The Commissioner does not have oversight of matters that are overseen by the Intelligence Services Commissioner, Sir Mark Waller (see also **Chapter 8.3**), and the Chief Surveillance Commissioner, the Rt Hon the Lord Judge (see also **Chapter 8.4**).

Under section 58 (4) of RIPA (as amended by DRIPA), the Commissioner is 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 are subsequently published and laid before Parliament.

The most recent annual report of the Commissioner, covering January to December 2014, was published on 12 March 2015 and contained more detailed information and statistics than ever before in relation to the use of the investigatory powers that he oversees. 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 7.1** and **Chapter 7.2** of this report. In addition to his 2014 Annual Report, the Commissioner's first half-yearly report was published on 16 July 2015. The main purpose of this report was to provide reassurance that the Data Retention and Investigatory Powers Act 2014 (DRIPA) has not increased or extended powers. In addition, the half-yearly report provided an update on the implementation of the revised Acquisition and Disclosure of Communications Data Code of Practice, as well as details of 17 serious communications data error investigations initiated by the Commissioner in 2014.[38] Further to the Commissioner's twice yearly reports, IOCCO also publishes 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.[39]

Interception

The Commissioner's 2014 Annual Report sets out details of the rigorous processes that his office, IOCCO, undertake to ensure that interception powers are being used lawfully and in accordance with RIPA. This includes inspections of the intercepting agencies and warrant granting departments. During 2014, each of the intercepting agencies and warrant granting

38 The Commissioner's reports can be found in full at www.iocco-uk.info

39 www.iocco-uk.info

departments was inspected twice by IOCCO. There are three primary objectives during these inspections, which are 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 936 interception warrants, including associated paperwork. This is equivalent to one third of the total number of new warrants issued during 2014, and three fifths of the warrants extant at the end of the year. Following each inspection, IOCCO provides an inspection report to the head of the agency or department, outlining the formal recommendations. The relevant agency is 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 2014 was 85. During 2014, 60 errors were reported to IOCCO in relation to interception. The breakdown of the causes of these errors is outlined below.

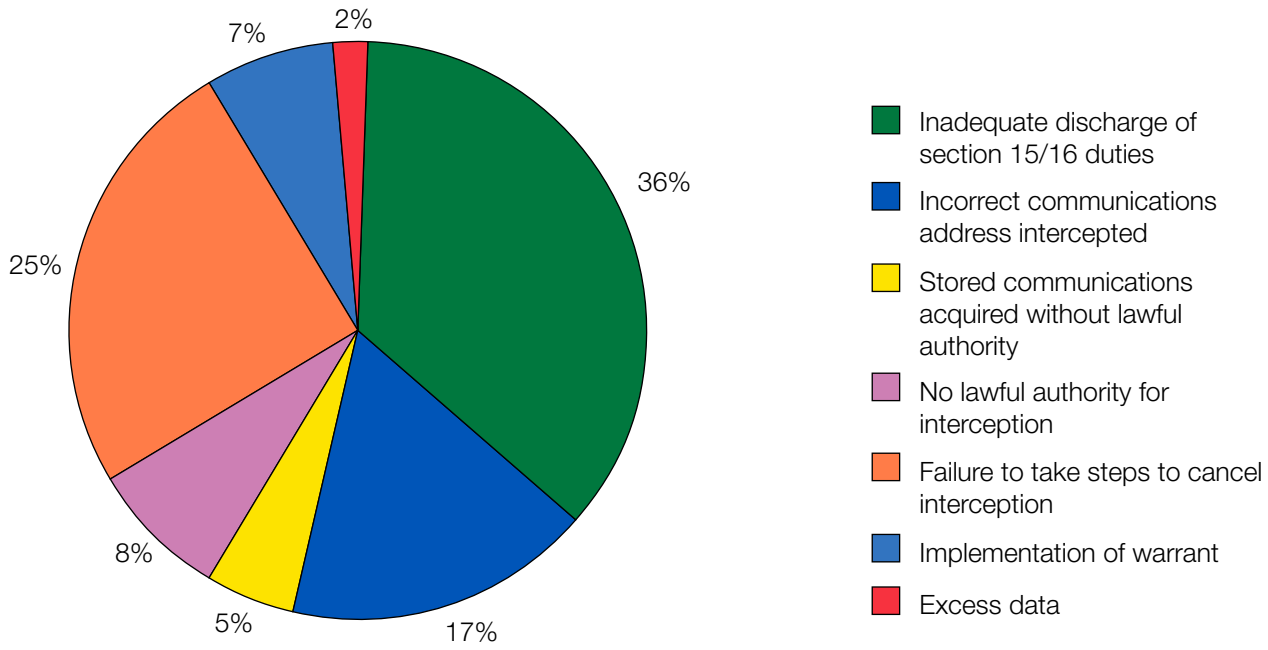


Figure 6: Interception errors by cause, 2014

The largest category of errors was in relation to the "inadequate discharge of sections 15/16 duties". 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.

Communications Data

During 2014, IOCCO undertook 90 communications data inspections. Of these 90 inspections, 51 were of police forces and law enforcement agencies, three were of an intelligence agency, 18 were of local authorities, including the National Anti-Fraud Network (NAFN), and the remaining 18 were of other public authorities that have powers to acquire communications data under RIPA. An additional 102 local authorities were inspected during the NAFN inspection. NAFN continues to provide a SPoC service for local authorities and over 90% of the local authorities that reported using their powers in 2014 submitted their requirements via NAFN. Since 1 December 2014, all local authority requests for communications data must be made through NAFN.

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

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

Over the course of these inspections, IOCCO examined several thousand applications for communications data. Where they are inspecting public authorities that only make a small number of applications, IOCCO will generally examine all applications that are made. For larger users, a random sample will be taken. In addition, a larger sample set is examined using query based searching methods. As with interception inspections, IOCCO completes a report following each inspection, outlining recommendations, which the public authority is required to respond to within two months. From the 90 inspections in 2014, the total number of recommendations made was 346.

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 IOCCO within five working days of the error being discovered.

In total, 998 communications data errors were reported to IOCCO during 2014, including those discovered during inspections.

At the end of each inspection, the public authority is given an overall compliance rating of good, satisfactory or poor. In 2014, 80% of public authorities achieved a good compliance rating, compared to 87% in 2013 and 85% in 2012. In addition, 14% received a satisfactory rating and only 6% of public authorities received a poor rating in 2014.

Of the 998 errors in 2014, 17 serious errors were identified. IOCCO defines the following as serious errors:

- technical errors relating to communications service providers secure disclosure systems which result in a significant number of erroneous disclosures;
- errors where the public authority has, as a consequence of the data, initiated a course of action that impacts on persons not connected with the investigation or operation (for example, the sharing of information with another public authority stating a person is 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 result in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

The Commissioner's first half-yearly report provides details of IOCCO's investigations into each of these serious errors. Of the 17 errors, nine were caused by human mistakes and eight were as a result of technical system faults.

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

The total of 998 errors in 2014, including the 17 serious errors, should be viewed in the context of the total number of notices and authorisations: 517,236 for 2014.

8.3 – Intelligence Services Commissioner

The Intelligence Services Commissioner, the Rt Hon Sir Mark Waller, was appointed by the Prime Minister under section 59 of the Regulation of Investigatory Powers Act 2000 (RIPA). The Commissioner is independent of Government and is responsible for providing independent, external oversight of the use of intrusive powers by the UK intelligence agencies and parts of the Ministry of Defence. The Justice and Security Act 2013 conferred additional functions on the Intelligence Services Commissioner requiring him to keep under review the carrying out of any aspect of the functions of the Intelligence Services, as directed by the Prime Minister (except for anything that is required to be kept under review by the Interception of Communications Commissioner; for example the Intelligence Services Commissioner is not responsible for oversight of directions under section 94 of the Telecommunications Act 1984.)

To be appointed the Commissioner must hold, or have held, high judicial office. The statutory functions of the Commissioner are set out in RIPA, as amended by the Justice and Security Act 2013. The Commissioner's statutory functions can be broken down into five main areas:

- to keep under review the exercise by the Secretaries of State of their powers to issue warrants and authorisations to enable the intelligence services to carry out their functions. Such warrants and authorisations can relate to entering onto or interfering with property (or with wireless telegraphy), acts done outside the United Kingdom, intrusive surveillance, and the investigation of electronic data protected by encryption;
- to keep under review the exercise and performance of the powers and duties imposed on the intelligence services and MOD/Armed Forces personnel in relation to covert activities, which 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;
- 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 (direction dated 27 November 2014);
- 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 (direction dated 11 March 2015); and
- to keep under review the carrying out of any other aspect of the functions of the Intelligence Services, as directed by the Prime Minister.

The Commissioner is also required to provide the Prime Minister with an annual report on the discharge of his functions, and lay that report before Parliament.[40] The Commissioner's latest report covers 2014. As part of his continued drive for greater openness the Commissioner has restructured his report and dealt with issues thematically including, for example, sections on intrusive surveillance, directed surveillance, covert human intelligence sources and Intelligence Services Act section 7 authorisations. There is also a section on his recently publically avowed bulk personal data oversight.

The Commissioner's oversight of the use of warrants and authorisations issued to the UK intelligence agencies includes those issued to authorise equipment interference (EI), as set out in the draft equipment interference code of practice published for consultation on 6 February 2015. This code avowed that the Commissioner's oversight extends to operations to interfere with computers and other equipment information obtained from EI operations. It also introduced a requirement for the Commissioner to oversee the internal arrangements as to the safeguards applied to the processing, retention, disclosure and destruction of information obtained by EI.

During 2014, the Commissioner carried out two formal oversight inspections of each of the agencies that are able to apply for and authorise warrants (the Security Service, the Secret Intelligence Service, the Government Communications Headquarters and the Ministry of

40 The Commissioner's annual reports can be found in full at intelligencecommissioner.com

Defence). 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. In addition, the Commissioner met each of the respective Secretaries of State responsible for signing warrants at each department (the Home Secretary, the Foreign Secretary, the Defence Secretary and the Northern Ireland Secretary).

The total number of warrants and authorisations approved across the intelligence agencies and MOD in 2014 was 2032. The Commissioner individually scrutinised 343 warrants/ authorisations and their associated paperwork, which is 16.7% of the total. This is consistent with 2013, when the Commissioner examined 318 out of 1887 warrants and authorisations, which was 16.8% of the total for that year.

An important aspect of the Commissioner's role is to examine errors that occur during the process of the application and authorisation of warrants, or during their subsequent implementation. The Commissioner examines errors in two ways. Firstly, through the scrutiny of individual warrants and authorisations as part of his inspection regime. Secondly, the agencies are required to report to the Commissioner any error that has resulted in any unauthorised activity where an authorisation should have been in place. Where the agencies are reporting errors to the Commissioner, he expects 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 include details of the steps taken to avoid errors happening again.

During 2014, there were 43 errors. Of this total, 34 were errors reported to the Commissioner by the agencies and the remaining nine were discovered during his inspections.

Of the intelligence agencies, MI5 reported 27 errors to the Commissioner during 2014 and an additional four errors were discovered by the Commissioner during his inspections. The Commissioner notes that MI5 obtain a larger number of warrants and authorisations than the other agencies and that their error rate is low as a proportion of authorisations. SIS reported six errors to the Commissioner during 2014 and GCHQ reported one. The Commissioner did not discover any additional errors during his inspections of these agencies.

In relation to warrant granting departments, the Commissioner discovered three administrative errors when inspecting the Home Office and two administrative errors at the Ministry of Defence.

Of the 34 errors reported the most common error was failure to obtain authorisation in time. The breakdown of the causes of these errors is outlined below.

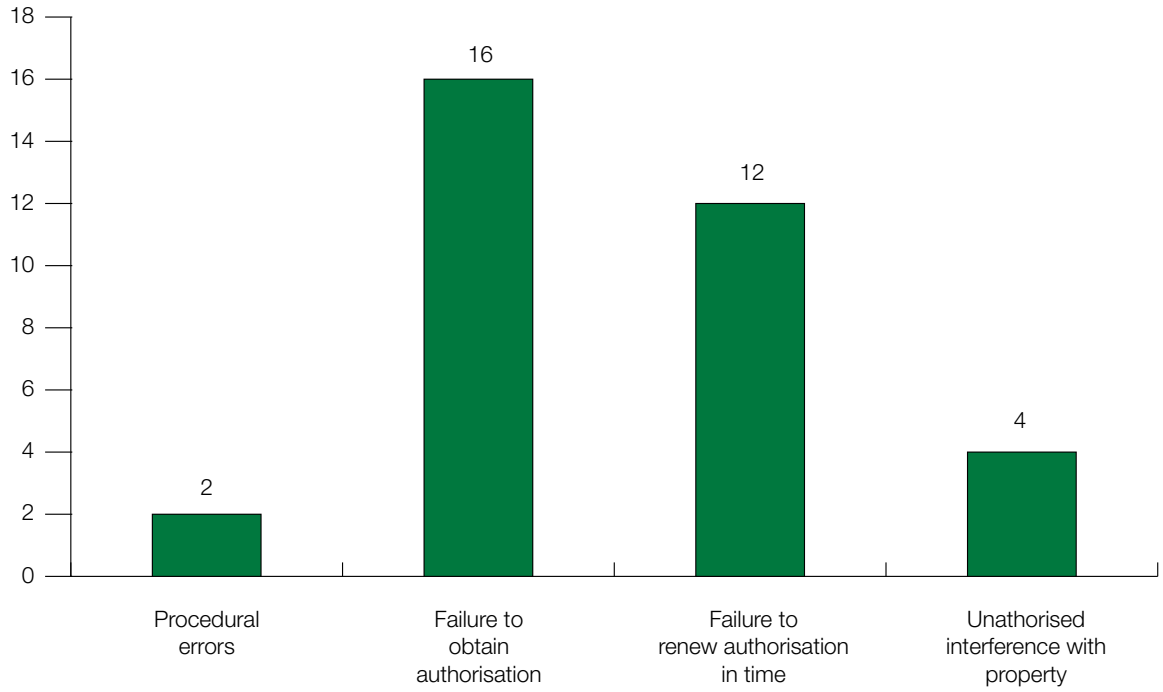


Figure 7: Reported errors by cause, 2014

The Intelligence Services Commissioner conducts his oversight through a formal four stage regime beginning with his selection of warrants from a list containing a brief summary of all warrants. He then selects some for closer scrutiny including the submissions and other underlying documents. He conducts formal inspections where he is briefed on current operations and is able to question the intelligence officers and senior personnel to ensure they can justify their activity. Finally he gets "under the bonnet" [41] of the intelligence agencies by scrutinising the underlying processes and culture and how the authorisations are put into operational practice. He attends training courses to gain a better understanding of the culture and ethos of the organisation and checks that the organisations have in place robust and rigorous internal checks and assurances.

The Commissioner's overall conclusion in his 2014 report is that "the agencies and the MOD take compliance extremely seriously and seek to obtain their authorisations on a correct legal basis, establishing necessity to do what they seek to do, and properly considering proportionality and the justification for any intrusion into privacy. Equally where a warrant or authorisation has to be obtained from a Secretary of State, the warrantry units consider with care whether the case for necessity and the justification for any intrusion into privacy has been made out and the Ministers themselves only sign the warrant or authorisation if they are satisfied of the necessity and proportionality of the activity they are authorising".[42]

41 "Report of the Intelligence Services Commissioner for 2014", page 9.

42 "Report of the Intelligence Services Commissioner for 2014", page 56.

8.4 – Office of Surveillance Commissioners

The Office of Surveillance Commissioners is responsible for providing robust, independent oversight of the use of covert surveillance by public authorities, excluding the 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 are 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 are drawn from the Police Act 1997, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A). His specific responsibilities are to oversee:

- the performance of functions under Part III of the Police Act 1997, which relate to the entry onto or interference with property or wireless telegraphy;
- except in relation to the intelligence agencies and the Ministry of Defence, the exercise and performance of the powers and duties conferred or imposed by or under Parts II and III of RIPA, which relate to the use of directed surveillance, intrusive surveillance, the conduct and use of covert human intelligence sources (CHIS), and the investigation of electronic data protected by encryption; and
- the exercise and performance of the powers and duties conferred or imposed by or under the Regulation of Investigatory Powers (Scotland) Act 2000.

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

There are six Surveillance Commissioners working under the Chief Surveillance Commissioner. These six Commissioners have statutory responsibilities to undertake the following activities:

- grant prior approval for authorisations and renewals of any intrusive surveillance;
- grant prior approval for property interference where it involves a hotel bedroom, a dwelling, or office premises, or where it might involve the acquisition of matters subject to legal privilege, confidential personal information or journalistic material;
- grant prior approval for any CHIS whose activities will result in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege;
- since 1 January 2014, grant prior approval for the renewal of law enforcement “relevant sources” (commonly termed undercover officers);
- note all other property interference authorisations, renewals and cancellations, and “relevant source” authorisations and cancellations;
- assist the Chief Surveillance Commissioner in his oversight of notification of disclosure requirement notices served in respect of electronic information protected by encryption; and
- assist the Chief Surveillance Commissioner in his duty to keep under review the use of directed surveillance and CHIS by law enforcement agencies.

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

In addition to the six Commissioners, the Office of Surveillance Commissioners also includes three Assistant Surveillance Commissioners and a number of Inspectors. The primary responsibility of the Assistant Commissioners is 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 must 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 are responsible for assisting the Chief Surveillance Commissioner by undertaking detailed inspections of the public authorities whose activities he is tasked to oversee.

The Chief Surveillance Commissioner reports annually to the Prime Minister and to Scottish Ministers on the matters for which he is responsible under the Police Act 1997, RIPA and RIP(S)A. These reports are presented to Parliament and laid before the Scottish Parliament, and are publically available. The Chief Surveillance Commissioner's most recent report covers the period from 1 April 2014 to 31 March 2015.[43]

The Commissioner's annual report includes statistics on the use of the powers he has oversight of. Further details are included in **Chapter 7.3** 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 103 irregularities reported to the Commissioner and for other public authorities, there were 24. The Commissioner outlines that these irregularities included pre-emptive activity before the authorisation had been granted through misunderstanding or poorly completed checks, overdue switching off of a recording device once an authorisation had been cancelled and the use of a CHIS without an authorisation for use and conduct.

The Commissioner is clear that there is nothing to suggest wilful misconduct or bad faith in relation to any of these irregularities and that a total of 127 irregularities is an extremely small proportion of the total number of authorisations.

The Commissioner concludes in his report that: "The public can be reassured that these powers are almost always used only when necessary and proportionate and to ensure that those who are planning or have committed offences or acts that threaten the safety and well-being of the public, are held to account."[44]

43 The Commissioner's annual reports can be found in full at https://osc.independent.gov.uk/

44 "Annual Report of the Chief Surveillance Commissioner for 2014-2015" (then the Rt Hon Sir Christopher Rose), paragraph 5.56, page 31.

8.5 – Investigatory Powers Tribunal

The Investigatory Powers Tribunal (IPT) was established in October 2000 under Part IV of the Regulation of Investigatory Powers Act 2000 (RIPA). It is one part of a range of oversight provisions that ensure public authorities act in a way that is compatible with the Human Rights Act 1998, which translated the European Convention on Human Rights into UK law.[45]

The IPT is independent of Government and ensures that members of the public have an effective right of redress if they believe they have been a victim of unlawful action under RIPA, or wider human rights infringements in breach of the Human Rights Act 1998. Members of the IPT must be senior members of the legal profession and both the president and vice president must have held high judicial office. There are currently ten members of the IPT. The President, Mr Justice Burton, is a serving judge of the High Court of Justice, Queen's Bench Division (Commercial Court) and Chairman of the Central Arbitration Committee. The current Vice President is Mr Justice Mitting, who is also a serving judge of the High Court of Justice, Chancery Division.

The Tribunal investigates and determines two types of application on behalf of the public. First, interference complaints against a broad range of public authorities, including law enforcement and intelligence agencies, that use the investigatory powers regulated under RIPA. Such a complaint can concern any interference a member of the public believes has taken place against their person, property or communications and can relate to a range of investigatory powers including interception, communications data acquisition, surveillance and property interference.

Second, the Tribunal handles human rights claims relating to the use of covert techniques by intelligence, military and law enforcement agencies, as well as a wider range of human rights breaches believed to have been committed by the intelligence agencies.

Members of the public are free to make interference complaints against public authorities to the ordinary courts. However, there will be certain complaints about alleged human rights breaches by the intelligence agencies where the IPT will be the only court able to investigate the claim.

IPT Statistics

During 2014, the IPT received 215 new cases and decided 211 cases. Out of these 211 cases, 104 (49%) 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 always taken by at least two Tribunal Members. In 61 (29%) of the cases, there was a "no determination outcome". This means that the Tribunal ruled there was no unlawful or unreasonable activity involving the complainant. Thirty six (17%) cases were ruled to be out of the Tribunal's jurisdiction, or were either withdrawn or invalid. Eight (4%) cases were ruled to be out of time and in 2 (1%) cases, the Tribunal found in favour.

[45] The Human Rights Act 1998 is available at www.legislation.gov.uk/ukpga/1998/42/contents

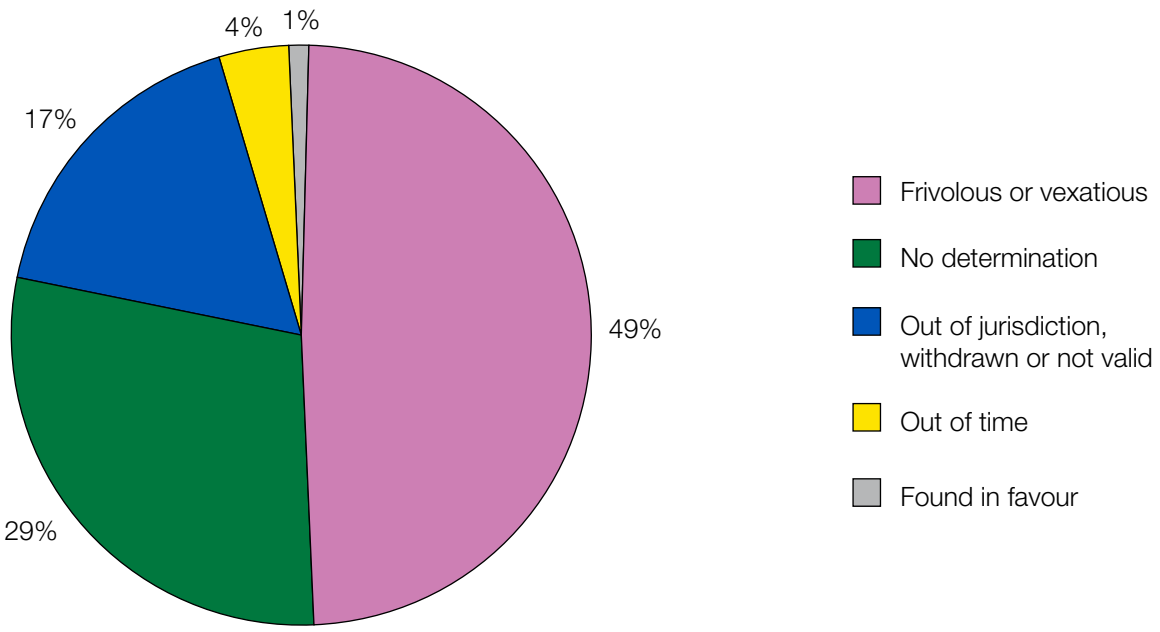


Figure 8: Outcomes of cases decided at the IPT, 2014

Details of all of the cases received and decided by the IPT, between 2010 and 2014, are at **ANNEX E**.[46]

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

9 – Recommended Reading List

Legislation

- **Anti-social Behaviour, Crime and Policing Act 2014** – www.legislation.gov.uk/ukpga/2014/12/contents
- **Counter-Terrorism and Security Act 2015** – http://services.parliament.uk/bills/2014-15/counterterrorismandsecurity/documents.html
- **Data Protection Act 1998** – www.legislation.gov.uk/ukpga/1998/29/contents
- **Data Retention and Investigatory Powers Act 2014** – www.legislation.gov.uk/ukpga/2014/27/contents/enacted
- **Data Retention Regulations 2014** – www.legislation.gov.uk/uksi/2014/2042/contents/made
- **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
- **Intelligence Services Act 1994** – www.legislation.gov.uk/ukpga/1994/13/contents
- **Justice and Security Act 2013** – www.legislation.gov.uk/ukpga/2013/18/contents
- **Police Act 1997** – www.legislation.gov.uk/ukpga/1997/50/contents
- **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

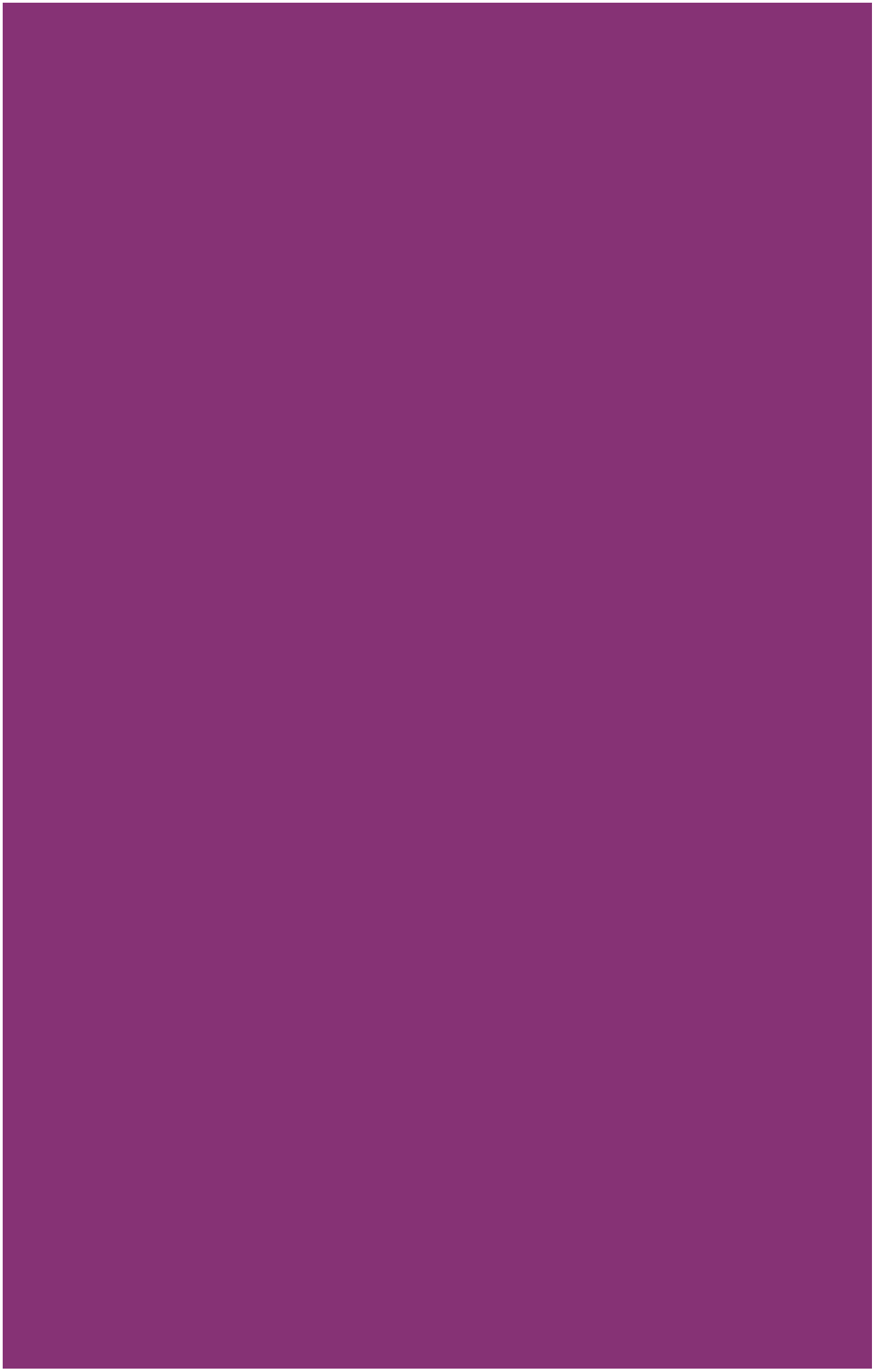
Government Publications

- **CONTEST: The United Kingdom's Strategy for Countering Terrorism** – www.gov.uk/government/collections/contest
- **CONTEST Annual Report for 2014** – www.gov.uk/government/collections/contest
- **Counter-Terrorism Statistics, Operation of Police Powers under the Terrorism Act 2000** – www.gov.uk/government/collections/counter-terrorism-statistics
- **HM Government Serious and Organised Crime Strategy** – www.gov.uk/government/publications/serious-organised-crime-strategy
- **HM Government Serious and Organised Crime Strategy Annual Report for 2014** – https://www.gov.uk/government/collections/serious-and-organised-crime-strategy
- **Second Annual Report of the National Crime Agency 2014/2015** – https://www.gov.uk/government/publications/second-annual-report-of-the-national-crime-agency-nca
- **Statistics on Closed Material Procedure** – www.gov.uk/government/publications/use-of-closed-material-procedure-report-25-june-2014-to-24-june-2015
- **Statistics on Terrorist Asset-Freezing** – www.gov.uk/government/collections/operation-of-the-uks-counter-terrorist-asset-freezing-regime-quarterly-report-to-parliament
- **Statistics on Terrorism Prevention and Investigation Measures** – www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2015-09-17/HLWS198/
- **Tackling Extremism in the UK, Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism, December 2013** – www.gov.uk/government/publications/tackling-extremism-in-the-uk-report-by-the-extremism-taskforce

Independent Publications

- **A Question of Trust: Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation** – https://terrorismlegislationreviewer.independent.gov.uk/
- **Chief Surveillance Commissioner, Annual Report 2014/2015** – https://osc.independent.gov.uk/
- **Independent Reviewer of Terrorism Legislation, Annual Reports (Terrorism Acts, TPIMs, Asset-Freezing)** – https://terrorismlegislationreviewer.independent.gov.uk/category/reports
- **Intelligence and Security Committee, Report on Privacy and Security** – http://isc.independent.gov.uk/committee-reports/special-reports
- **Intelligence Service Commissioner, Annual Report for 2014** – http://intelligencecommissioner.com

- **Interception of Communications Commissioner, Annual Report 2014 and half-yearly report** – www.iocco-uk.info
- **Investigatory Powers Tribunal, Case Statistics and Judgments** – www.ipt-uk.com
- **Royal United Services Institute, Independent Surveillance Review** – www.rusi.org



10 – ANNEXES

ANNEX A – Terrorist Asset-Freezing Figures, 1 April 2015 – 30 June 2015

	TAFA 2010	EU Reg(EC) 2580/2001	Al-Qaida regime UNSCR 1989
Assets frozen (as at 30/06/2015)	£39,000	£11,000[46]	£53,000[47]
Number of accounts frozen in UK (at 30/06/2015)	49	10	21
New accounts frozen (during Q2 2015)	11	0	0
Accounts unfrozen (during Q2 2015)	3	0	4
Total number of designations (at 30/06/2015)	30	33	304
Number of designations that were confidential	0	N/A	N/A
(i) New designations (during Q2 2015, including confidential designations)	0	0	3
(ii) Delistings (during Q2 2015)	1	0	7
(iii) Individuals in custody in UK (at 30/06/2015)	3	0	0
(iv) Individuals in UK, not in custody (at 30/06/2015)	1	0	3
(v) Individuals overseas (at 30/06/2015)	19	10	230
(vi) Groups	7	23	71
Individuals by Nationality			
(i) UK Nationals[48]	9	n/a	n/a
(ii) Non UK Nationals	14		
Renewal of designation (during Q2 2015)	2	n/a	n/a

47 This does not duplicate funds frozen under TAFA.

48 This figure reflects the most up-to-date account balances available and includes approximately $64,000 of funds frozen in the UK. This has been converted using exchange rates as of 31/12/2014. Additionally the figures reflect an updating of balances of accounts for certain individuals during the quarter, depleted through licensed activity.

49 Based on information held by the Treasury, some of these individuals hold dual nationality.

	TAFA 2010	EU Reg(EC) 2580/2001	Al-Qaida regime UNSCR 1989
General Licences			
(i) Issued in Q2		(i) 0	
(ii) Amended		(ii) 0	
(iii) Revoked		(iii) 0	
Specific Licences:			
(i) Issued in Q2	6	0	1
(ii) Amended	0	0	0
(iii) Expired	1	0	0
(iv) Refused	1	0	0

ANNEX B – Proscribed Organisations

- 67 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 and is therefore accurate as at that time.

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.

INTERNATIONAL TERRORIST ORGANISATIONS

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 for 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-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 AlAl 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 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 an Order, in July 2013, which provided that the **al-Nusrah Front (ANF)** and **Jabhat al-Nusrah li-ahl 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.

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 is 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.

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.

Hezb-E Islami Gulbuddin (HIG) – *Proscribed October 2005*

Led by Gulbuddin Hekmatyar who is in particular very anti-American, HIG is anti-Western and desires the creation of a fundamentalist Islamic State in Afghanistan.

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.

International Sikh Youth Federation (ISYF) – *Proscribed March 2001*

ISYF is an organisation committed to the creation of an independent state of Khalistan for Sikhs within India.

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 also reported to 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 2001and 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.

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.

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.

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.

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 another name 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.

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.

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**.

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.

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.

ORGANISATIONS 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 C – Case studies demonstrating the use of communications data

Catherine Wells-Burr – murder: On 12 September 2012 the badly burned body of Catherine Wells-Burr was discovered in her car. Her partner Rafal Nowak told police that she had been receiving text messages from a mystery male, and had driven to the arson scene to meet him. However, communications data revealed that Nowak and two co-conspirators were responsible for her death. It revealed that the mystery male was a fabrication in order to cover up their crime, and that the offenders had communicated secretly using "covert" phones. Furthermore, IP data showed that online accounts had been set up in the name of the mystery male, and on pornographic dating sites in the victim's name to create the illusion that she was promiscuous. All three were found guilty of the murder, and in June 2013 were sentenced to serve a minimum of 32 years each.

CD was the critical investigative tool that uncovered the offenders' deception in this case.

Mohammed Benares – terrorism offences: Mohammed Benares was arrested by West Midlands Police in March 2012 after downloading material from an online magazine linked to al-Qaeda, including instructions on bomb-making and weapons handling. During the trial in June 2013, communications data obtained from his mobile phone demonstrated contact with known radical Islamic preachers. This discredited his claim of innocent curiosity in the material, and was instrumental in demonstrating his true ideology and mind set. He was convicted and jailed for two years.

CD was a critical tool in proving the offender's contacts with known radicalising influencers.

Innocence proven – rape: A 17 year old girl was subjected to a number of sexual offences, including rape, by a group of men. Communications data identified one of the perpetrators but it transpired that he had an identical twin brother who he shared an address with. They both matched the description given by the witness, and shared the same DNA profile. After examining location data for phones belonging to both brothers, police established which brother was in the area of the attack at the time, and which one was not. In December 2013 the culprit and a second defendant were found guilty of the offences and sentenced to 45 years imprisonment between them.

CD was the only tool in this case that enabled investigators to ascertain, which of the brothers was guilty.

Operation BULLFINCH – Oxford grooming case: CD was crucial during this investigation. It corroborated relationships between offending groups as well as between offenders and victims. These relationships had been developed over a significant period and CD that

had been retained for a period of several months was important in substantiating these relationships. Out of the nine suspects in the investigation, seven were found guilty of 58 out of 63 indictments. On 27 June 2013 five of the offenders were sentenced to life in prison.

CD was important in this case in identifying relationships between a complex group of offenders and victims.

ANNEX D – Total Communications Data Applications, and Notices and Authorisations, for each Public Authority under Chapter II of Part I of RIPA

This annex includes the total number of communications data applications, and notices and authorisations, under Chapter II of Part I of RIPA for each public authority that acquired communications data during 2014, as set out in the Report of the Interception of Communications Commissioner for 2014. The list excludes notices and authorisations that were granted under the urgent oral process.

Police Forces and Law Enforcement Agencies

	Total Applications	Total Notices & Authorisations		Total Applications	Total Notices & Authorisations
Avon & Somerset Constabulary	5,510	8,766	Metropolitan Police	45,249	94,630
Bedfordshire Police	1,864	2,468	Ministry of Defence Police	29	141
British Transport Police	1,218	1,298	National Crime Agency	24,665	41,716
Cambridgeshire Constabulary	820	1,419	Norfolk Constabulary & Suffolk Police	1,839	2,414
Cheshire Constabulary	2,064	4,247	North Wales Police	1,228	2,342
City of London Police	1,049	2,174	North Yorkshire Police	1,017	1,538
Cleveland Police	1,336	5,591	Northamptonshire Police	1,473	3,194
Cumbria Constabulary	3,549	3,549	Northumbria Police	2,663	5,979
Derbyshire Constabulary	1,120	2,714	Nottinghamshire Police	4,268	10,023
Devon & Cornwall Police	5,228	8,467	Police Scotland	11,778	24,303
Dorset Police	710	1,879	Police Service of Northern Ireland	4,532	4,768
Durham Constabulary	1,256	4,145	Royal Air Force Police	11	16
Dyfed Powys Police	1,149	1,474	Royal Military Police	49	209
Gloucestershire Constabulary	807	2,465	Royal Navy Police	1	11
Greater Manchester Police	18,042	26,704	South Wales Police	1,814	4,977
Gwent Police	1,568	5,588	South Yorkshire Police	2,271	7,020
Hampshire Constabulary	3,596	9,335	Staffordshire Police	2,310	5,162
Hertfordshire Constabulary	4,708	8,723	Surrey Police	2,742	5,206
HMRC	6,219	10,397	Sussex Police	1,725	5,340
Humberside Police	1,525	2,653	Thames Valley Police	5,098	5,704

	Total Applications	Total Notices & Authorisations		Total Applications	Total Notices & Authorisations
Kent Police & Essex Police	8,403	15,785	The Home Office (Immigration Enforcement)	561	4,602
Lancashire Constabulary	4,203	11,471	Warwickshire Police & West Mercia Police	4,083	9,272
Leicestershire Police	2,171	4,942	West Midlands Police	14,095	33,780
Lincolnshire Police	745	1,496	West Yorkshire Police	6,655	15,239
Merseyside Police	4,678	22,230	Wiltshire Police	1,317	2,353
			Grand Total	**225,011**	**459,919**

The Civil Nuclear Constabulary, The Port of Dover Police and Port of Liverpool Police all reported to the Interception of Communications Commissioner's Office that they did not grant any Authorisations or give any Notices in 2014.

Some Police Forces share the services of a SPoC and where this is so combined figures are reported.

Intelligence Agencies

	Total Applications	Total Notices & Authorisations
GCHQ	1,291	1,291
The Secret Intelligence Service (Mi6)	298	652
The Security Service (Mi5)	39,815	48,639
Grand Total	**41,404**	**50,582**

Other Public Authorities

	Total Applications	Total Notices & Authorisations		Total Applications	Total Notices & Authorisations
Air Accident Investigation Branch	6	10	Information Commissioner's Office	28	35
Criminal Cases Review Commission	2	2	Marine Accident Investigation Branch	1	1
Department for Business, Innovation & Skills	8	22	Maritime and Coastguard Agency	3	3

	Total Applications	Total Notices & Authorisations		Total Applications	Total Notices & Authorisations
Department of Enterprise Trade & Investment (Northern Ireland)	28	167	Medicines and Healthcare Products Regulatory Agency	61	102
Department for Environment, Food & Rural Affairs	2	3	Ministry of Justice – National Offender Management Service	55	84
Department of Work & Pensions – Child Maintenance Group	21	30	NHS Protect	4	10
Environment Agency	22	22	Office of Communications	21	58
Financial Conduct Authority	224	3,768	Office of Fair Trading/Competition and Markets Authority	2	2
Gambling Commission	8	12	Office of the Police Ombudsman for Northern Ireland	2	2
Gangmasters Licensing Authority	20	35	Rail Accident Investigation Branch	2	2
Health & Safety Executive	3	11	Royal Mail	71	164
Independent Police Complaints Commission	13	30	Serious Fraud Office	32	50
			Grand Total	**639**	**4,625**

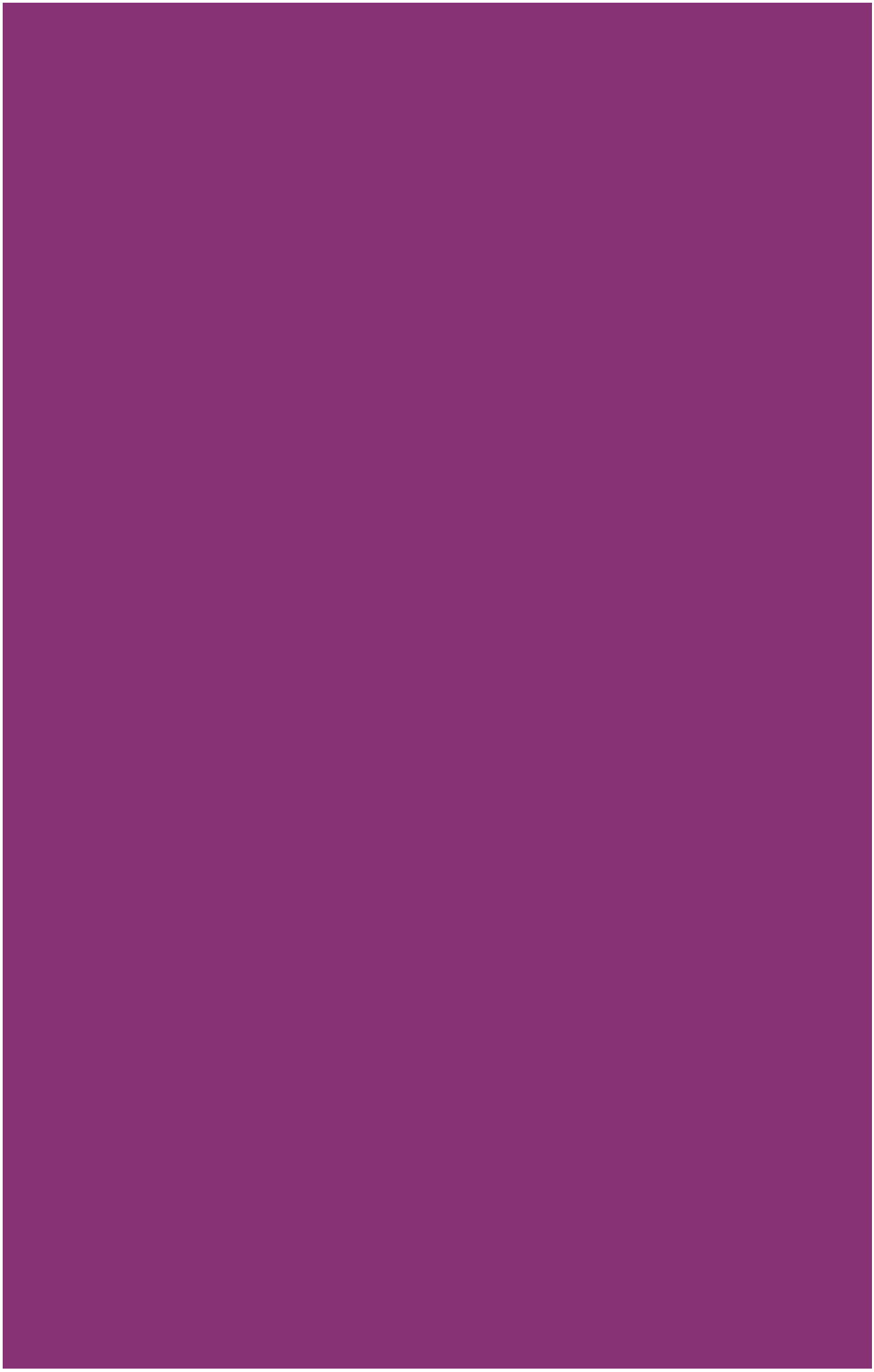
The following "other" public authorities reported to the Interception of Communications Commissioner's Office that they did not grant any Authorisations or give any Notices during 2014:

- Charity Commission
- Department of Environment Northern Ireland
- Department of Agriculture and Rural Development Northern Ireland
- Food Standards Agency
- NHS Scotland Counter Fraud Services
- Northern Ireland Office – Northern Ireland Prison Service
- Northern Ireland Health & Social Services Central Services Agency
- Pensions Regulator
- Prudential Regulation Authority
- Scottish Criminal Cases Review Commission
- Scottish Environmental Protection Agency
- All Fire Authorities
- All Ambulance Services/Trusts

Local Authorities

	Total Applications	Total Notices & Authorisations		Total Applications	Total Notices & Authorisations
Aberdeenshire Council	1	1	Glasgow City Council	1	7
Barnsley Metropolitan Borough Council	2	2	Gloucestershire County Council	3	9
Bedford Borough Council	2	2	Hambleton District Council	1	4
Birmingham City Council	12	23	Hampshire County Council	5	5
Blackburn with Darwen Borough Council	2	11	Hartlepool Borough Council	1	21
Blackpool Borough Council	2	3	Hertfordshire County Council	2	15
Bolton Metropolitan Council	2	6	Huntingdonshire District Council	2	2
Bracknell Forest Borough Council	1	2	Isle of Wight Council	1	4
Bridgend County Borough Council	2	4	Kent County Council	25	127
Bristol City Council	3	3	Kingston upon Hull City Council	1	1
Buckinghamshire County Council	5	30	Knowsley Metropolitan Borough Council	1	2
Bury Metropolitan Borough Council	5	8	Lancashire County Council	12	46
Caerphilly County Borough Council	2	6	Leicestershire County Council	5	11
Cambridgeshire County Council	4	5	Lincolnshire County Council	8	13
Cardiff City and County Council	3	4	Liverpool City Council	8	23
Ceredigion County Council	1	1	London Borough of Barnet	2	33
Cheshire East Council	3	7	London Borough of Brent	1	2
Cheshire West & Chester Council	9	21	London Borough of Bromley	4	21
City of London Corporation	1	2	London Borough of Enfield	1	5
Cornwall County Council	2	14	London Borough of Hammersmith and Fulham	1	19
Coventry City Council	7	32	London Borough of Havering	3	12
Darlington Borough Council	4	5	London Borough of Hillingdon	1	2
Derbyshire County Council	1	1	London Borough of Islington	3	7
Devon County Council & Somerset Council	5	9	London Borough of Newham	34	1,173
Dudley Metropolitan Borough Council	2	6	London Borough of Redbridge	3	28
Durham County Council	1	8	London Borough of Wandsworth	1	2
East Dunbartonshire Council	1	3	Manchester City Council	1	4
East Riding of Yorkshire Council	1	1	Milton Keynes Council	2	16
East Sussex County Council	1	11	Neath Port Talbot County Borough Council	2	7
Flintshire County Council	3	4	Norfolk County Council	1	3
Gateshead Metropolitan Borough Council	5	8	North Lanarkshire Council	2	3

	Total Applications	Total Notices & Authorisations		Total Applications	Total Notices & Authorisations
North Lincolnshire Council	7	10	St Helens Metropolitan Borough Council	8	16
Northamptonshire County Council	2	5	Staffordshire County Council	2	2
Northumberland County Council	2	6	Stirling Council	1	3
Oldham Metropolitan Borough Council	5	11	Stockport Metropolitan Borough Council	2	6
Oxfordshire County Council	1	5	Stockton-on-Tees Borough Council	1	2
Perth and Kinross Council	2	13	Stoke-on-Trent City Council	1	1
Redcar & Cleveland BC	1	6	Suffolk County Council	1	3
Rhondda Cynon Taff County BC	4	13	Swansea City and County Council	5	20
Rotherham Borough Council	3	3	Tameside Metropolitan Borough Council	1	3
Royal Borough of Greenwich	2	3	Test Valley Borough Council	1	1
Royal Borough of Kensington and Chelsea	1	1	Thurrock Council	5	23
Salford City Council	1	2	Torbay Borough Council	1	2
Sheffield City Council	3	4	Warrington Council	4	19
Slough Borough Council	1	2	Watford Borough	2	2
South Gloucestershire Council	6	13	West Berkshire Council	3	14
Southampton City Council	1	14	West Lothian Council	2	4
			York City Council	4	8
			Grand Total	**319**	**2,110**



ANNEX E – Decisions made in cases at the Investigatory Powers Tribunal, 2010-2014

Year	New Cases Received	Cases Decided	Decision Breakdown
2010	164	210	99 (47%) received a 'no determination' outcome
			65 (31%) were ruled as 'frivolous or vexatious'
			18 (8.5%) were ruled out of jurisdiction
			15 (7%) were ruled out of time
			6 (3%) were found in favour
			4 (2%) were judged to be not a valid complaint
			3 (1.5%) were withdrawn
2011	180	194	86 (44%) were ruled as 'frivolous or vexatious'
			72 (36%) received a 'no determination' outcome
			20 (11%) 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
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	211	104 (49%) were ruled as frivolous or vexatious
			61 (29%) received a 'no determination' outcome
			36 (17%) were ruled out of jurisdiction, withdrawn or not valid
			8 (4%) were ruled out of time
			2 (1%) Found in Favour

ISBN 978-1-4741-2561-1