| | |
|---|---|
| **Title:** Investigatory Powers Bill – Interception<br>**IA No:** HO0198<br>**Lead department or agency:**<br>Home Office<br>**Other departments or agencies:**<br>FCO, Cabinet Office, NIO, GCHQ, MI5, SIS, NCA, MPS, PSNI, Police Scotland, HMRC | **Impact Assessment (IA)**<br>**Date:** 4 November 2015<br>**Stage:** Consultation<br>**Source of intervention:** Domestic<br>**Type of measure:** Primary legislation<br>**Contact for enquiries:** investigatorypowers@homeoffice.gsi.gov.uk |

## Summary: Intervention and Options

**RPC Opinion:** Not Applicable

| Cost of Preferred (or more likely) Option | | | | |
|---|---|---|---|---|
| **Total Net Present Value** | **Business Net Present Value** | **Net cost to business per year** (EANCB on 2009 prices) | **In scope of One-In, Measure qualifies as One-Out?** | |
| £0m | £0m | £0m | No | NA |

**What is the problem under consideration? Why is government intervention necessary?**

Increasingly terrorists and criminals are using a range of services provided by domestic and overseas communications companies to radicalise, recruit and plan their attacks, commit crime and evade detection. Our law enforcement and security and intelligence agencies must ~~be able to continue to access terrorists~~ and criminals' communications on these services to counter these threats and protect the public. In order to maintain interception capability, new legislation must be enacted before the sunset provision in the Data Retention and Investigatory Powers Act 2014 (DRIPA), which clarified the extra-territoriality of the Regulation of Investigatory Powers Act 2000 (RIPA), takes effect on 31 December 2016.

**What are the policy objectives and the intended effects?**

This legislation will seek to ensure that agencies are able to continue to intercept the communications, both targeted and in bulk, of terrorists and serious criminals where it is necessary and proportionate to do so. It does not seek to extend the UK's reach or increase the powers of agencies beyond the original intention of RIPA and subsequent clarification in DRIPA. Legislation will also respond to recommendations laid out in David Anderson QC's report into the UK's investigatory powers regime, as well as recommendations made by the Intelligence Services Committee of Parliament (ISC) and Royal United Services Institute (RUSI).

**What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)**

OPTION 1: No legislation / do nothing.

OPTION 2: Legislate to maintain current targeted and bulk interception capabilities provided for under RIPA and DRIPA, subject to additional safeguards and oversight as recommended by David Anderson, the ISC and RUSI; and to ensure that these capabilities can be maintained after DRIPA sunsets in December 2016.

**Will the policy be reviewed?** It will be reviewed. **If applicable, set review date:** December 2021

| | | | | | |
|---|---|---|---|---|---|
| Does implementation go beyond minimum EU requirements? | | | N/A | | |
| Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base. | **Micro**<br>No | **< 20**<br>No | **Small**<br>No | **Medium**<br>No | **Large**<br>No |
| What is the $CO_2$ equivalent change in greenhouse gas emissions? (Million tonnes $CO_2$ equivalent) | | | **Traded:**<br>N/A | **Non-traded:**<br>N/A | |

***I have read the Impact Assessment and I am satisfied that (a) it represents a fair and reasonable view of the expected costs, benefits and impact of the policy, and (b) that the benefits justify the costs.***

Signed by the responsible Minister ..... Date: 3/11/15

# Summary: Analysis & Evidence

Policy Option 1

**Description:** No legislation / do nothing

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low:** | **High:** | **Best Estimate:** 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | | | | |
| **High** | | | | |
| **Best Estimate** | 0 | | 0 | 0 |

**Description and scale of key monetised costs by 'main affected groups'**

This is the baseline option. There are no additional monetised costs associated with this option.

**Other key non-monetised costs by 'main affected groups'**

This is the baseline option. There are no additional non-monetised costs associated with this option.

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| **Low** | | | | |
| **High** | | | | |
| **Best Estimate** | 0 | | 0 | 0 |

**Description and scale of key monetised benefits by 'main affected groups'**

This is the baseline option. There are no additional monetised benefits associated with this option.

**Other key non-monetised benefits by 'main affected groups'**

This is the baseline option. There are no additional non-monetised costs associated with this option.

Key assumptions/sensitivities/risks — **Discount rate (%)** 3.5

A failure to respond to the recommendations made by David Anderson, RUSI and the ISC could have an impact on public confidence and the willingness of some communications service providers to cooperate with law enforcement and security and intelligence agencies on interception. If this were realised, the resulting loss of intelligence poses a number of risks. It would lead to a rapid degradation of the operational capabilities of our law enforcement and security and intelligence agencies, and severely undermine their ability to investigate and protect the public from threats such as that of terrorism and serious crime.

**BUSINESS ASSESSMENT (Option 1)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OIOO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** 0 | **Benefits:** 0 | **Net:** 0 | Yes | NA |

# Summary: Analysis & Evidence

Policy Option 2

**Description:** Legislate to maintain current interception capabilities

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low: 0** | **High: 0** | **Best Estimate:** 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | N/K | | N/K | **N/A** |
| **High** | N/K | | N/K | **N/A** |
| **Best Estimate** | 0 | | 0 | **0** |

**Description and scale of key monetised costs by 'main affected groups'**

There are no additional costs when compared to OPTION (1) other than those associated with a new two-stage authorisation regime and compliance with safeguards and oversight processes in the Bill. The cost of implementing this system are considered separately in the Oversight Impact Assessment.

**Other key non-monetised costs by 'main affected groups'**

None.

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| **Low** | | | | |
| **High** | | | | |
| **Best Estimate** | N/K | | N/K | **N/K** |

**Description and scale of key monetised benefits by 'main affected groups'**

None.

**Other key non-monetised benefits by 'main affected groups'**

Legislation will provide for greater safeguards and transparency, providing the public with greater confidence and assurance in the oversight and accountability of interception. Legislation will allow UK intercepting agencies to continue to investigate threats to ensure they can keep the public safe. Case studies highlighting the critical importance of interception to law enforcement and security and intelligence agencies are provided in the Evidence Base below.

Key assumptions/sensitivities/risks — **Discount rate (%)** 3.5

Assumptions and risks are detailed in the Evidence Base. Key risks are:

- Non-cooperation from communication service providers (CSPs)
- Technological challenges

**BUSINESS ASSESSMENT (Option 2)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OIOO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** 0 | **Benefits:** 0 | **Net:** 0 | Yes | N/A |

# Evidence Base

## A. Problem under consideration

Background

Interception is the act of obtaining and making available the contents of communications sent via a telecommunications system or public postal service to a person who is neither the sender nor intended recipient. Warranted interception is a powerful tool for law enforcement and the security and intelligence agencies in tackling threats such as serious crime and terrorism. The use of interception by the state is limited to only a few agencies, for a limited range of purposes set out in legislation on both a targeted basis, and in bulk, to allow the agencies to discover new targets. It is subject to strong internal controls and independent oversight.

Interception in the UK is used as a source of intelligence, and is a vital tool in the fight against serious crime and terrorism. Intelligence derived from interception helps law enforcement to identify and disrupt threats from terrorism and serious crime, and enable arrests. It can provide real-time intelligence on the plans and actions of terrorists and criminals, allowing law enforcement to identify opportunities to seize prohibited drugs / firearms / the proceeds of crime, and to disrupt or frustrate their plans. Interception of communications enables the gathering of evidence against terrorists and criminals, and means that they can be arrested and prosecuted.

Interception also ensures that finite law enforcement and agency resources – money and staff – are used to best effect. While other investigative techniques and intelligence-gathering methods may be deployed by law enforcement and/or security and intelligence agencies as part of an investigation where required, not all are necessarily available in all cases where interception is currently used. These techniques may also be more intrusive, increase costs and operational risks, and, crucially, may not provide the same insight and assurance as interception.

Existing legal framework

Interception is one of the most intrusive powers available to the state and is subject to a strict authorisation and oversight regime. The use of interception is currently governed by the Regulation of Investigatory Powers Act 2000 (RIPA). Interception can only be used for purposes relating to serious crime, national security, or the protection of the UK's economic wellbeing where that relates to national security. The power to intercept communications is limited to the following organisations:

- The Security Service (MI5);
- The Secret Intelligence Service (SIS);
- Government Communications Headquarters (GCHQ);
- The National Crime Agency;
- The Metropolitan Police Service;
- The Police Service of Northern Ireland;
- Police Scotland;
- Her Majesty's Revenue and Customs; and
- The Ministry of Defence.

Under the current regime, a warrant issued by the Secretary of State must consider the necessity and proportionality of the proposed interception and whether the information collected through interception could reasonably be obtained by other means. We propose to maintain this important safeguard.

The security and intelligence agencies (SIA) (MI5, SIS and GCHQ) are able to acquire the content of communications in bulk, under section 8 of the Regulation of Investigatory Powers Act (2000). The new legislation will ensure that the security and intelligence agencies can continue to acquire and examine bulk interception data when it is necessary and proportionate for them to do so. Bulk interception warrants will be focused on the communication of those who are based outside the UK, as is currently the case. They will continue to be used to identify new and emerging threats and quickly establish links between priority investigations. The ability to acquire interception data in bulk remains a crucial factor in being able to both track known threats and targets, and discover those that were hitherto unknown.

As currently, given the intrusive nature of acquiring data in bulk the power will continue to be available only to protect national security and to prevent serious crime. The Investigatory Powers Bill will provide clearer safeguards in relation to bulk interception. A decision to issue a warrant will continue to be made by the Secretary of State with the additional approval of a judicial commissioner. As is currently the case, the process for access, retention, storage, destruction, disclosure and auditing of bulk interception will be set out in detail in the accompanying Code of Practice.

The Data Retention & Investigatory Powers Act 2014 (DRIPA) was enacted to respond to the challenges presented by the changing nature of the global telecommunications market; it clarifies RIPA by putting beyond doubt the obligations imposed on services provided from outside the UK. DRIPA is due to sunset in December 2016.

The Challenge

When RIPA was enacted 15 years ago, it was intended to provide a legislative regime fit for the information age. Since then, it has broadly kept pace with changing technology.

However, the increasing globalisation of the telecommunications market has brought about new challenges. The days when we all relied on a small number of domestic telecommunications companies to communicate with each other are in the past. Today, we use a wide range of communication methods sourced from a range of global providers to live our everyday lives. And so do those that mean to do us harm.

It is now part of everyday life for people in the UK to communicate using services such as social media, instant messaging and web-based e-mail provided by overseas companies. These companies may not have any physical infrastructure in the UK and the services they provide are innovative, diverse and ever expanding. It is not, therefore, surprising that the nature of the national security threat has been affected by technological developments and diversification.

The changing nature of global communications means that suspects in national security and serious crime investigations are increasingly making use of communications services provided from overseas. This issue was addressed through the enactment of DRIPA, which is due to sunset in December 2016. In addition, through DRIPA, 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 agency investigatory powers, specifically including the interception of communications. David Anderson's Report, entitled "A Question of Trust", was published in June 2015 and includes a number of interception-related recommendations for the Government to consider alongside the recommendations put forward in the ISC's report entitled "Privacy and Security: A modern and transparent legal framework" (March 2015) and RUSI's report entitled "A Democratic License to Operate" (July 2015).

## B. Rationale for Intervention

Interception is a vital tool for law enforcement, armed forces and security and intelligence agencies and they are heavily reliant on it for intelligence gathering purposes. Any reduction in cooperation will have a serious impact on national security and the ability to prevent or detect serious crime. We need to continue to ensure that there is no doubt that interception obligations apply equally to all companies who provide communications services to, or have infrastructure in the UK, and that new legislation captures the range of services that are inevitably used by terrorists and criminals in their attack planning and criminal activities.

## C. Policy Objective

The objective of new legislation is to ensure that law enforcement, armed forces and security and intelligence agencies are able to continue to intercept the communications of terrorists and serious criminals where it is necessary and proportionate to do so. This will maintain their ability to intercept the communications of those who wish to do us harm. It does not seek to extend the UK's reach or increase the powers of law enforcement, armed forces and security and intelligence agencies beyond the original intention of RIPA and subsequent clarification in DRIPA.

New legislation will also have the objective of responding to specific interception-related recommendations made by David Anderson, RUSI and the ISC.

## D. Options

Two policy options have been considered:

OPTION 1: No legislation / do nothing;

OPTION 2: Legislate to maintain current interception capabilities provided for under RIPA and DRIPA, subject to additional safeguards, and oversight as recommended by David Anderson, the ISC and RUSI; and to ensure that these capabilities can be maintained after DRIPA sunsets in December 2016.

## E. Appraisal (Costs and Benefits)

**OPTION (1) – No legislation / do nothing**

RIPA provides for obligations to be imposed on anyone providing telecommunications services to customers in the UK. However, it is not currently explicit that obligations may be imposed on companies overseas. DRIPA sought to address the issue of extra-territoriality, but it is due to sunset in December 2016.

Costs of Option 1

This is the baseline option, there will be no additional costs under this option.

Benefits of Option 1

There will be no additional benefits under this option. Given the public and media concerns around the use of investigatory powers, maintaining the status quo would invite considerable criticism and risk further undermining public confidence in the current arrangements.

Risks of Option 1

This option could potentially see declining public confidence in the current interception regime, which may have a bearing on the willingness of some communications service providers to work with law enforcement and the security and intelligence agencies. If the risk of reduced cooperation were realised, the resulting loss of intelligence following an expected decline in cooperation poses a number of risks. It would lead to a rapid degradation of the operational capabilities of our law enforcement and security and intelligence agencies, and severely undermine their ability to investigate and protect the public from the threat of terrorism and serious crime. More crimes would go unsolved and the public could be put at risk.

This option would force intercepting agencies to attempt to mitigate the loss of intercept-related intelligence through increased use of other investigative techniques and intelligence-gathering methods. These techniques are already available to law enforcement, armed forces and security and intelligence agencies, subject to the same necessity and proportionality considerations as interception, and may currently be deployed as part of an investigation where required. However, some of these techniques are particularly intrusive and resource-intensive (and may also carry higher costs and operational risks), would not necessarily be available in all cases where interception is currently used, and most importantly would not provide the same insight and assurance as interception.

**OPTION (2) – Legislate to maintain current interception capabilities provided for under RIPA and DRIPA, subject to additional safeguards and oversight as recommended by David Anderson, the ISC and RUSI**

This option would secure public support for the capabilities in RIPA and DRIPA, enabling law enforcement, armed forces and security and intelligence agencies to continue to intercept the communications of terrorists and serious criminals where it is necessary and proportionate to do so.

This option includes a new, 'double-lock' authorisation system which will create additional safeguards for interception warrants. The specific details of this system, including cost implications and benefits, are discussed separately in the Oversight Impact Assessment.

Costs of Option 2

There are no extra costs when compared with OPTION (1) other than those associated with a new authorisation model (considered separately in the Oversight IA). Under section 14 of RIPA, HMG already provides a "fair contribution" towards the costs of warranted interception to CSPs subject to RIPA obligations. In practice, this has been up to 80% of the capital cost of new interception capabilities and 100% of the ongoing operational costs. Where a CSP expands its network, it is expected to meet any increased capital costs of interception that arise. CSPs' capital costs are paid by the Home Office, while the operational costs are met by the intercepting agencies. Costs of interception are not made public so that inferences cannot be drawn about the nature of these capabilities. As the current regime is simply being replicated through new legislation, the principle of "fair contribution" will continue as before.

Benefits of Option 2

Legislation will improve the oversight and safeguards that apply to the interception of communications, giving the general public greater confidence in the transparency and accountability of the state's ability to interfere with communications. There will also be benefit to the general public of the continued ability by the UK intercepting agencies to continue to investigate threats to ensure they can keep the public safe. It will enable law enforcement

agencies to continue to intercept the communications of a member of a serious organised crime group arranging the importation of arms or Class A drugs; to identify where the pick-up is going to take place so they can do something about it. It will enable security and intelligence agencies to continue to intercept the communications of a would-be terrorist planning an attack in the UK; to identify who he is talking to, what he is planning to do and when, and to disrupt the plot before it is carried out.

It is difficult to monetise the benefits accruing from interception, as the capability provides only part of the intelligence picture in national security, economic wellbeing where it relates to national security and serious crime investigations. Therefore while the role played by interception is vital, it is difficult to distinguish what benefits arise specifically from interception alone. However, the following data and case studies highlight the critical importance of interception to law enforcement and intelligence agencies:

- Since 2010, the majority of MI5's top priority UK counter-terrorism investigations have used intercepted material in some form to identify, understand or disrupt plots seeking to harm the UK and its citizens. In 2013, this was estimated to be 15-20% of the total intelligence picture in counter-terrorism investigations. *[Source: "A Question of Trust", p126, para 7.12(a)]*

- Data obtained from the NCA suggested that in 2013/14, interception played a critical role in investigations that resulted in:

    - Over 2,200 arrests;
    - Over 750kg of heroin and 2,000kg of cocaine seized;
    - Over 140 firearms seized; and
    - Over £20m seized. *[Source: "A Question of Trust, p126, para 7.12(b)]*

- In their evidence provided to David Anderson, law enforcement also highlighted the importance that intercepted material may be useful in other types of cases, ranging from corruption investigations to domestic murder. *[Source: "A Question of Trust, p126, para 7.12(c)]*

**CASE STUDY: A criminal investigation into a UK-based organized crime group involved in the importation of Class A drugs from South America**

Interception assisted in identifying the command and control structure of the group and their associates in other European countries. It identified individuals responsible for facilitating the supply of drugs and also those involved in establishing front companies for importing legal goods. Intercept provided intelligence on the modus operandi employed by the group, the dates and location of the importation, and the storage place of a series of drug shipments.

This resulted in the arrest of UK-based members of the group and their co-conspirators overseas, as well as the seizure of significant quantities of Class A drugs, foreign currency, firearms and ammunition. Intercept material provided key intelligence which was pivotal in building an evidential case and ended in the successful prosecution of the defendants. It also served to enhance the Serious Organised Crime Agency's (SOCA, now replaced by the NCA) working relationship with overseas partners involved in the investigation.

*[Source: "A Question of Trust", Annex 8, p334, paras1-2]*

**CASE STUDY: A criminal investigation into a pattern of escalating violence between a number of rival organized crime groups, including street gangs linked to the London drug economy, operating across the capital**

Intelligence derived from interception indicated a conflict between organised crime groups as each sought to control a greater section of the drugs market. The intelligence suggested the use of firearms

by the groups. This prompted immediate steps to tackle the group, with the intention of dismantling the network, disrupting the supply of Class A drugs, preventing further loss of life and arresting those involved. The operation also targeted individuals directly involved in gun possession and crime while disrupting other criminal activities such as small-scale drug dealing, acquisitive crime and serious assaults.

Intercepted material identified the individual co-ordinating the sale of significant amounts of Class A drugs, led to the location of his safe storage premises, and identified senior gang members involved in the supply chain. It also enabled junior gang members to be identified as couriers of the drugs to numerous locations across London, the Home Counties and beyond, including the method and timing transport. Interception also revealed that the head of the organised crime group was conspiring with others to shoot a rival. This led to an armed stop of the target while he was en route to the hit location. He was found to be in possession of a loaded firearm and arrested.

The primary operation led to the collapse of the network operating across London and the Home Counties. During the course of the operation, intelligence form interception led to the seizure of over 40 firearms, in excess of 200kg of Class A drugs, the seizure of over £500,000 of cash and over 100 arrests.

*[Source: "A Question of Trust", Annex 8, p334-5, paras8-11]*

Risks of Option 2

This option would mitigate the risks associated with the degradation of cooperation highlighted in OPTION (1), and would ensure that warranted interception could continue as before: law enforcement, armed forces and security and intelligence agencies would continue to be able to detect, investigate and prevent serious crime and terrorism.

This option assumes continued compliance from CSPs, with technology capable of facilitating interception. There is a risk that CSPs could refuse to comply and that interception technology is less effective.

Impact of Option 2

Currently, RIPA sets out the circumstances in which a company is required to maintain a permanent interception capability. It is however possible that a company may refuse to comply either with an interception warrant, or with a notice to maintain a permanent interception capability. In accordance with RIPA and DRIPA, we intend that new legislation will continue to make clear that companies can be obliged to provide assistance in relation to interception warrants.

We are also proposing new legislation makes clear that blocking and filtering is lawful (though not mandated), where it is necessary for the purposes connected with the restriction of access to material that is unlawful to publish or material which a subscriber has determined is otherwise unsuitable. Furthermore, we plan to clarify the definition of a stored communication (such as an email stored on a web-based server or saved voicemail) to put beyond doubt that it applies to communications stored on phones, tablets and other individual devices.

The Bill will also provide additional protections for the communications of Members of Parliament and other legislators. In addition to approval by a Judicial Commissioner, the Bill will state that the Prime Minister must be consulted before the Secretary of State can decide to issue a warrant to intercept an MP's communications. This will cover all warrants for targeted interception that are carried out by the Security and Intelligence Agencies. It will also include a requirement for Prime Ministerial authorisation prior to the selection for examination of a Parliamentarian's communications collected under a bulk warrant. It will apply to MPs,

members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments/Assemblies.

**DIRECT COSTS AND BENEFITS TO BUSINESS**

As under the current RIPA regime, new legislation would be designed to ensure that no public communications provider is either advantaged or disadvantaged by their interception obligations. As under current Part 1, Chapter 1 RIPA provisions, only those companies issued with a warrant will be required to provide interception capabilities. This legislation does not intend to introduce any new requirements for communications companies, or place any unnecessary burdens on them. We will work with communications companies to ensure that any requests for assistance could be carried out with the least amount of impact on their business.

The infrastructure to support the provision of warranted intercept is already in place. Under section 14 of RIPA, HMG already provides a "fair contribution" towards the costs of warranted interception to communications companies subject to RIPA obligations. This "fair contribution", current safeguards and prior consultation before obligations are imposed also minimise the effect on competition. The intention is for this process to be maintained under new legislation. The continuation of this system will also will ensure that there is no additional impact on small or micro firms which have interception obligations placed on them. It is worth noting that under the current regime, which will be replicated, very small companies (with under 10,000 customers) are unlikely to be obligated to provide a strategic / permanent interception capability, although they may still have tactical obligations to fulfil.

Section 13 of RIPA established the Technical Advisory Board (TAB), which provides an important safeguard for communications companies and the Government, and ensures that any disputes that arise from the obligations imposed on communications companies can be resolved satisfactorily. TAB's role, in the event of such a dispute, is to advise the Home Secretary on the reasonableness of a communications company's obligations. The TAB will continue to fulfil its interception function under new legislation.

## F. Risks

Our policy intention is to maintain the ability of law enforcement and intelligence agencies to intercept the communications of those who wish to do us harm.

If the risk associated with OPTION (1) were realised, loss of interception capability and the associated intelligence gaps would represent a significant loss for law enforcement and intelligence agencies, and would seriously undermine their ability to detect, investigate and prevent serious crime and terrorism, putting lives at risk. The intelligence gap which could arise under this option could be partially mitigated, but the additional monetary costs and the increased level of intrusion associated with deploying other investigative techniques in lieu of warranted intercept would be disproportionate.

We judge that the implementation of OPTION (2) would meet our policy objectives, and ensure the continued ability of law enforcement and intelligence agencies to detect, investigate and prevent serious crime and terrorism, mitigating the risk associated with OPTION (1). We assess that the benefits to the public of implementing this option greatly outweigh the limited cost of doing so. The infrastructure to support the provision of warranted intercept is already in place. HMG already provides a "fair contribution" towards the costs of warranted interception to communications companies subject to RIPA obligations. This will continue under new legislation.

Base costs of interception would remain the same as they do currently under both options, albeit that OPTION (2) will include some additional compliance and authorisation costs borne by the public sector which are detailed in a separate Impact Assessment (Oversight). However, if the risks associated with OPTION (1) were to materialise, the resulting intelligence gap would present a far higher risk to public safety and national security when compared with OPTION (2), which would mitigate these potential risks.

There is an ongoing risk with all options outlined above that technology will continue to evolve and develop rapidly, outpacing legislation. There is also a risk that in consolidating existing legislation criminals and terrorists will be more greatly aware of the capabilities of the security and intelligence agencies, armed forces and law enforcement to detect and prevent terrorism and serious crime, and will take new or additional measures to evade discovery.

## G. Implementation

The Government will introduce a Bill following any revisions necessary after pre-legislative scrutiny, in the New Year. The Bill will need to be enacted by 31 December 2016, by which point the Data Retention and Investigatory Powers Act will fall away.

## H. Monitoring and Evaluation

The proposed legislation will be scrutinised by a Joint Committee of Parliament, before being introduced in the early New Year. The application of the legislation will be scrutinised on an ongoing basis by the Investigatory Powers Commission, an independent body of the judiciary, responsible for oversight of the use of investigatory powers by all public authorities, who will provide yearly reports on the exercise of powers within the Bill. The Intelligence and Security Committee of Parliament will continue to oversee the activities of the security and intelligence agencies, including their exercise of investigatory powers. And the Investigatory Powers Tribunal will provide a right of redress to any individual who believes they have been unlawfully surveilled.

## I. Feedback

The Government recognises the importance of consulting as widely as possible with those affected by legislative proposals. This includes law enforcement, and Communication Service Providers. As such, the provisions contained within the proposed Bill have been consulted on across Government and with the intercepting agencies. They have also been shared with a limited number of Communications Service Providers to date. The Government is committed to continuing to work closely with the industry as the proposals are developed. The new Bill will be subject to pre-legislative scrutiny by a Joint Committee of Parliament in the autumn and subject to full public consultation. The Government will consider carefully the recommendations of the Joint Committee before bringing forward revised proposals for Introduction. Public consultation will also form part of the pre-legislative scrutiny process.