

Title: Investigatory Powers Act – Interception IA No: HO0266 Lead department or agency: Home Office Other departments or agencies: FCO, Cabinet Office, NIO, GCHQ, MI5, SIS, NCA, MPS, PSNI, Police Scotland, HMRC	Impact Assessment (IA)		
	Date: 3 March 2017		
	Stage: Enactment		
	Source of intervention: Domestic		
	Type of measure: Primary legislation		
Contact for enquiries: public.enquiries@homeoffice.gsi.gov.uk			

Summary: Intervention and Options	RPC Opinion: Green
--	---------------------------

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 Two-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, armed forces 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 was required before the sunset provision in the Data Retention and Investigatory Powers Act 2014 (DRIPA) which was due to take effect on 31 December 2016.

What are the policy objectives and the intended effects?

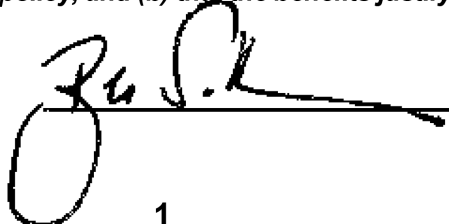
This legislation will ensure that agencies are able to continue to intercept the communications of terrorists and serious criminals where it is necessary and proportionate to do so. It does not extend the UK's reach or increase the interception powers of agencies beyond the original intention of RIPA and subsequent clarification in DRIPA. The legislation responds to recommendations 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). In drafting this legislation, the Government also considered recommendations made by the Joint Committee of both Houses of Parliament on the draft Bill, alongside the reports from the Intelligence and Security Committee and Commons Science and Technology Committee.

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

Option one: No legislation / do nothing.
 Option two: 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 the DRIPA sunset in December 2016.

Will the policy be reviewed? It will be reviewed. If applicable, set review date: June - Dec 2022						
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.		MicroYes	< 20 Yes	Small Yes	Medium Yes	Large Yes
What is the CO ₂ equivalent change in greenhouse gas emissions? (Million tonnes CO ₂ equivalent)				Traded: N/A		Non-traded: 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: 20-4-17

1

Summary: Analysis & Evidence

Policy Option 1

Description: Do nothing

FULL ECONOMIC ASSESSMENT

Price Base Year 2016	PV Base Year 2016	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	0	0	0
High	0	0	0
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 may be some additional non-monetised costs of this option in public confidence in the exercise of interception by the intercepting agencies, given the extensive reviews of investigatory powers.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0	0	0
High	0	0	0
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
<p>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.</p>		

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:	In scope of OIOO?	Measure qualifies as
Costs: 0	No.	NA
Benefits: 0		
Net: 0		

Summary: Analysis & Evidence

Policy Option 2

Description: Legislate to maintain current interception capabilities

FULL ECONOMIC ASSESSMENT

Price Base Year 2016	PV Base Year 2016	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 other than those associated with the new oversight and authorisation regime and compliance with safeguards and oversight processes in the Act. The cost of implementing this is 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	N/K	N/K	N/K
High	N/K	N/K	N/K
Best Estimate	N/K	N/K	N/K

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

N/A

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
Key risks relate to a lack of co-operation by communication service providers (CSPs). There is also a risk that technical solutions will be outpaced by technical change and/or changes in consumer behaviour.		

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:	In scope of OIOO?	Measure qualifies as
Costs: 0	No	N/A
Benefits: 0		
Net: 0		

Evidence Base

A. Strategic Overview

A.1 Background

Interception is the act of obtaining and making available some or all of the content of communications sent via a telecommunication 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, armed forces and the security and intelligence agencies in tackling threats such as serious crime and terrorism. The use of interception by the state is limited so that targeted interception can only be carried out by only nine agencies for a limited range of statutory purposes. It is subject to strong internal controls and independent oversight currently provided by the Interception of Communications Commissioner.

The use of interception is currently governed by the Regulation of Investigatory Powers Act 2000 (RIPA). Warranted interception can only be authorised for the purpose of preventing or detecting serious crime, in the interests of national security, or in the interests of the UK's economic well-being, so far as those interests are also relevant to national security.

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 or 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, the armed forces and the 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.

Under the current regime, the Secretary of State in considering a warrant application must assess the necessity and proportionality of the proposed interception and whether the information collected through interception could reasonably be obtained by other less intrusive means.

It is also possible to acquire the content of communications in bulk, under section 8 of RIPA. The Investigatory Powers Act 2016 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 communications 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 in the interests of national security, to prevent or detect serious crime or in the interests of the economic well-being of the UK so far as those interests are also relevant to national security, and to prevent serious crime. One of the purposes for a bulk warrant must be national security. The Investigatory Powers Act 2016 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 and Investigatory Powers Act 2014 (DRIPA) was enacted to respond to the challenges presented by the changing nature of the global telecommunications market. It clarified Parliament's intent as to the territorial extent of RIPA, but DRIPA's provisions are subject to a 31 December 2016 sunset clause. Three independent reviews of investigatory powers were conducted to inform replacement legislation: by the Independent Reviewer of Terrorism Legislation, David Anderson QC who published his report 'A Question of Trust' in June 2015, the Intelligence and Security Committee of Parliament, who published their report 'Privacy and Security' in March 2015 and the panel convened by the Royal United Services Institute, at the behest of the then Deputy Prime Minister, in July 2015.

All of the reviews concluded that the legislative framework for investigatory powers needed to be updated and modernised, to make clear the statutory basis for their use. A draft Bill was published on 4 November 2015 and was subject to pre-legislative scrutiny by a Joint Committee of both Houses of Parliament. The Intelligence and Security Committee and the Commons Science and Technology Committee also considered the Bill in parallel. Between them, those Committees received over 1,500 pages of written submissions and heard oral evidence from the Government, industry, civil liberties groups and many others. The recommendations made by those Committees informed changes to the Bill and the publication of further supporting material.

A Bill was introduced in the House of Commons on 1 March, and completed its passage on 16 November, meeting the timetable for legislation set by Parliament during the passage of the Data Retention and Investigatory Powers Act 2014. Over 1,700 amendments to the Bill were tabled and debated during this time. The Investigatory Powers Act 2016 was given Royal Assent on 29 November 2016.

A.2 Groups Affected

- The Security Service (MI5)
- The Secret Intelligence Service (SIS)
- Government Communications Headquarters (GCHQ)
- Home Office
- Foreign and Commonwealth Office
- Northern Ireland Office
- The National Crime Agency (NCA)
- The Metropolitan Police Service (MPS)
- The Police Service of Northern Ireland (PSNI)
- Police Scotland
- Her Majesty's Revenue and Customs
- The Ministry of Defence
- Communication service providers
- The public

A.3 Consultation

Within Government

All of the Government departments affected by the legislation were consulted in the policy development process, throughout pre-legislative scrutiny and during the passage of the Bill through Parliament.

Public Consultation

Operational stakeholders, companies affected by the legislative provisions and other key stakeholders were consulted by the Home Office as part of the policy-development making process and throughout pre-legislative scrutiny. The draft Bill was published on 4 November 2015 and subject to pre-legislative scrutiny by three Parliamentary Committees. A Bill was introduced in the House of Commons on 1 March, and completed its passage on 16 November, gaining Royal Assent on 29 November 2016.

B. Rationale

Three independent reviews of investigatory powers conducted by the Independent Reviewer of Terrorism Legislation, David Anderson QC, the Intelligence and Security Committee of Parliament and the Royal United Services Institute. They concluded that the power to intercept communications remained necessary, but that the regime could be made more transparent and additional safeguards could be applied. New legislation is necessary in order to respond to these recommendations, and to re-legislate for the continued use of interception by law enforcement, the armed forces and the security and intelligence agencies to intercept the communications of terrorists and perpetrators of serious crime where it is necessary and proportionate to do so.

David Anderson QC recommended that:

'Pending a satisfactory long-term solution to the problem, extraterritorial application should continue to be asserted in relation to warrants and authorisations (DRIPA 2014 s4) and consideration should be given to extraterritorial enforcement in appropriate cases' (A Question of Trust, Recommendation 25)

The draft Bill published on 4 November 2015 was scrutinised by three Parliamentary Committees. The Joint Committee scrutinising the draft Bill recommended that:

'We agree that the targeted interception power should be part of the Bill, subject to appropriate warrant authorisation arrangements'

And that:

'We are aware that the bulk powers are not a substitute for targeted intelligence, but believe that they are an additional resource. Furthermore, we believe that the security and intelligence agencies would not seek these powers if they did not believe they would be effective and that the fact they have been operating for some time would give them the confidence to assess their merits'.

C. Objectives

The objective of the new legislation is to provide greater public confidence in and understanding of the use of interception by law enforcement, armed forces and security and intelligence agencies and to apply enhanced safeguards, including the introduction of the 'double-lock' authorisation process for interception warrants. Greater public confidence will help maintain the ability of law enforcement, supported by the intelligence agencies, to investigate those who wish to do us harm. Interception is a vital tool for law enforcement, the armed forces and security and intelligence agencies and they are heavily reliant on it for intelligence gathering purposes. 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.

The Act will also provide statutory protections for the communications of Members of Parliament and members of other legislatures. In addition to approval of a warrant by a Judicial Commissioner, the Act states that the Secretary of State may not issue a warrant to intercept an MP's communications without the approval of the Prime Minister. This will cover all warrants for targeted interception. 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. These provisions will apply to communications of MPs, members of the House of Lords, UK MEPs, members of the Scottish Parliament and members of the Welsh and Northern Ireland Assemblies.

D. Options

Option 1 was to make no changes (do nothing).

Under this option, the intercepting agencies would retain the power to undertake interception under the existing legislative framework. However, the clarification provided in the Data Retention and Investigatory Powers Act 2014 would lapse on 31 December 2016, and we would not respond to the recommendations made by the independent reviews of investigatory powers.

Option 2 The Investigatory Powers Act re-legislates for the continued use of targeted and bulk interception, applying new safeguards and a new authorisation process.

This option seeks to secure public support for the capabilities in RIPA and DRIPA, enables law enforcement, the armed forces and security and intelligence agencies to continue to intercept the communications of terrorists and perpetrators of serious crime 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.

This option provides for the Secretary of State, by notice, to impose on communications service providers the obligation to maintain permanent technical capabilities. The purpose of maintaining a technical capability is to ensure that, when a warrant is served, companies can give effect to it securely and quickly. This provision replaces the existing position in RIPA where a company can be obligated to maintain a permanent interception capability, but with improved safeguards. A notice may only be given by the Secretary of State where the notice is necessary and where the conduct required is proportionate to what is sought to be achieved, and where the decision to give a notice has been approved by a Judicial Commissioner. In practice, these requirements will only be placed on companies that are required to give effect to warrants and authorisations on a recurrent basis.

This option will also provide additional protections for the communications of Members of Parliament and other legislators. In addition to approval by a Judicial Commissioner, the Act states that the Secretary of State may not issue a warrant to intercept an MP's communications without the approval of the Prime Minister.

E. Appraisal (Costs and Benefits)

GENERAL ASSUMPTIONS & DATA

- While efforts have been made to understand the costs and benefits to all affected groups, it is necessary to make some assumptions. The Home Office has consulted Government departments; communication service providers; and operational partners including law enforcement and the security and intelligence agencies.
- Without new legislation, there may be a decline in 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 was 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.
- The Government has a long-standing policy of contributing to the reasonable costs incurred by telecommunications operators giving effect to warrants. This policy will be maintained under the Act. As a result, the provisions in the Act will not impose any new costs on industry.

OPTION 2 – Re-legislate for the use of interception by the security and intelligence agencies, armed forces and law enforcement

COSTS

There will be no additional costs to companies as a result of the legislation. The Government recognises that the obligations imposed on CSPs can result in CSPs incurring additional costs and it does not expect those subject to such obligations to be put at commercial disadvantage. The current government policy, and that of its predecessors, is that it would not be appropriate to expect CSPs to meet the costs themselves and that CSPs will receive a fair contribution towards the costs of obligations in respect of warranted interception. 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 there are no additional costs whatsoever to industry as a result of this policy from the baseline.

The requirement to seek the approval of the Prime Minister before the Secretary of State can decide to issue a warrant to intercept an MP's communications builds on existing practice whereby the Prime Minister is consulted, so will not incur additional costs.

The only additional costs as a result of the policy are those in respect of additional reporting requirements as a result of new oversight measures that fall on the intercepting agencies. These are reflected within the oversight impact assessment and are not addressed here.

BENEFITS

There will be no monetised benefits as a result of this option. 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 intercept 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 be able, for example, to intercept the communications of a member of a serious organised crime group arranging the importation of arms or Class A drugs and to identify where the pick-up is going to take place so they can take action. It will enable security and intelligence agencies to continue to be able to intercept the communications of a terrorist planning an attack in the UK: to identify who they are talking to, what they are 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. 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 National Crime Agency 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 of intercepted material 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 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 from 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]

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]

F. Risks

OPTION 2 – Re-legislate for the use of interception by law enforcement, armed forces and security and intelligence agencies

There is a risk 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. There is also a risk that this option does not fully realise the objective of policy to improve public confidence in the legislative regime.

G. Enforcement

As is currently the case under Chapter 1 of Part 1 of RIPA, only those companies that will be served with warrants on a recurrent basis will be given a notice. This legislation does not intend to introduce any new requirements for communications companies, or place any unnecessary burden on them. The government will work with communications companies to ensure that any requests for assistance can be carried out with the least amount of impact on their business.

The infrastructure to support the provision of warranted interception 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 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 the new legislation. The continuation of this regime will also ensure that there is no additional impact on small 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 permanent interception capability, although they may still be obligated to give effect to a warrant.

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. The 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 Act includes clear provisions for CSPs to request a review of the requirements placed on them in a technical capability notice. However, under the new legislation a person may refer the whole or any part of a technical capability notice back to the Secretary of State for review under Clause 257 of the Act. Before deciding the review, the Secretary of State must consult and take account of the views of the TAB and a Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice on the person who has made the referral. The Commissioner will consider whether the notice is proportionate. After considering reports from the TAB and the Commissioner, the Secretary of State may vary, withdraw or confirm the effect of the notice. Where the Secretary of State varies or confirms the effect of the notice, the Investigatory Powers Commissioner must approve this decision. Until this decision is made, there is no requirement for the CSP to comply with the notice. The CSP will remain under obligation to provide assistance in giving effect to an interception warrant.

H. Summary and Recommendations

The table below outlines the costs and benefits of the proposed changes.

Table H.1 Costs and Benefits		
Option	Costs	Benefits
2	£0	£0
	Cost not quantified: None	Benefits not quantified: Greater safeguards and transparency, providing the public with greater confidence and assurance in the oversight and accountability of interception
Source: Refer to costs and benefits section		

Option 2 is recommended on the basis it is considered to offer the most cost effective approach to meeting the policy objectives. There are no additional costs as a result of the legislation.

I. Implementation

The Government will commence the provisions in the Act once full implementation plans have been considered and the associated public cost of establishing the Investigatory Powers Commissioner has been approved. A full consultation process with affected Government departments and stakeholders will form part of implementation.

J. Monitoring and Evaluation

The Investigatory Powers Commissioner will be obliged to report annually on the exercise of investigatory powers under this Act. The IPC will be advised on the impact of changing technology by the Technology Advisory Panel. The Act will be subject to post-legislative scrutiny five years after the Act has received Royal Assent (on 29 November 2016). 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. The Technical Advisory Board will also provide a source of advice to the Secretary of State.

K. Feedback

The Government has considered all of the recommendations of the three Parliamentary Committees and the public submissions made as part of the consultation process in responding with revised legislation. The Government continually considered and responded to feedback from interested stakeholders throughout the Bill's passage through Parliament and will continue to do so during the public consultation on Codes of Practice. Ongoing consultation with affected stakeholders will continue throughout implementation of the Act.

Impact Assessment Checklist

The impact assessment checklist provides a comprehensive list of specific impact tests and policy considerations (as of October 2015). Where an element of the checklist is relevant to the policy, the appropriate advice or guidance should be followed. Where an element of the checklist is not applied, consider whether the reasons for this decision should be recorded as part of the Impact Assessment and reference the relevant page number or annex in the checklist below.

The checklist should be used in addition to [HM Treasury's Green Book guidance](#) on appraisal and evaluation in central government.

Economic Impact Tests

Does your policy option/proposal consider...?	Yes/No (page)
<p>Business Impact Target The Small Business, Enterprise and Employment Act 2015 (s. 21-23) creates a requirement to assess the economic impacts of qualifying regulatory provisions on the activities of business and civil society organisations. [Better Regulation Framework Manual] or [Check with the Home Office Better Regulation Unit]</p>	N/A
<p>Review clauses The Small Business, Enterprise and Employment Act 2015 (s. 28) creates a duty to include a review clause in secondary legislation containing regulations that impact business or civil society organisations. [Check with the Home Office Better Regulation Unit]</p>	N/A
<p>Small and Micro-business Assessment (SaMBA) The SaMBA is a Better Regulation requirement intended to ensure that all new regulatory proposals are designed and implemented so as to mitigate disproportionate burdens. The SaMBA must be applied to all domestic measures that regulate business and civil society organisations, unless they qualify for the fast track. [Better Regulation Framework Manual] or [Check with the Home Office Better Regulation Unit]</p>	N/A
<p>Clarity of legislation Introducing new legislation provides an opportunity to improve the clarity of existing legislation. Legislation with multiple amendments should be consolidated, and redundant legislation removed, where it is proportionate to do so.</p>	N/A
<p>Primary Authority Any new Government legislation which is to be enforced by local authorities will need to demonstrate consideration for the inclusion of Primary Authority, and give a rationale for any exclusion, in order to obtain Cabinet Committee clearance. [Primary Authority: A Guide for Officials]</p>	N/A
<p>New Burdens Doctrine The new burdens doctrine is part of a suite of measures to ensure Council Tax payers do not face excessive increases. It requires all Whitehall departments to justify why new duties, powers, targets and other bureaucratic burdens should be placed on local authorities, as well as how much these policies and initiatives will cost and where the money will come from to pay for them. [New burdens doctrine: guidance for government departments]</p>	N/A
<p>Competition The Competition guidance provides an overview of when and how policymakers can consider the competition implications of their proposals, including understanding whether a detailed competition assessment is necessary. [Government In Markets Guidance]</p>	N/A

Social Impact Tests

<p>New Criminal Offence Proposals Proposed new criminal offences will need to be agreed with the Ministry of Justice (MOJ) at an early stage. The Justice Impact Test (see below) should be completed for all such proposals and agreement reached with MOJ before writing to Home Affairs Committee (HAC) for clearance. Please allow 3-4 weeks for your proposals to be considered.</p>	N/A
<p>Justice Impact Test The justice impact test is a mandatory specific impact test, as part of the impact assessment process that considers the impact of government policy and legislative proposals on the justice system. [Justice Impact Test Guidance]</p>	N/A
<p>Statutory Equalities Duties The public sector equality duty requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity, and foster good relations in the course of developing policies and delivering services. [Equality Duty Toolkit]</p>	N/A
<p>Privacy Impacts A Privacy Impact Assessment supports an assessment of the privacy risks to individuals in the collection, use and disclosure of information. [Privacy Impact Assessment Guidance] or [Contact the Corporate Security Information Assurance Team Helpline on 020 7035 4969]</p>	Yes
<p>Family Test The objective of the test is to introduce a family perspective to the policy making process. It will ensure that policy makers recognise and make explicit the potential impacts on family relationships in the process of developing and agreeing new policy. [Family Test Guidance]</p>	N/A
<p>Powers of Entry A Home Office-led gateway has been set up to consider proposals for new powers of entry, to prevent the creation of needless powers, reduce unnecessary intrusion into people's homes and to minimise disruption to businesses. [Powers of Entry Guidance]</p>	N/A
<p>Health Impact Assessment of Government Policy The Health Impact Assessment is a means of developing better, evidenced-based policy by careful consideration of the impact on the health of the population. [Health Impact Assessment Guidance]</p>	N/A

Environmental Impact Tests

<p>Environmental Impacts The purpose of the environmental impact guidance is to provide guidance and supporting material to enable departments to understand and quantify, where possible in monetary terms, the wider environmental consequences of their proposals. [Environmental Impact Assessment Guidance]</p>	N/A
<p>Sustainable Development Impacts Guidance for policy officials to enable government departments to identify key sustainable development impacts of their policy options. <i>This test includes the Environmental Impact test cited above.</i> [Sustainable Development Impact Test]</p>	N/A
<p>Rural Proofing Guidance for policy officials to ensure that the needs of rural people, communities and businesses are properly considered. [Rural Proofing Guidance]</p>	N/A