

Title: IP Bill: Investigatory Powers Bill: Equipment Interference IA No: HO0198	Impact Assessment (IA) Date: 7 July 2016 Stage: Final Source of intervention: Domestic Type of measure: Primary legislation Contact for enquiries: investigatorypowers@homeoffice.gsi.gov.uk
Lead department or agency: Home Office Other departments or agencies: FCO, Cabinet Office, MOD, NIO, GCHQ, MI5, SIS, NCA, MPS, PSNI, Police Scotland and wider law enforcement agencies	

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 (EANDCB on 2014 prices)	In scope for One-in, Two-out (OI2O)?	Business Impact Target status
£0m	£0m	£0m	N/A	Not a Regulatory Provision

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

The internet and related forms of technology are now used extensively by terrorists and criminals to organise and carry out their activities. In order to keep pace, it has been necessary for law enforcement agencies, the armed forces and the security and intelligence agencies to develop techniques to enable them to gain access to computers, devices and equipment to gather evidence or intelligence. These techniques are known collectively as equipment interference. New legislation needs to be clear about how equipment interference is being used and the robust safeguards that apply.

What are the policy objectives and the intended effects?

To provide for the use of equipment interference for the acquisition of electronic communications and other data by law enforcement agencies, the armed forces and the security and intelligence agencies. The Bill will provide robust oversight and safeguards on use of equipment interference and consolidate the existing legislative basis for the use of this capability. The Bill will also improve public understanding of the need for and the use of these increasingly important and sensitive techniques. The Bill will explicitly provide for targeted equipment interference directed at a particular person, group or premises; and bulk equipment interference, which collects data from outside of the UK - a small amount of which will be analysed.

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

Option 1: No new legislation. Option 2: Re-legislate for the use of targeted and bulk equipment interference for the acquisition of electronic communications by security and intelligence agencies only, replacing existing legislative framework for obligations on telecommunication operators. This option would require law enforcement agencies to rely on existing legislation, they would therefore not benefit from the new processes instated by the Bill. Option 3: Re-legislate in the Investigatory Powers Bill for the use of targeted equipment interference for the acquisition of electronic communications and other data by law enforcement agencies, the armed forces, and the security and intelligence agencies, also replacing the existing legislative framework for obligations on telecommunication operators. Bulk equipment interference capability will be reserved for use by the security and intelligence agencies. Option 3 is the preferred option.

Will the policy be reviewed? It will be reviewed. If applicable, set review date: December 2022

Does implementation go beyond minimum EU requirements?	N/A			
What sizes of organisation are affected?	Micro N/A	Small N/A	Medium N/A	Large N/A
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 am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impacts of the leading options.

Signed by the responsible Minister:

Date: 7/7/16

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		10		
High				
Best Estimate	0		0	0

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

This option is the baseline and there are no additional costs or benefits associated with this option.

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

This option is the baseline and there are no additional costs or benefits associated with this option.

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low		10		
High				
Best Estimate	0		0	0

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

This option is the baseline and there are no additional costs or benefits associated with this option.

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

This option is the baseline and there are no additional costs or benefits associated with this option.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5%
That the current legislation would stand and powers would continue to be exercised under existing statutory frameworks. There is a risk that public confidence in the application of these powers may be degraded.		

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			
Costs: 0	Benefits: 0	Net: 0	Score for Business Impact Target £m (qualifying regulatory provisions only)

Summary: Analysis & Evidence

Policy Option 2

Description: Re-legislate for equipment interference conducted by the security and intelligence agencies only

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	10	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 costs by 'main affected groups'

The only identified costs associated with the change in policy will be those associated with greater transparency and reporting of compliance with the legislation. The costs of increased compliance are contained within the oversight impact assessment and are not reflected here.

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

N/A

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	N/K	10	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'

Increased public confidence and understanding of the legislation and how it provides a clear and transparent statutory framework for the activities of the security and intelligence agencies. Continued ability to investigate terrorist activity and serious crime including cyber-crime and online child sexual exploitation. Improved understanding of how telecommunication operators may be required to work with organisations carrying out equipment interference and increased confidence due to the safeguards that are applied.

Key assumptions/sensitivities/risks

Discount rate (%) 3.5%

By consolidating existing legislation criminals and terrorists may be more aware of the capabilities of the security and intelligence agencies to prevent and detect terrorism and serious crime, and may take new or additional measures to evade discovery.

BUSINESS ASSESSMENT (Option 2)

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

Summary: Analysis & Evidence

Policy Option 3

Description: Re-legislate for the use of equipment interference by both security and intelligence agencies and law enforcement

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	10	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 costs by 'main affected groups'
The only identified costs associated with the change in policy will be those associated with greater transparency and reporting of compliance with the legislation. These costs are likely to be small and are contained within the oversight impact assessment.

Other key non-monetised costs by 'main affected groups'
N/A

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	N/K	10	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'
Increased public confidence and understanding of the legislation and how it provides a clear and transparent statutory framework underpinning the activities of the security and intelligence agencies and law enforcement. Continued ability to investigate terrorist activity, and serious crime including cyber-crime and online child sexual exploitation. Improved understanding of how telecommunication operators may be required to work with organisations carrying out equipment interference and increased confidence due to the safeguards that are applied.

Key assumptions/sensitivities/risks
By consolidating existing legislation criminals and terrorists may be more greatly aware of the capabilities of law enforcement agencies, armed forces, and security and intelligence agencies to detect and prevent terrorism and serious crime, and may take new or additional measures to evade discovery.

Discount rate (%) 3.5%

BUSINESS ASSESSMENT (Option 3)

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

Evidence Base

A. Strategic Overview

A.1 Background

Equipment interference is the term used to describe a range of techniques used by the security and intelligence agencies, armed forces, and law enforcement agencies – primarily the police, HM Revenue and Customs and the National Crime Agency – to gain covert access to computers and other devices to gather intelligence or evidence, in connection with investigations or operations.

Developments in technology have transformed the way that we all communicate and carry out our daily business. These developments have also provided new opportunities for criminals to exploit in planning, organising and carrying out their illegal activities. For some criminals, technology provides a means to communicate more effectively with contacts, in a way that is harder to detect or trace. Others have found ways to use technology to evade other investigatory techniques such as interception of communications. It is vital that investigatory capabilities continue to be available to law enforcement agencies, the armed forces and the security and intelligence agencies in order to protect the public from the atrocities of terrorist attacks, protect our armed forces from those who would do them harm, and to guard against the devastation serious and organised crime can have upon communities and individuals. In order to keep pace with the changing methodologies of criminals, law enforcement agencies, the armed forces and the security and intelligence agencies have had to develop techniques to enable them to gather intelligence and evidence and respond to the changing environment in which terrorists and criminals now operate. These techniques are collectively referred to as equipment interference.

Equipment interference techniques vary in complexity. At the lower end of the scale, an investigating agency may use someone's login credentials to covertly gain access to communication and other information on a device. More complex operations may involve exploiting vulnerabilities in software to gain control of devices or networks to enable the remote extraction of communications or other information, or to monitor the user of the device. These types of activities can be carried out illegally by hackers or criminals. These types of operations may also be carried out lawfully by law enforcement agencies, the armed forces and the security and intelligence agencies in limited and carefully controlled circumstances.

Using these techniques it is possible for law enforcement agencies and the security and intelligence agencies to locate subjects of interest, find out who they are working with, understand how they are financing their illegal operations and gather evidence where computers or other devices are used to plan or carry out their illegal exploits. This enables law enforcement agencies and the security and intelligence agencies to try to keep pace with advances in the technology by criminals to communicate with each other, such as use of the "dark web", a highly encrypted area of the internet. Equipment interference is one of the tools and techniques that law enforcement, the armed forces and the security and intelligence agencies deploy to look to ensure that there is no safe space for criminals and terrorists online to plot atrocities and cause us harm.

The scale of equipment interference operations also varies. Some operations target a single device belonging to a single person whilst larger 'thematic' operations may target a number of devices that share particular characteristics. 'Bulk' equipment interference would involve equipment interference that will collect data from a range of devices in order to discover target devices amongst a larger group of devices. As with other bulk powers provided under the Bill, once the data has been collected only a small amount of that data is then analysed. The ability to conduct bulk equipment interference in this way will become increasingly important as technology continues to change the way in which people communicate. Only the security and intelligence agencies may exercise this bulk power.

The current legislative framework provides a statutory basis for equipment interference, both targeted and bulk. However, we intend to provide a clearer and transparent statutory basis for both targeted and bulk equipment interference. The legislation also includes greater and robust oversight of equipment interference and heightened safeguards including handling, destruction and retention arrangements (as set out in the draft Equipment Interference Code of Practice and the current Code which has been in effect since January 2016) to ensure that the power is used proportionately, fairly and with the appropriate protection that minimises potential incursions of privacy. The increased safeguards are addressed primarily in the oversight impact assessment.

The current use of equipment interference by law enforcement agencies is authorised under the property interference provisions in the Police Act 1997. Use of equipment interference by the security and intelligence agencies is authorised by warrants issued under the Intelligence Services Act 1994. The Code of Practice for equipment interference, which sets out the robust procedures and safeguards governing equipment interference techniques that the security and intelligence agencies already apply, came into force in January 2016.

There have been three independent reviews of investigatory powers, which include equipment interference for the purposes of acquiring electronic communications. The first is the review conducted by David Anderson QC, the Independent Reviewer of Terrorism Legislation who was commissioned during the passage of the Data Retention and Investigatory Powers Act, to carry out a review of Investigatory Powers. Two others were conducted in parallel: the Intelligence and Security Committee of Parliament looked into the activities of the security and intelligence agencies, and published a report in March 2015; and the Royal United Services Institute established a panel to review the impact on civil liberties of Government surveillance, which concluded in July 2015. Anderson's report was published in June 2015. All of the reviews concluded that the legislative framework for equipment interference needed to be updated and modernised to make clear the statutory basis for its use. The draft Investigatory Powers Bill was published in November 2015, and was subject to pre-legislative scrutiny by three Parliamentary Committees.

The Investigatory Powers Tribunal held (in February 2016) that the exercise of equipment interference by the security and intelligence services under the existing legal framework is lawful when authorised as necessary and proportionate, and that the law strikes a proper balance between the use of equipment interference and the protection of privacy.

While the exercise of equipment interference by law enforcement agencies, armed forces and the security and intelligence agencies is conducted in full compliance with the current statutory framework, it could be made more transparent and further safeguards applied to its use. EI is a fundamental intelligence gathering and investigative capability for law enforcement agencies armed forces and the security and intelligence agencies, and it is important to ensure that new legislation is clear and transparent. Moreover the Government wishes to ensure that there is consistency in the robust safeguards that will apply to law enforcement agencies, armed forces and the security and intelligence agencies when exercising powers to acquire communications.

A.2 Groups Affected

- Government Departments (Home Office, Foreign and Commonwealth Office, Ministry of Defence, Northern Ireland Office, Cabinet Office)
- Security and intelligence agencies (MI5, SIS, GCHQ)
- Armed forces
- Law enforcement agencies
- Intelligence Services Commissioner and the Office of the Surveillance Commissioners
- Telecommunications operators
- The general public, whose safety and security are affected by the capabilities of the police and other agencies to prevent and detect crime, and whose privacy needs to be protected

A.3 Consultation

Within Government

All Government departments who are affected by the legislation were consulted as part of the policy development and pre-legislative scrutiny process.

Public Consultation

Government has conducted consultation with public authorities, CSPs and other industry groups. The Government has also consulted civil liberties groups to hear their views on the scope of the legislation and the safeguards they consider should apply.

B. Rationale

In order that Government can protect its citizens, it must ensure that law enforcement, the armed forces and the security and intelligence agencies have the necessary powers to protect national security and safeguard public security by preventing terrorism and tackling serious and organised crime. Equally, the Government must ensure that the use of these powers are scrupulously overseen, and subject to robust safeguards. It has a responsibility to ensure that law enforcement, the armed forces and the security and intelligence agencies can be held to account for their activities and that those activities are transparent, whilst protecting sensitive techniques. It is also important that there is public understanding as to what types of activity may be undertaken, in what circumstances, and that the public has confidence that the appropriate safeguards are in place.

Equipment interference is an investigative technique that is important for the detection and prevention of serious crime, including organised crime and terrorism, and for the protection of national security. It is vital that these techniques continue to be available to law enforcement, the armed forces and the security and intelligence agencies in order to protect the public from the atrocities of terrorist attacks and the devastation that serious and organised crime, such as drug trafficking or child sexual exploitation, can have on individuals and communities. At the same time, the Government recognises that these can include highly sensitive and potentially intrusive investigatory techniques, and that they must be subject to appropriate controls, safeguards and oversight. Separating equipment interference from other forms of property interference and creating a free-standing equipment interference provision for law enforcement agencies armed forces and the security and intelligence agencies, will enable a regime to be created that sets out clearly the circumstances in which equipment interference can be deployed and the checks and controls on its use.

This will also answer the recommendations of David Anderson, in respect of:

"1. ...a comprehensive new law, drafted from scratch which (b) prohibits interference with [communications] by public authorities, save on terms specified] 6. The following should be brought into the new law and/or made subject to equivalent conditions to those mentioned here: (b) equipment interference (or CNE) pursuant to ISA 1994 ss5 and 7, so far as it is conducted for the purposes of obtaining electronic communications (c.f. ISC Report Recommendations MM-PP)"

"7. The new law should repeal or prohibit the use of any other powers providing for interference with communications. For the avoidance of doubt, no recommendations are made in relation to the use of court orders to access stored communications (e.g. PACE s9) or the searching of devices lawfully seized, save that it is recommended that oversight be extended to the former."

"92 (d). There should be statutory provision for oversight of the operation of powers for interception and/or obtaining communications data other than in the new law to the extent

that such powers survive, including the power to access stored data by order of the court under PACE s9."

It will also go toward answering the recommendation of the Intelligence and Security Committee of Parliament, that:

"The Agencies may undertake IT Operations against computers or networks in order to obtain intelligence. These are currently categorised as 'Interference with Property' and authorised under the same procedure. Given the growth in, and intrusiveness of, such work we believe consideration should be given to creating a specific authorisation regime". (Recommendation CC)

The draft Investigatory Powers Bill was published on 4 November 2015 and was subject to pre-legislative scrutiny by three Parliamentary Committees: the Joint Committee convened to scrutinise the draft Bill; the Intelligence and Security Committee of Parliament; and the House of Commons Science and Technology Committee, which undertook an inquiry into the technological issues of the Bill. Their conclusions were published on 1, 9 and 11 February. A revised Bill, that took account of the recommendations made during pre-legislative scrutiny, was introduced into the House of Commons on 1 March 2016, and received its Third Reading on 7 June 2016. The Bill has been updated further with amendments at Commons Committee and Report stage.

C. Objectives

To introduce legislation which will authorise the acquisition of electronic communications, information and other data by use of targeted and bulk equipment interference, and update and modernise the legal framework. The intended effect will be to ensure the activities that law enforcement agencies, the armed forces and the security and intelligence agencies undertake in respect of equipment interference can be applied to protect national security and prevent and detect serious crime, including child sexual exploitation, cyber-crime and other harms. The policy does not provide for new powers in respect of equipment interference, rather it makes clear where and how these important but sensitive techniques may be exercised, with a new regime for the authorisation and oversight applied to equipment interference.

D. Options

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

Under this option, no changes would be made to the legislation governing equipment interference. The exercise of these powers would continue to be in accordance with the current legal framework: sections 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997. The power to levy obligations on domestic CSPs would remain under Section 94 of the Telecommunications Act 1984. The Equipment Interference Code of Practice would remain in place to govern the activities of the security and intelligence agencies use of equipment interference and it would be possible to update the existing Covert Surveillance and Property Interference Code of Practice to provide further detail on the use of equipment interference by law enforcement agencies.

This option would not modernise the legal framework, or provide for the enhanced safeguards of bulk equipment interference and not respond to David Anderson's recommendation in respect of consolidating legislation. It would not respond to the pre-legislative scrutiny by Parliament.

Option 2 Re-legislate for the use of equipment interference by the security and intelligence agencies

Provision within the Investigatory Powers Bill would be made to provide for the use of targeted and bulk equipment interference by the security and intelligence agencies and armed forces. This would respond to the letter of Anderson's recommendation (No. 6) but not his principle that the

legislation should, so far as is possible, prohibit interference with electronic communications outside of the legislation. Law enforcement agencies would continue to exercise powers under section 93 of the Police Act 1997 to provide for equipment interference. The ability to levy obligations on domestic CSPs would remain under Section 94 of the Telecommunications Act 1984 for the security and intelligence agencies.

This option would provide for increased transparency of the use of targeted equipment interference by the security and intelligence agencies and armed forces, and the robust safeguards that would apply. It would also extend a heightened set of safeguards to oversee the use of bulk equipment interference by the security and intelligence agencies. However, it would not provide for increased safeguards and robust oversight of law enforcement agencies use of targeted equipment interference techniques as these would continue to be provided under existing legislation – including the present model for authorisation of these techniques. As a result the legislative framework for equipment interference would remain inconsistent and lack coherency.

Equipment interference today will rely in some instances on the co-operation of telecommunications operators. This option would replace the existing statutory framework that would allow the security and intelligence agencies to levy obligations on domestic telecommunications operators and would provide for the issuing of technical capability notices that would require telecommunications operators to provide reasonable assistance and support the implementation of equipment interference warrants when required. Any costs to industry would be reimbursed by Government. As with technical capability notices issued in relation to interception and communications data, the Secretary of State would be obliged to consult with the Technical Advisory Board and the Investigatory Powers Commissioner should such a notice be appealed by a telecommunications operator. This would provide a clearer and more transparent framework for the security and intelligence agencies to require assistance with implementing a warrant for equipment interference. As this is not a new policy, the costs have not been included as part of the impact assessment.

Option 3 Re-legislate for both law enforcement and security and intelligence agencies' use of equipment interference.

The new legislation would consolidate the statutory framework for targeted equipment interference for the purposes of acquiring electronic communications that provides for the activities and jurisdiction of law enforcement agencies, armed forces and the security and intelligence agencies. It would restrict the powers exercised under the Police Act and under the Intelligence Services Act for equipment interference for acquisition of electronic communications and place them on a clear and transparent statutory footing. It would make apparent the robust safeguards and rigorous oversight that applies and improve public confidence and understanding of how and when these powers are exercised, in strict accordance with necessity and proportionality. It would extend a heightened set of safeguards to the provision of bulk equipment interference, reserved for use by the security and intelligence agencies regarding matters of national security. The existing Equipment Interference Code of Practice brought into force in January 2016 would be replaced by a Code that extended to law enforcement as well as the intelligence agencies.

As amended, 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 approve a warrant before the Secretary of State or law enforcement chief can decide to issue a warrant to acquire an MP's communications or private information through equipment interference. The inclusion of warrants issued by law enforcement chiefs, and the required approval (rather than consultation) of the Prime Minister, represent expansion of this provision following Committee stage in the House of Commons. 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.

Equipment interference today will rely in some instances on the co-operation of telecommunications operators. This option would replace the existing statutory framework that

would allow the security and intelligence agencies to levy obligations on domestic telecommunications operators and would provide for the issuing of technical capability notices that would require telecommunications operators to provide reasonable assistance and support the implementation of equipment interference warrants when required. Any costs to industry would be reimbursed by Government. As with technical capability notices issued in relation to interception and communications data, the Secretary of State would be obliged to consult with the Technical Advisory Board and the Investigatory Powers Commissioner should such a notice be appealed by a telecommunications operator. This would provide a clearer and more transparent framework for the security and intelligence agencies to require assistance with implementing a warrant for equipment interference. As this is not a new policy, the costs have not been included as part of the impact assessment.

This option would go furthest to answer the recommendations made by David Anderson, the ISC and RUSI, and is the preferred option.

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 (as far as is possible) strengthened and confirmed the evidence base through information gathered through consultation with other Government Departments and operational partners including law enforcement agencies and the security and intelligence agencies.
- Were we not to legislate, the provisions in existing legislation for both targeted and bulk equipment interference (with the existing economic costs of the policy as applicable) would remain. The ongoing baseline costs of the technical systems and resource used to carry out equipment interference would remain, with no cost incurred above those already established.
- The Government has a long-standing policy of contributing to the reasonable costs incurred by telecommunications operators giving effect to warrants or complying with other obligations. This policy will be maintained under the Bill. As a result, the provisions in the Bill will not impose any new costs on industry.

OPTION 2 – Re-legislate for the use of equipment interference by the security and intelligence agencies only

COSTS

There is provision in existing legislation for targeted and bulk equipment interference. The ongoing baseline costs of the technical systems and resource used to carry out equipment interference would remain, with no cost incurred above those already established.

This option would replace the existing legislative provision for domestic companies to be required to give effect to an equipment interference warrant, with a new framework with a route of appeal for companies given a technical capability notice.

Non-monetary costs would include the inconsistency of the legislative framework for law enforcement and the security and intelligence agencies.

BENEFITS

There would be no monetary benefits to affected groups as a result of legislation. Non-monetary benefits would include: greater public confidence in the transparency and clarity of the legislation that applies to interference with equipment to acquire electronic communications and other data as a result of the strengthened safeguards and additional oversight, through the introduction of a double-lock authorisation process, whereby a Judicial Commissioner approves warrants issued for equipment interference.

OPTION 3 – Re-legislate for use of equipment interference by both law enforcement and the security and intelligence agencies

COSTS

There is provision in existing legislation for bulk and targeted equipment interference. The ongoing baseline costs of the technical systems and resource used to carry out equipment interference would remain, with no cost incurred above those already established.

This option would replace the existing legislative provision for domestic companies to be required to give effect to an equipment interference warrant, with a new framework with a route of appeal for companies given a technical capability notice.

BENEFITS

Non-monetary benefits would include: greater public confidence in the exercise of equipment interference by law enforcement agencies, the armed forces and the security and intelligence agencies, to acquire electronic communications and other data as a result of the clearer, robust safeguards and oversight applied to the use of equipment interference. Greater transparency for companies in giving effect to an equipment interference warrant.

Re-legislating for equipment interference as part of the Investigatory Powers Bill will provide for continued use of investigatory techniques that help to achieve the following benefits below:

Counter terrorism and protection of national security

The use of equipment interference can provide for the acquisition of communications and other private data via operations against a target's computer or network. In limited and controlled circumstances this might mean the security and intelligence agencies obtain authorisation to use a terrorist's e-mail credentials to log into their e-mail account and access e-mails with details of contacts and, potentially, attack planning. This can give access to material that would be encrypted if intercepted, or material which cannot be obtained because there is no CSP on whom a warrant can be served.

Safeguarding children

Many cases of child sexual exploitation rely heavily on use of computer technology to organise and carry out the crime, in an attempt to evade detection and identification by law enforcement agencies. Police make use of equipment interference to gather intelligence and evidence on paedophiles operating on the internet, tracking the sharing of indecent images of children, and others exploiting children for these purposes. Similarly, the security and intelligence agencies may, in limited and controlled circumstances, be authorised to exploit a vulnerability in software which would give them access to a machine belonging to a serious criminal in order to obtain intelligence to disrupt a paedophile ring.

Other crime

Intelligence and evidence obtained through the use of equipment interference is used to investigate and prosecute serious criminals (such as drug traffickers and illegal arms traders) and to protect UK cyber security. For example, the security and intelligence agencies may be authorised, in limited and controlled circumstances, to counter the activities of cyber criminals to prevent large scale disruption or compromise of computers in the UK.

The following case studies are presented to demonstrate the value of equipment interference in previous operations:

CASE STUDY A

Equipment interference, when used with other intelligence gathering techniques, is vital in time-limited cases of threat-to-life when the police need to act quickly.

In one example, intelligence was received that several suspects were at large after being involved in an attempted murder. Equipment interference and other intelligence gathering techniques were used to identify and locate the suspects leading to their arrest before further offences could be committed. Due to the high quality of intelligence achieved through equipment interference, the suspects were arrested within hours of receiving the initial intelligence. Without the use of equipment interference it would not have been possible to arrest the suspects simultaneously which was critical to preserving the evidence.

CASE STUDY B

The ability to use equipment interference alongside other intelligence gathering techniques provides operational flexibility enabling the police to progress long term criminal investigations even when crime groups use specific tactics to try and disguise their activities.

A law enforcement operation into an organised crime group importing Class A drugs into the UK used equipment interference alongside other intelligence gathering to identify the criminal network. The intelligence was used to make numerous arrests and seize a significant amount of Class A drugs before it reached the streets. Through the combined intelligence approach law enforcement were able to dismantle the drugs network.

F. Risks

OPTION 2 – Re-legislate for the use of equipment interference by the security and intelligence agencies only

There is a risk that by legislating only for the security and intelligence agencies, either the regime becomes inconsistent (Police forces would still have access to equipment interference under the Police Act 1997, which is not subject to the 'double-lock' authorisation process) or that we would be required to prohibit the use of equipment interference by Police forces, hindering their ability to carry out their functions.

OPTION 3 – Re-legislate for the use of equipment interference by both law enforcement and the security and intelligence agencies

There is an ongoing 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 law enforcement agencies, armed forces, and the security and intelligence agencies to detect and prevent terrorism and serious crime, and will take new or additional measures to evade discovery.

G. Enforcement

The government will work with telecommunications operators to ensure that any requests for assistance can be carried out with the least amount of impact on their business.

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 Bill includes clear provisions for CSPs to request a review of the requirements placed on them in a technical capability notice should they consider these to be unreasonable. Under 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 section 191 of the Act. Before deciding the review, the Secretary of State must consult and take account of the views of the TAB and the Investigatory Powers 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 Investigatory Powers Commissioner, the Secretary of State may vary, withdraw or confirm the effect of the notice. Until this decision is made, there is no requirement for the CSP to comply with the notice.

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	Costs associated with greater transparency and reporting of compliance with the legislation (contained within oversight IA)	N/A
	Non-monetised: N/A	Non-monetised: Increased public confidence and understanding of the legislation. Continued ability to investigate criminal activity. Improved understanding of CSPs work with organisations carrying out equipment interference.
3	Costs associated with greater transparency and reporting of compliance with the legislation (contained within oversight IA)	N/A
	Non-monetised: N/A	Non-monetised: Increased public confidence and understanding of the legislation. Continued ability to investigate criminal activity. Improved understanding of CSPs work with organisations carrying out equipment interference.
Source: Refer to costs and benefits section		

Option 3 is recommended on the basis it is considered to offer the most cost effective approach to meeting the policy objectives.

I. Implementation

The Government will commence the provisions in the Investigatory Powers Act once full implementation plans have been considered and the associated public cost has been approved by Parliament. A full consultation process with affected Government departments, agencies, CSPs and stakeholders will form part of implementation. A Code of Practice, which will be approved by Parliament, will set out the practical effects of the legislation.

J. Monitoring and Evaluation

The Investigatory Powers Commissioner will be obliged to report annually on the exercise of investigatory powers under this act. The Act will be subject to post-legislative scrutiny five years after the Act has received Royal Assent. 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. The Technical Advisory Board will provide a source of technical advice to the Secretary of State and the Investigatory Powers Commissioner on an ongoing basis. A Code of Practice, which will be approved by Parliament, will set out the practical effects of the legislation.

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.

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)
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]	N/A
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]	N/A
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]	N/A
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.	Yes.
Primary Authority	N/A

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]	
--	--

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]	N/A
---	-----

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]	N/A
---	-----

Social Impact Tests

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.	Yes.
--	------

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]	Yes.
--	------

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]	N/A
---	-----

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]	Yes
--	-----

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]	N/A
--	-----

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]	N/A
--	-----

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]	N/A
---	-----

Environmental Impact Tests

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]	N/A
--	-----

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]	N/A
--	-----

Rural Proofing Guidance for policy officials to ensure that the needs of rural people, communities and businesses are properly considered. [Rural Proofing Guidance]	N/A
--	-----

