

**Title:** Investigatory Powers Bill: Overarching Impact Assessment

**IA No:** HO0206

**Lead department or agency:** Home Office

**Other departments or agencies:**

FCO, Cabinet Office, MOJ, CPS, MOD, HMRC, MI5, SIS, GCHQ, NCA, wider law enforcement

## Impact Assessment (IA)

**Date:** 4 November 2015

**Stage:** Consultation

**Source of intervention:** Domestic

**Type of measure:** Primary legislation

**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?	
£247.0m	£0m	£0m	No	NA

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

The legislation that governs the use of investigatory powers by the security and intelligence agencies and law enforcement is spread out over a number of statutes and has not kept pace with technology. New legislation is required to update and modernise the use of investigatory powers, apply greater safeguards and oversight and to prevent the degradation of the capabilities of law enforcement and the security and intelligence agencies necessary to protect the public and to keep us safe. The Data Retention and Investigatory Powers Act 2014 is sunsetted to 31 December 2016 and legislation is necessary to ensure a legislative basis for these powers and oversight arrangements

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

To provide a clear and transparent framework for the exercise of investigatory powers by the security and intelligence agencies and law enforcement, with greater oversight and safeguards. To consolidate existing legislation into a concise and comprehensive Act that will improve public understanding of the need for, and the use of, these important and sensitive capabilities. To modernise and update the legal framework to ensure the security and intelligence agencies and law enforcement can continue to exercise the capabilities they need to maintain public safety and protect us from terrorism, and serious crime including cyber-crime, human trafficking and child sexual exploitation.

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

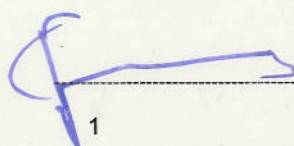
Option one, do nothing: The capability gap for law enforcement remains. Investigatory powers remain spread out over a number of statutes. Option two, re-legislate for investigatory powers: Clarify the existing legal framework for investigatory powers, including interception, communications data and equipment interference, the safeguards for SIA use of bulk personal datasets, as well as requiring the retention of communications data, including internet connection records. Increasing oversight and consolidating existing oversight structures, as well as providing for judicial approval of warrants. Option two is the preferred option as it meets the required policy objectives.

### 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 No	< 20 Yes	Small Yes	Medium Yes	Large Yes
What is the CO <sub>2</sub> equivalent change in greenhouse gas emissions? (Million tonnes CO <sub>2</sub> 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:

3/11/16



# Summary: Analysis & Evidence

Policy Option 1

Description: Do nothing

## 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	0		0	0
High	0		0	0
Best Estimate	0		0	0

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

The 'do nothing' option is the baseline, and the agencies and law enforcement would continue to exercise the existing powers proposed in the draft Bill under the current statutory basis. Therefore costs and benefits are zero.

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

The 'do nothing' option is the baseline and therefore costs and benefits are zero.

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'

The 'do nothing' option is the baseline and therefore costs and benefits are zero.

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

The 'do nothing' option is the baseline and therefore costs and benefits are zero.

Key assumptions/sensitivities/risks

Discount rate (%)

3.5

That the data retention regime would not be allowed to lapse. No changes would be made to the oversight and authorisation regimes and legislation would remain spread over a number of Acts. The agencies and law enforcement would continue to exercise powers (equipment interference, bulk powers in respect of the agencies) under existing statutory bases. A gap would still remain in capabilities to gain access to electronic communications to progress investigations.

### BUSINESS ASSESSMENT (Option 1)

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



# Summary: Analysis & Evidence

## Policy Option 2

**Description:** Legislate comprehensively for investigatory powers

### FULL ECONOMIC ASSESSMENT

Price Base Year 2015	PV Base Year 2015	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: N/K	High: N/K	Best Estimate: -246.7

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	N/K	N/K	N/K
High	N/K	N/K	N/K
Best Estimate	170.4	13.9	247.0

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

A small cost associated with increased compliance, reporting and safeguards to the agencies, law enforcement and other public authorities.

A minimal cost to the justice system for offences and changes to the Investigatory Powers Tribunal.

A large cost to Government Departments associated with the establishment of the Investigatory Powers Commission and authorisation of warranting.

A large cost associated with the ongoing running costs, compliance and reimbursement to business of costs associated with new communications data provisions.

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

Greater transparency of the investigatory powers available to the state to tackle crime and conduct investigations may result in greater use of obfuscation techniques by criminals, making it more difficult for the agencies and law enforcement to protect the public.

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'

Benefits have not been quantified.

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

Reduced costs to the Agencies and law enforcement as no need to deploy covert surveillance to replace investigatory powers. Increased detection and prevention of crime, safeguarding of the general public and a likely reduction in threat to individuals from terrorism. Greater transparency, and public understanding of the use of investigatory powers, including public confidence in the oversight of investigatory powers and the accountability of those who may use them.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5
Technical complexity can increase projected costs. There is also a risk that technical solutions will be outpaced by technical change and/or changes in consumer behaviour. Continued use of powers available currently to the agencies and law enforcement under existing statutory bases provided for under the Investigatory Powers Bill.		

### BUSINESS ASSESSMENT (Option 2)

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



# Evidence Base

## A. Define the problem

The Data Retention and Investigatory Powers Act 2014 (DRIPA) was a fast-tracked piece of legislation responding to a ruling by the Court of Justice of the EU (CJEU), that the EU Data Retention Directive was invalid. DRIPA forms the basis for the UK's data retention regime, but is sunsetted to December 31 2016. DRIPA also clarified the application of the UK's legislation (the Regulation of Investigatory Powers Act 2000) to communication service providers. During the passage of that legislation, the Government committed to a review of investigatory powers by the Independent Reviewer of Terrorism Legislation, David Anderson QC. Two other reviews have been carried out in parallel, the Intelligence and Security Committee of Parliament (ISC) looked into the activities of the security and intelligence agencies and published a report in March 2015, and the Royal United Services Institute (RUSI) established a panel to review the impact on civil liberties of Government surveillance which concluded in July 2015. David Anderson's report was published in June 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. Existing legislation governing the use of investigatory powers is spread over a number of Acts, including but not limited to, the Regulation of Investigatory Powers Act 2000 (RIPA), the Telecommunications Act 1984, the Wireless Telegraphy Act 2006 (WTA), the Police Act 1997, the Intelligence Services Act 1994 (ISA), the Anti-Terrorism, Crime and Security Act 2001 (ATCSA), the Security Services Act 1989 (SSA), the Counter-Terrorism and Security Act 2015 (CTSA) as well as the Data Retention and Investigatory Powers Act 2014 (DRIPA).

The principal recommendation made by David Anderson was

1. *RIPA Part I, DRIPA 2014 and Part 3 of the CTSA 2015 should be replaced by a comprehensive new law, drafted from scratch, which:*
  - (a) *Affirms the privacy of communications;*
  - (b) *Prohibits interference with them by public authorities, save on terms specified;*
  - (c) *Provides judicial, regulatory and parliamentary mechanisms for authorisation, audit and oversight of such interferences'* (A Question of Trust, pg. 285)

The speed of technological change has increased rapidly over the last 15 years, since the enactment of RIPA. The use of cloud computing has made it easier to enter the market and provide new services, while the increase in encryption has made it more difficult for law enforcement and security and intelligence agencies to access, where necessary and proportionate, the content of communications and communications data. The use of electronic communications has grown: the Office of National Statistics reported 74% of adults in 2015 had used the internet 'on the go' using a mobile device<sup>1</sup>. Investigatory powers are a vital tool in the detection and prevention of terrorism and crime, such as cyber-crime, human trafficking and online child sexual exploitation. Without legislating to modernise the legal framework for the use of investigatory powers by law enforcement and the security and intelligence agencies, capabilities will continue to degrade.

David Anderson went further to recommend:

3. *The new law should be written so far as possible in non-technical language*

---

<sup>1</sup> Internet Access – Households and individuals 2015, Office of National Statistics release 6 August 2015



*4. The new law should be structured and expressed so as to enable its essentials to be understood by intelligent readers across the world' (A Question of Trust, pg. 285)*

The report of the Intelligence and Security Committee of Parliament concluded that the security and intelligence agencies do not seek to circumvent the law, but seek rigorously to comply with it. However, the legislation could be made clearer and more transparent to increase public understanding of what the agencies and law enforcement can and cannot do.

Without introducing new legislation, law enforcement and the security and intelligence agencies will continue to operate within the bounds of the law, but will see further erosion of the capabilities they rely upon to keep the public safe.

## **B. Rationale**

The Government must ensure that law enforcement, armed forces and the security and intelligence agencies have the powers they need to prevent terrorism and tackle serious and organised crime. Equally, the Government must ensure that the use of these powers is scrupulously overseen and subject to effective safeguards. It has a responsibility to ensure that the agencies that can exercise these powers can be held to account for their activities, that they are transparent (while protecting sensitive techniques), and that there is public understanding as to what types of activity may be undertaken and in what circumstances.

The use of investigatory powers is vital to preventing and detecting all forms of crime and for the purpose of safeguarding national security. Such powers might be necessary for the location of a missing and vulnerable person, to exonerate a suspect of a crime, or to avert a terrorist attack.

However, investigatory powers are by their nature intrusive, and their use must be subject to effective oversight and safeguards. Existing safeguards and oversight arrangements must be strengthened and made clearer. A clear expectation was set by the reviews undertaken by RUSI, the ISC and David Anderson that the Government should bring forward a comprehensive and comprehensible Bill that will provide a clear basis for the future use of investigatory powers.

## **C. Objectives**

The objective of any legislative change should be to update and modernise the legal framework for the use of investigatory powers, including communications data (targeted, and in bulk), interception (targeted, and in bulk), equipment interference (targeted, and in bulk) and the agencies' use of bulk personal datasets, as well as improvements to the oversight and safeguards that apply to these powers. The intended effect will be to mitigate the erosion of the capabilities used by law enforcement and the security and intelligence agencies by technological change, but to make sure these can be applied in order to protect the public, in a transparent way, with greater safeguards and controls on their use and where necessary and proportionate. Our objective is to improve public understanding and the ability of the agencies to lawfully detect, prevent and tackle terrorism and crime, including child sexual exploitation, fraud, human trafficking, cyber-crime, drug-trafficking and other harms. A key objective should be to make clear where and how those powers can be exercised, with a new regime for the authorisation and oversight of them.

## **D. Options**

Two options have been considered for legislation (although as the accompanying impact assessments set out, a further sub-set of options have been considered for each provision within the Bill). As with all options, our basic assumption is that the Government must retain a



data retention regime and retain the use of investigatory powers currently provided for under existing legislation.

- Option one: do nothing

No changes would be made to the authorisation and oversight regime and the legislation would remain spread over a number of Acts. All of the powers within the Bill in respect of interception, equipment interference and communications data – both targeted and bulk acquisition powers – would continue to be exercised under the existing statutory bases under existing safeguards. A gap would still remain in the ability of the agencies to gain access to the communications data required to progress investigations in an increasingly internet-based communications environment, and the capabilities of law enforcement would be further eroded over time.

- Option two: introduce a comprehensive piece of legislation

This option would re-legislate for all the investigatory powers that are used by law enforcement, armed forces and the security and intelligence agencies in respect of the acquisition, retention and examination of communications. It would consolidate RIPA Part I and IV, DRIPA, CTSA, ATCSA, parts of the Police Act, WTA, Telecommunications Act, and sections of ISA and SSA into a single, transparent and clear piece of legislation, and make apparent the safeguards and oversight that apply.

A powerful new the Investigatory Powers Commissioner would be established, replacing the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner. The Commissioner would lead a new oversight body, which would review and approve warrants authorised by the Secretary of State before they came into force, and audit the activities of the security and intelligence agencies and surveillance undertaken by law enforcement. It would be supplied with technical expertise, and have the power to refer cases to the Investigatory Powers Tribunal.

The powers in the legislation would be more transparent and subject to greater safeguards, with codes of practice to illustrate the retention, handling, destruction and audit arrangements for material acquired under the power, for each of the powers within the Bill. Legislation would be clearer and have greater foreseeability as the public understand when and how these powers can be used, with public confidence in the accountability to the public and to Parliament of the exercise of the powers.

## **Overview of the Investigatory Powers Bill**

An overview of each of the measures in the Investigatory Powers Bill is as below:

- Communications Data

The ability of law enforcement, armed forces and security and intelligence agencies to access communications data is eroding as communications change, including the ability to resolve IP addresses. The UK's data retention regime rests upon the Data Retention and Investigatory Powers Act 2014, which falls away on 31 December 2016. Government intervention is necessary to ensure continued availability of, and access to communications data, primarily for law enforcement.

Our proposal is to legislate to maintain the capability of relevant public authorities designated by Parliament to access communications data, both on a targeted basis and in bulk. This will



require replacing the provisions under RIPA Part IV and other statutes, and legislating for data retention necessary to provide for the identification of individuals accessing a specific service or device or identifying the services a specific device has accessed via internet connection records (local authorities will be prohibited from acquiring internet connection records.), and for the creation of a safeguard in the form of a request filter. It will also provide for an offence for the reckless or wilful acquisition of communications data, and a disclosure provision backed by a criminal offence. The legislation will provide for additional protections, in the form of Judicial Commissioner authorisation of acquisition of communications data for the identification of journalistic sources.

- Interception

Legislation is required to make clearer and more transparent the legislative basis for the interception of communications by law enforcement, the armed forces and the security and intelligence agencies on a targeted basis, and the interception of communications in bulk by the security and intelligence agencies.

Our proposal is to re-legislate to consolidate and maintain current interception capabilities provided for under RIPA and DRIPA and sections of the Wireless Telegraphy Act into the new Investigatory Powers Bill, 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. New legislation will include additional protections for the communications of Members of Parliament and other legislators. It will state that the Prime Minister must personally authorise any case where it is necessary to intercept a MP's communications. This 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

Legislation is required to make clearer and more transparent the use of targeted equipment interference for the acquisition of electronic communications by security and intelligence agencies, armed forces and law enforcement agencies, and the use of bulk equipment interference reserved for use by security and intelligence agencies, and to increase the safeguards and oversight of these powers.

Our proposal is to replace existing statutory bases for equipment interference for the acquisition of electronic communications into a single legislative provision that will provide for equipment interference by law enforcement, the armed forces and the security and intelligence agencies on a targeted basis, for equipment interference in bulk by the security and intelligence agencies, and to provide for requests to be made of communication service providers (CSPs) in respect of equipment interference.

- Bulk Personal Data

Legislation is required to make explicit and transparent the protections that apply to the security and intelligence agencies' acquisition and use of bulk personal data and the robust safeguards that are engaged.

Our proposal is to provide reinforced statutory safeguards, including the requirement for class-based authorisations, issued by the Secretary of State, subject to review by a judicial commissioner for the acquisition of BPD, and introducing a mechanism by which security and intelligence agencies would have to seek specific authorisation to exploit the most sensitive datasets, as well as making explicit the safeguards surrounding the acquisition and use of bulk personal data by the security and intelligence agencies in a statutory Code of Practice.



- Oversight of Investigatory Powers

The use of investigatory powers by public authorities and oversight of the work of the security and intelligence agencies more generally is split between three bodies: the Office of Surveillance Commissioners; the Intelligence Services Commissioner; and the Interception of Communications Commissioner.

Our proposal is to legislate to consolidate the existing oversight structures into the Investigatory Powers Commission, headed in statute by the Investigatory Powers Commissioner, who will approve warrants as part of a double-lock authorisation process and will have oversight of all the investigatory powers within the Bill.

- Right of domestic appeal from the Investigatory Powers Tribunal

Individuals who believe themselves to have been unlawfully surveilled can bring a case before the Investigatory Powers Tribunal (IPT) and currently those wishing to challenge a judgment from the IPT must bring it before the European Court of Human Rights (ECtHR), a system which is time consuming, opaque and difficult to understand. Legislation is necessary to provide the public with reassurance that the processes for holding the agencies to account are robust and effective.

Our proposal is to legislate to allow appeals to be brought in the domestic courts following permission to appeal from the IPT. This is intended to increase public confidence that those who use investigatory powers are fully held to account by the law, and that Articles 8 and 10 of the European Convention on Human Rights are respected. It will also serve to bring the IPT in line with the wider British Tribunal system and to lessen the cost of time and inconvenience for those who appeal.

## **E. Appraisal (Costs and Benefits)**

The legislation does not in the main provide for new powers, or expansion of existing capabilities. It replaces the existing statutory basis for investigatory powers, with three areas of associated cost:

- A new authorisation and oversight regime: costs borne by the public sector to set up the Investigatory Powers Commission and to run it on an ongoing basis;
- Increased costs associated with the data retention regime, to be borne by the public sector as a reimbursement to CSPs;
- Increased compliance costs associated with training and reporting requirements for law enforcement and the security and intelligence agencies.

There are no identified increased costs that should be incurred by the private sector that are not reimbursed by Government.

## **GENERAL ASSUMPTIONS & DATA**

We have assumed that the powers currently available to law enforcement, the armed forces and the security and intelligence agencies would remain in the long run were this Bill not brought forward.

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.

### **GROUPS AFFECTED**

- **Government Departments** (Home Office, FCO, MOD, NIO)
- **SIAs** (Security Service, Secret Intelligence Service, GCHQ)
- **LEAs** (National Crime Agency, the Police, HM Revenue and Customs)
- **Ministry of Justice**
- **HM Courts and Tribunal Service**
- **Crown Prosecution Service**
- **HM Prison Service**
- **The public**
- **The communications industry** – telecommunication service providers.

### **Option one: do nothing**

#### **COSTS**

The ongoing baseline costs of exercising investigatory powers would remain, with no cost incurred above those already established. A risk is that capabilities would continue to degrade as technological change develops. The resultant impact upon law enforcement and the security and intelligence agencies' ability to detect and prevent terrorism, serious and organised crime and other investigations would be an ongoing risk. There would be associated increased financial costs for covert surveillance as law enforcement and the security and intelligence agencies would be required to deploy alternate, more intrusive and more expensive methods to detect and prevent terrorism and serious crime. It is likely that safeguarding of vulnerable and missing people would not be possible as covert surveillance would not provide an alternate method of protecting those at risk from suicide, kidnap or sexual exploitation.

#### **BENEFITS**

There are no identified benefits associated with this option.

If we were to pursue this option, capabilities would continue to degrade as technological change develops. The resultant impact upon law enforcement and the security and intelligence agencies' ability to detect and prevent terrorism, serious and organised crime and other investigations would put public safety and national security at risk. Law enforcement and the security and intelligence agencies would be required to deploy less efficient and more intrusive methods to detect and prevent terrorism and serious crime.

Option 1 is the baseline against which option 2 is compared.

### **Option two: legislate for all investigatory powers**

#### **COSTS**

There would be minimal increases above existing baseline costs for interception, equipment interference and bulk personal data. The costs of the Bill are primarily in relation to increased cost of establishing a new oversight body (led by the Investigatory Powers Commissioner), including accommodation, overheads, running costs and the administration of a new warrant process. The provisions in the Bill in relation to internet connection records and the request filter



for communications data also have associated costs to business, which are reimbursed by Government.

## **BENEFITS**

The monetary benefits derived from this option would stem from the cost-effectiveness of investigatory techniques that would obviate the need for greater use of covert surveillance. These have not been quantified. The non-monetary benefits of this policy would include: greater public confidence in the transparency and clarity of the investigatory powers regime, greater safeguards and accountability of the investigatory powers regime to independent oversight, Parliament and the public, crimes detected, investigated and averted.

The specific costs and benefits relating to all of the measures within the Bill are set out in the table below. A discount rate of 3.5% has been applied to these costs, in accordance with HMT Green Book guidance.

<b>Policy provision</b>	<b>Net Present Cost over 10 years, £m (discounted)</b>	<b>Net Present Benefit over 10 years £m</b>	<b>Non-monetised cost</b>	<b>Non-monetised benefit</b>
Oversight	59.9	N/K	There are additional non-monetised costs as staff in the new bodies take time to familiarise themselves with new structures and reporting arrangements.	Increased public understanding of the oversight and accountability of investigatory powers. Public and Parliamentary trust and confidence in the rigour of Commissioner oversight and the way in which the use of investigatory powers is authorised. There are also likely to be efficiency savings from the merger of the existing oversight bodies, as shared resources and knowledge reduce duplication of effort.
Domestic right of appeal from the IPT	The Home Office and Ministry of Justice have agreed that the impact to the justice system is likely to be minimal.	N/K	There will likely be a necessary cost of time in order to train the IPT and its secretariat in the new rules and procedures.	Bringing the IPT in line with the broader British justice system will have a positive impact on those who are able to appeal. It will: <ul style="list-style-type: none"> <li>- be less time consuming than the current arrangements - whereby challenges are heard via the ECtHR process</li> <li>- be easier to understand</li> <li>- be less stressful to those involved</li> <li>- reassure the public that those who use investigatory powers can be fully held to account for their lawfulness, and that Article 8 and Article 10 of the European Convention on Human Rights are being upheld; and</li> <li>- Increase the transparency of proceedings as the IPT would confirm whether there was a valid point of law for appeal.</li> <li>- Fewer cases referred to the ECtHR, having been dealt with in the domestic courts – thus saving those bringing challenges both time and cost, and reducing the stress associated with long, drawn-out legal cases</li> </ul>
Interception	N/K	N/K	N/K	Greater public confidence and transparency in the interception regime. Legislation will allow UK intercepting agencies to continue to investigate threats to ensure they can keep the public safe.



Communications Data	187.1	N/K	There will be minimal business change costs associated with each of these capabilities, such as training for operational personnel.	Greater public confidence and transparency in the communications data regime. Law enforcement and public authorities able to access the data they need as part of investigations.
Bulk Personal Data	N/K	N/K	There will be additional training and familiarisation costs for the reporting arrangements, applicable to the Commissioners, SIAs, the Home Office and the Foreign and Commonwealth Office, policy officials and legal advisers as they spend time understanding the new authorisation and reporting arrangements.	Will improve public confidence in the safeguards that apply to the SIA use of bulk personal datasets, providing the public with greater understanding and transparency.
Equipment Interference	N/K	N/K	N/K	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 private data as a result of the clearer, robust safeguards and oversight applied to the use of equipment interference, with accountability to Parliament.

## **DIRECT COSTS AND BENEFITS TO BUSINESS**

There are no direct costs to businesses other than those for which there is reimbursement by the Government.

## **F: Risks**

There is an ongoing risk with all options outlined above that technology will continue to evolve and develop rapidly, outpacing legislation. We have assumed that 'do nothing' in part E would allow the Government to retain the existing data retention regime.

## **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 and statutory basis by the Investigatory Powers Commissioner. 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 will consider carefully the recommendations of the Joint Committee before bringing forward revised proposals for Introduction. Public consultation will form part of the pre-legislative scrutiny process.