Title: DATA RETENTION & INVESTIGATORY POWERS BILL - INTERCEPTION **IA No:** HO0125 **Lead department or agency:** Home Office **Other departments or agencies:** Law Enforcement, Security and Intelligence agencies	**Impact Assessment (IA)** **Date: 26/06/2014** **Stage:** Development/Options **Source of intervention:** Domestic **Type of measure:** Primary legislation **Contact for enquiries:** DRIPBill@homeoffice.x.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, Two-Out?**	**Measure qualifies as**
£0m	£0m	£0m	No	Zero Net Cost

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

The changing nature of global communications means that suspects in national security and serious crime investigations are increasingly making use of communications services provided from overseas. RIPA imposes obligations on any company providing services to the UK to comply with warrants issued by the Secretary of State for the interception of communications. It has become necessary to clarify RIPA in order to put beyond doubt the obligations imposed on services provided from outside the UK. This is essential to the prevention of terrorism and the detection of serious crime.

What are the policy objectives and the intended effects?

This legislation seeks to put beyond doubt the fact that RIPA obligations in relation to interception apply to all companies providing services to people in the UK, irrespective of where they are based.

It does not seek to extend the UK's reach or increase the powers of law enforcement and intelligence agencies beyond the original intention of RIPA. The costs and benefits associated with legislation are therefore unchanged from the status quo. However, the risk of companies failing to comply with their obligations will be reduced.

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

OPTION 1: No legislation / do nothing.

OPTION 2: Legislation to explicitly assert that RIPA obligations in relation to interception apply to all companies providing services to people in the UK (as required by recent case law).

As legislation is intended to maintain the status quo, there is no cost or benefit change associated with legislation. However, OPTION 2 presents a lower risk of non-compliance.

Will the policy be reviewed? It will not be reviewed. **If applicable, set review date:** Month/Year

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** No	**Small** No	**Medium** No	**Large** No
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)			**Traded:** 0	**Non-traded:** 0	

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister: Date: 9 July 2014

Summary: Analysis & Evidence

Policy Option 1

Description: Option 1 - No legislation / do nothing

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low: Optional	**High:** Optional	**Best Estimate:**

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

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

Base costs will remain the same under this option.

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

There are no non-monetised costs associated with this option. If the risk of companies failing to comply with their obligations were to be realised, costs may be incurred by seeking to compensate for the gap in intelligence coverage through the use of other investigative techniques.

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

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

n/a

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

n/a

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

1. Assumption that a perceived weakness in law may result in overseas CSPs reducing LI cooperation
2. Increased costs / resources through deployment of other investigative techniques if cooperation declines
3. Risk that HMG is seen to be failing to maintain the capabilites of law enforcement / intelligence agencies

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			In scope of OITO?	Measure qualifies as
Costs: 0	**Benefits:** 0	**Net:** 0	No	Zero net cost

Summary: Analysis & Evidence — Policy Option 2

Description: Option 2 - Legislation to recreate the mandatory data retention regime of the DRD, without addressing the European Court Judgment.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low:	High:	Best Estimate:

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

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

Base costs will remain the same under this option.

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				
High				
Best Estimate				

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

n/a

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

This option would reduce the risk of non-compliance with RIPA obligations associated with OPTION (1)

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

1. Assumption that legislation will address a perceived weakness in law that may have resulted in overseas CSPs reducing LI cooperation

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	Zero net cost

Background

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

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

3. Interception also ensures that finite law enforcement and agency resources – money and staff – are used to best effect.

Existing legal framework

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

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

5. To undertake interception, an agency must seek an interception warrant signed by a Secretary of State or a Scottish Minister. A warrant must consider the necessity and proportionality of the proposed interception and whether the information collected through interception could reasonably be obtained by other means.

6. The oversight regime provided under RIPA is intended to minimise intrusion and ensure that the intercepting agencies are acting lawfully. Agencies and warrant-granting departments are subject to scrutiny by an independent Interception of Communications Commissioner, whose findings are published annually. Redress for individuals who believe they have been wrongfully subjected to interception is provided by the Investigatory Powers Tribunal.

7. Safeguards are also in place to protect interception capabilities and the intelligence gathered through them. RIPA provides a framework for the protection of information collected through interception. It also creates a criminal offence for revealing that interception has taken place.

Problem under consideration

8. When RIPA was enacted 14 years ago, it was intended to provide a legislative regime fit for the information age. Since then, it has kept pace with changing technology.

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

10. It is now part of everyday life for people in the UK to communicate using services such as social media, instant messaging and web-based e-mail provided by overseas companies. These companies may not have any physical infrastructure in the UK and the services they provide are innovative, diverse and ever expanding.

11. It is not, therefore, surprising that the nature of the national security threat has been affected by technological developments and diversification. In his open evidence to the Intelligence and Security Committee of Parliament in November last year, the Director of GCHQ (Sir Iain Lobban) stated: "*I think [technological change] has helped the terrorists. I think our job is harder, has got harder, is getting harder. If you think about what the internet does for terrorists, it gives them a myriad of ways to communicate covertly. It gives them a platform, to fund-raise, to radicalise, to spread propaganda. It gives them the means to plan, to command and control, to spread lethal ideas, to exhort violence.*"

12. The changing nature of global communications means that suspects in national security and serious crime investigations are increasingly making use of communications services provided from overseas. RIPA imposes obligations on any company providing services to the UK to comply with warrants issued by the Secretary of State for the interception of communications. It has become necessary to clarify RIPA in order to put beyond doubt the obligations imposed on services provided from outside the UK. This is essential to the prevention of terrorism and the detection of serious crime.

Rationale for intervention

13. It is important that the UK's ability to investigate terrorism and serious crime is not eroded by the globalisation of telecommunications. It is vital therefore that there is no doubt as to whether RIPA imposes obligations on the range of services that are inevitably used by terrorists and criminals in their attack planning and criminal activities.

14. Part 1, Chapter 1 of RIPA sets out the obligations imposed on service providers to ensure the agencies can intercept the communications of those who would seek to do us harm. The original statute places an obligation on anyone providing a service to customers in the UK, regardless of where the company's infrastructure is based. But the law now needs to be more explicit.

15. In the absence of explicit extraterritoriality, these companies have started to question whether the law, as it currently stands, applies to them. This represents a real risk to the national security of the UK. Whilst these companies have always been bound by RIPA obligations, we want to put the matter beyond doubt.

16. Interception is a vital tool for law enforcement and security and intelligence agencies and they are heavily reliant on it for intelligence gathering purposes. Any reduction in co-operation will have a serious impact on national security and the ability to prevent or detect serious crime. We need to ensure that there is no doubt that the legislation is intended to apply to companies who are based outside the UK, and that it captures the range of services that are inevitably used by terrorists and criminals in their attack planning and criminal activities. Legislation must address this risk as quickly as possible.

17. This legislation is not intended to extend the UK's reach around the world. Rather, it is to confirm that RIPA obligations in relation to interception apply to all companies providing services to people in the UK irrespective of where they are based. Legislation will allow UK intercepting agencies to continue to investigate threats to ensure they can keep the public safe. It will enable law enforcement agencies to continue to intercept the communications of a member of a serious organised crime group arranging the importation of arms or Class A drugs; to identify where the pick-up is going to take place so they can do something about it. It will enable security and intelligence agencies to continue to intercept the communications of a would-be terrorist planning an attack in the UK; to identify who he's talking to, what he's planning to do and when, and to disrupt the plot before it is carried out.

Policy objective

18. The objective of this legislation is to put beyond doubt the fact that RIPA obligations in relation to interception apply to all companies providing services to people in the UK, irrespective of where they are based. This will maintain the ability of law enforcement and intelligence agencies to intercept the communications of those who wish to do us harm. It does not seek to extend the UK's reach or increase the powers of law enforcement and intelligence agencies beyond the original intention of RIPA. The proposed legislation will not impose any new obligations on UK business. Instead, it is intended to put beyond doubt the obligations that already apply to overseas providers.

Policy options

19. Two policy options have been considered:

OPTION 1: No legislation / do nothing;

OPTION 2: Legislation to explicitly assert that RIPA obligations in relation to interception apply to all companies providing services to people in the UK (as required by recent case law);

OPTION (1) – No legislation / do nothing

20. RIPA provides for obligations to be imposed on anyone providing telecommunications services to customers in the UK. However, it is not currently explicit that obligations may be imposed on companies overseas. In the absence of such provisions in RIPA, some overseas communications service providers have started to question whether the obligations set out in

Part 1, Chapter 1 of RIPA apply to them. Base costs of interception will remain the same under this option.

Risks

21. This option assumes that no action will be taken to address this perceived weakness in law, which could result in some communications companies reducing or ceasing their cooperation with law enforcement and intelligence agencies on interception.

22. If the risk of reduced cooperation were realised, the resulting loss of intelligence following an expected decline in cooperation poses a number of risks. It would lead to a rapid degradation of the operational capabilities of our law enforcement and 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.

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

OPTION (2) – Legislation to assert that RIPA obligations in relation to interception apply to all companies providing services to people in the UK irrespective of where the companies are based

24. This option would put beyond doubt Parliament's intention that RIPA should apply to companies providing services to customers in the UK irrespective of where they or their data is based. It would also address the calls from some communications companies to make this explicit in statute.

25. Given that this legislation is to put the current position beyond doubt, there are no extra costs when compared with OPTION (1). Under section 14 of RIPA, HMG already provides a "fair contribution" towards the costs of warranted interception to communications companies subject to RIPA obligations. As the current regime is simply being affirmed through new legislation, this process will continue as before. Base costs of interception will therefore remain the same under this option.

26. We anticipate no impact on HM Courts Service because the provisions will neither constitute a change to the current position as set out in law nor create a new criminal or civil offence. We intend to make explicit that the civil proceedings referred to in sections 11(8) and 12(7) of RIPA can be brought against a provider located outside the UK. However, this will not change the existing legislation, rather it will make explicit on the face of RIPA that sections 11 and 12 apply extra-territorially to communications service providers delivering services to those in the UK.

Risks

27. This option assumes that that legislation will address a perceived weakness in law that might otherwise have resulted in some communications companies reducing or ceasing their cooperation with law enforcement and intelligence agencies on interception.

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

Summary and conclusions

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

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

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

32. Base costs of interception would remain the same as they do currently under both options. However, if the risk associated with OPTION (1) were to materialise, the resulting intelligence gap would presents a far higher risk to public safety and national security when compared with OPTION (2), which would mitigate these potential risks.

33. On this basis, we intend to introduce legislation to affirm that RIPA obligations in relation to interception apply to all companies providing services to people in the UK.

Annex A – effect on industry

34. As under the current RIPA regime, new legislation would be designed to ensure that no public communications provider is either advantaged or disadvantaged by their obligations under RIPA.

35. As under current Part 1, Chapter 1 RIPA provisions, only those companies issued with a warrant will be required to provide interception capabilities. This legislation does not introduce any new requirements for communications companies, or place any unnecessary burdens on them. We will work with communications companies to ensure that any requests for assistance could be carried out with the least amount of impact on their business. This legislation will not affect UK-based companies. As a result, this policy is out of scope of One-In, Two-Out.

36. The infrastructure to support the provision of warranted intercept is already in place. Under section 14 of RIPA, HMG already provides a "fair contribution" towards the costs of warranted interception to communications companies subject to RIPA obligations. As the current regime is simply being affirmed through new legislation, this process will continue as before.

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

Annex B – effect on competition

38. The existing RIPA regime, prior consultation with communications companies, and "fair contribution" from HMG towards the cost of a communications company's interception capability (provided under section 14 of RIPA), already minimise the effect on competition. As our policy is simply to maintain the status quo, there will be no change in this regard.

Annex C – small firms test

39. As is the case with the current RIPA regime, under new legislation there is the potential for small and micro firms to have interception obligations placed on them. However, current safeguards, the "fair contribution" provision enacted under section 14 of RIPA, and prior consultation before obligations are imposed will mean that there is no additional impact on small firms.

40. It is worth noting that very small companies (with under 10,000 customers) are unlikely to be obligated to provide a strategic / permanent interception capability under Section 12 of RIPA, although they may still have tactical obligations to fulfil under Section 11 of RIPA.

Annex D – human rights considerations

The UK has one of the strongest systems of checks and balances and democratic accountability for secret intelligence anywhere in the world; at its heart are the Security Service Act 1989, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000. Our agencies activities therefore are subject to one of the strongest legal and regulatory

frameworks in the world. This ensures that their actions are necessary, proportionate and carried out in accordance with the law.

41. Intelligence activity is overseen by Secretaries of State, independent Commissioners, the cross-party Intelligence and Security Committee of Parliament (ISC) and held to account by the Investigatory Powers Tribunal. We consider that these safeguards provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy.

42. The ISC is currently conducting a review of the laws that govern the intelligence agencies' ability to intercept private communications and the appropriate balance between our individual rights to privacy and our collective rights to security. The Government will continue to cooperate fully with that review.

43. Interception is one of the most intrusive powers available to the state and is, quite rightly, subject to a strict authorisation and oversight regime. Currently, monitoring of interception is conducted by the Interception of Communications Commissioner. This will continue under new legislation.

Annex E – enforcement, sanctions and monitoring

44. This legislation includes clauses which make clear that Part1, Chapter 1 of RIPA applies to companies providing telecommunications service, whether they are based in the UK or overseas. We believe that this will provide companies with the necessary certainty that they are required to comply with these provisions in RIPA.

45. RIPA imposes penalties in the event that a communications company refuses to comply with an interception warrant. It also sets out the circumstances in which a company is requested to maintain a permanent interception capability. It is however possible that a company may refuse to comply with a notice requested it to maintain a permanent interception capability. In the event that an overseas company refuses to comply with such a notice there is an established process for applying to a UK court via civil proceedings for an injunction to enforce their compliance.

46. There is a process for enforcing decisions of UK courts overseas. We hope that these amendments make clear the scope of Part 1, Chapter 1 of RIPA and that companies can be obliged to provide assistance in relation to interception warrants. If companies still do not comply, there is an established judicial process via civil proceedings which would be followed.

Annex F – implementation and delivery plan

47. This is fast-track legislation that has been brought forward to address a particular pressing issue and to clarify the current position. It will be implemented at the point at which Royal Assent is given. Given that it simply asserts our current interpretation of Chapter 1, Part 1 of RIPA, an implementation and delivery plan is not required.

Annex G – post-implementation review

48. This is fast-track legislation that has been brought forward to address a particular pressing issue and to clarify the current position. It will be implemented at the point at which Royal Assent is given. Given that it simply asserts our current interpretation of Chapter 1, Part 1 of RIPA, a post-implementation review is not required.

Annex H – diversity impact

49. Continuation of the status quo does not affect the way in which end users currently use their communications services, so there is no diversity impact.

Annex I – consultation

50. The provisions contained within the proposed Bill have been consulted on across Government and with the intercepting agencies. They have also been shared with (a limited number of) Communication Service Providers. Given that this is fast-track legislation that has been brought forward to address a particular issue which seeks to continue the status quo, they have not been consulted upon more broadly.