Title: Data Retention and Acquisition Regulations **IA No:** HO0301	**Impact Assessment (IA)**
RPC Reference No:	**Date:**
Lead department or agency: Home Office	**Stage:** Development/Options
Other departments or agencies: FCO, NIO, Cabinet Office, NCA, MPS, GCHQ, MI5, SIS, MOD, wider law enforcement, other public authorities	**Source of intervention:** Domestic
	Type of measure: Secondary legislation
	Contact for enquiries: public.enquiries@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** (EANDCB in 2014 prices)	**One-In, Three-Out**	**Business Impact Target Status**
£3.2	£0	£0	Not in scope	Non qualifying provision

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

The ability of public authorities including law enforcement and the intelligence agencies to acquire communications data is vital to public safety and national security. Communications data has played a significant role in major crime investigations and in every major MI5 counter-terrorist operation over the last decade. Following the judicial review proceedings concerning the Data Retention and Investigatory Powers Act 2014 (DRIPA), legislative changes are required to the Investigatory Powers Act 2016 to comply with EU case law. These changes are necessary to ensure the continued availability of, and access to, communications data, in order to protect the public and enshrine further safeguards to govern its use.

What are the policy objectives and the intended effects?

The objective is that public authorities including law enforcement and the intelligence agencies can continue to lawfully access communications data, when necessary and proportionate to do so, to keep the public safe from terrorism, criminality and protect vulnerable people. The new provisions will give the Investigatory Powers Commissioner power to authorise most communications data requests by most public authorities; narrow the crime purpose for which certain types of communications data can be retained and acquired to serious crime; and provide further safeguards for the retention and acquisition of communications data, including independent authorisation of communications data requests.

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. Ignore the DRIPA judgment and be in breach of EU law. In this case it is highly likely that the domestic courts would have quashed the UK's data retention regime on the basis that there was no lawful process to access the data. Public authorities would only be able to acquire data that is held by telecommunications operators and postal operators for their own business purposes.

Option 2: Legislate to amend the Investigatory Powers Act to introduce additional safeguards and independent authorisation for the acquisition of communications data. Legislation is the preferred option as it will uphold the capability, providing a benefit to public authorities including law enforcement, and the intelligence agencies in their ability to protect the public.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** 12/2019

Does implementation go beyond minimum EU requirements?		No		
Are any of these organisations in scope?	**Micro** No	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:**	**Non-traded:**	

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: 26 Nov 2017

Summary: Analysis & Evidence

Policy Option 1

Description: Do nothing

FULL ECONOMIC ASSESSMENT

Price Base Year 2017	PV Base Year 2017	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'

This is the do nothing option. The additional monetised costs associated with this option have not been calculated.

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

This is the do nothing option. The additional monetised costs associated with this option have not been calculated.

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

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

This is the do nothing option. The additional monetised costs associated with this option have not been calculated.

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

This is the do nothing option. The additional monetised costs associated with this option have not been calculated.

Key assumptions/sensitivities/risks — **Discount rate** 3

There would be no lawful basis for a data retention regime. Changing communications technology and the unlawfulness of the existing legislation would likely result in the inability to acquire the data required in the fight against terrorism and criminality with a consequential increase in crime and reduction in criminal prosecutions, particularly for cyber-enabled crime such as fraud, online child sexual abuse and hacking.

BUSINESS ASSESSMENT (Option 1)

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

Summary: Analysis & Evidence

Policy Option 2

Description: Legislate to amend the Investigatory Powers Act

FULL ECONOMIC ASSESSMENT

Price Base Year 2017	PV Base Year 2017	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: N/K	High: N/K	Best Estimate: 3.2

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	N/K	2	N/K	N/K
High	N/K		N/K	N/K
Best Estimate	17.0		5.2	58.3

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

The key monetised cost is giving the IPC power to authorise communications data requests and the setting up and running costs of the Office for Communications Data Authorisation (OCDA) which will sit under the IPC's remit. This has a transition cost of **£17.0m** spread across 2017/18 & 2018/19 followed by an annual running cost of **£5.2m** for the next 8 years.

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		N/K	N/K
High	N/K		N/K	N/K
Best Estimate	N/K		N/K	61.5

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

The transfer of responsibility of the authorisation of communication data requests to the IPC (OCDA) will result in time and resource savings for public authorities. This is estimated at a saving of **£61.5m** over the 10 years in present value.

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

The key non-monetised benefit is the maintenance of the existing data retention regime and the subsequent benefit to counter-terrorism and serious crime investigations, and wider cases. This benefit is likely to be significantly greater than the monetised benefit above.

Key assumptions/sensitivities/risks — **Discount rate** 3.5

The courts would quash the UK's data retention regime on the basis that there was no lawful basis to access retained communications data. Public authorities, including law enforcement and the intelligence agencies would only have access to targeted communications data that telecommunications operators and postal operators had kept for their own business purposes which would be significantly less than our existing data retention regime. This would result in a reduction of the ability to acquire the data required in the fight against terrorism and criminality.

BUSINESS ASSESSMENT (Option 2)

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

Evidence Base (for summary sheets)

A. Strategic Overview

A.1 Background

Communications data is the 'who', 'where', 'when', 'how' and 'with whom' of a communication, but not what was written or said, and includes information such as the subscriber to a telephone service.

The Investigatory Powers Act 2016 (IPA) provides that telecommunications operators and postal operators may be required by the Secretary of State to retain communications data generated by them in the UK for up to 12 months, where it is considered necessary and proportionate to do so and where that decision has been approved by a Judicial Commissioner. Specified public authorities, including the police and the security and intelligence agencies, may acquire communications data from a telecommunications operator or postal operator where it is both necessary and proportionate to do so, for specified purposes.

The retention of, and ability to access, communications data is an essential tool for UK law enforcement and national security investigations. It is used to investigate crime, keep children safe, support or disprove alibis and link a suspect to a particular crime scene, amongst many other purposes. Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud.

Following an earlier ruling by the Court of Justice of the European Union (CJEU) in 2014 (Joined Cases C-293/12 and 594/12: *Digital Rights Ireland ltd and Seitlinger*, quashing the EU Data Retention Directive), the UK Parliament legislated for a domestic communications data retention regime through the Data Retention and Investigatory Powers Act 2014 (DRIPA). DRIPA provided for the Secretary of State to, amongst other things, require telecommunications operators and postal operators to retain communications data for a maximum of 12 months, where necessary and proportionate to do so for a number of statutory purposes. DRIPA contained a sunset clause, which meant that the legislation would expire on 31 December 2016.

The IPA received Royal Assent on 29 November 2016. Part 4 of the IPA, which replaces the communications data retention provisions in DRIPA, came into force in December 2016. Part 3 of the IPA, which provides for the acquisition of communications data (including retained data) by public authorities, has not yet been commenced. The relevant legislative framework for the acquisition of communications data therefore remains Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA).

Legal proceedings were brought in 2014 alleging, amongst other things, that DRIPA was incompatible with EU law. Although the Divisional Court ruled against the Government, the Court of Appeal provisionally found broadly in favour of the Government, but referred the case to the CJEU to clarify EU law. The CJEU handed down its judgment on 21 December 2016 (Joined Cases C-203/15 and C-698/15), specifying a number of requirements that need to be in place for a data retention regime to be compliant with EU law, but making it clear that it was a matter for the domestic courts to consider how this judgment should be applied to national legislation.

A.2 Groups Affected

- Telecommunications operators and postal operators
- UK intelligence community (UKIC)
- Law enforcement agencies (LEAs)
- Other specified public authorities using communications data
- The Investigatory Powers Commissioner

- The Information Commissioner;
- 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 affected by the proposed amendments of legislation were consulted as part of the policy development process. The Government has consulted extensively with the law enforcement and intelligence community, the Investigatory Powers Commissioner and his staff, along with staff in the Office of the Interception of Communications Commissioner who until recently had oversight of the use of this legislation. The Government has also engaged with telecommunications operators and postal operators likely to be affected by the legislation.

Public Consultation

These are issues of public importance, and accordingly the Government is consulting on what changes should be made in response to the judgment. In particular, the consultation sets out what changes are currently proposed in response to the judgment and, where no changes are proposed, explains why the Government considers that the regime already addresses the requirements of the CJEU's judgment.

B. Rationale

Communications data remains a vital tool utilised in major crime investigations. The UK also continues to face significant threats from serious and organised crime and terrorism. These threats span "old" crimes using new technology to new threats such as cyber-dependent and cyber-enabled crimes. These threats are accentuated by the rapid and persistent expansion in the development and adoption of new communications technologies, which continue to transform government, business and the ways in which individuals interact. They confer a level of privacy that protects citizens but makes it easier for criminals to conceal their activities.

Following the CJEU ruling, the Government accepted in the domestic litigation that DRIPA, and consequently some aspects of Part 4 of the IPA, are inconsistent with EU law, in that:

a) there is no provision for independent authorisation of requests for access to retained data; and

b) the crime purpose for retaining and accessing data is not limited to serious crime.

The Government has given careful consideration to the CJEU's judgment, bearing in mind the importance of communications data as an investigative tool used by those responsible for keeping citizens safe. It is considered that some aspects of our current regime for the retention of and access to communications data do not satisfy the requirements of the CJEU's judgment and therefore the Government proposes to amend the Investigatory Powers Act 2016.

The Government proposes to make changes to the IPA through regulations made under section 2(2) of the European Communities Act 1972, which permits the Secretary of State to amend primary legislation by regulations to implement EU law obligations as in this case.

It is important that any changes support the important right to individual privacy and the collective right of citizens to be protected from crime and terrorism. It is also important to ensure that the police and other specified public authorities can continue to be able to access and use retained communications data in a way that is consistent with requirements of EU law and with our responsibilities to protect the public.

C. Objectives

Retention and Acquisition of communications data

The draft Regulations aim to ensure that the Secretary of State can continue to lawfully require telecommunications operators and postal operators to retain communication data in order to allow public authorities including law enforcement agencies and intelligence agencies to have continued lawful access to crucial communications data they need in the fight against terrorism and criminality, as well as to protect vulnerable people, when necessary and proportionate to do so and subject to strict safeguards.

The draft Regulations will provide for the independent authorisation of most communications data requests. The Investigatory Powers Commissioner will be responsible for the independent authorisation of most communications data via the Office for Communications Data Authorisations which will be under his control. The Regulations will also restrict the crime purpose for which certain data types can be retained and acquired to 'serious crime' and a small number of other offences where communications data is crucial.

The draft Regulations will also:

- Add additional considerations that must be taken into account by the Secretary of State before a retention notice is given to telecommunications operators and postal operators
- Allow for public authority authorisation where the request is related to national security or the work of the intelligence agencies or where there is an urgent need to acquire the data (for example where there is a threat to life).
- Replace magistrate approval of local authority applications with authorisation by the IPC. Local authorities are prohibited from authorising requests internally.
- Further restrict the purposes for which data can be acquired and retained by removing three purposes – public health, tax collection and financial regulations

D. Options

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

This would mean that the Government would ignore the CJEU judgment and the UK would be in breach of EU law. In response to this the domestic courts would very likely quash the UK's data retention regime because there would be no lawful basis upon which to access this data. Public authorities would only be able to acquire data that is held by telecommunications operators and postal operators for their own business purposes. This would have a significant adverse impact on terrorism and criminal investigations, and wider cases such as locating missing persons. Investigating crimes will become a lottery with capability highly variable across telecommunications operators and postal operators.

Option 2 Amendments to the Investigatory Powers Act introduce clearer safeguards and independent authorisation of most types of communications data requests.

This option includes a number of new provisions including:

- **Independent authorisation**: the draft Regulations create a new power for the Investigatory Powers Commissioner (IPC) to authorise communications data requests except in urgent cases. The IPC will be able to delegate these functions to a newly appointed body of staff, to be known as the Office for Communications Data Authorisations (OCDA). OCDA will report directly to the IPC, and will be responsible for considering the vast majority of requests to access communications data made by public authorities.

- **Restriction to serious crime:** the proposed amendments to the legislation provide a definition of 'serious crime' for the purposes of the retention or acquisition of events data, which will apply to investigations into all offences for which an adult is capable of being sentenced to six months or more in prison; any offence involving violence; any offence which involves a large number of people acting in pursuit of a common purpose; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or any offence involving a significant financial gain.

Additionally, three of the statutory purposes for which data can currently be retained or acquired will also be removed; namely public health, tax collection and financial regulation.

- **Internal authorisation for urgent cases:** the judgment recognises that it is acceptable to authorise requests internally in cases of validly established urgency. Accordingly, the new regime will allow for internal authorisation by a designated senior officer in a public authority where there is an urgent need to obtain communications data. Authorising urgent requests internally will be available to all public authorities except local authorities, who will be prohibited from authorising communications data requests internally for any purpose.

- **Internal authorisation in other cases**: the Regulations provide that communications data requests made for purposes related to national security, including serious crime requests made by the UK Intelligence Community can, if the public authority wishes to do so, continue to be authorised internally.

- **Magistrate approval of local authority application:** given previous concerns on local authority access to communications data, the Regulations will replace magistrate approval of local authority applications with authorisation by OCDA

- **Additional considerations before issuing a Retention Notice:** the Regulations include additional considerations that must be taken into account by the Secretary of State before a Retention Notice is given to a telecommunications operators and postal operators.

E. Appraisal (Costs and Benefits)

GENERAL ASSUMPTIONS & DATA

- The calculation of economic costs is in line with HM Treasury Green Book guidance, and includes discounting at 3.5%. The costs outlined below are also without allowing for inflation, Value Added Tax and depreciation.
- Optimism bias (OB) has been applied to costs as mitigation against projects and programmes being over optimistic about project costs and duration.

Cost assumptions are based on the following:

- These costs represent the expected cost of the Office for Communications Data Authorisation (OCDA). The expected volume of communication data requests was used to model the staff required. The majority of the start-up costs occur in 2018/19 with some minor CDEL costs of setting up occurring in 2017/18.
- Staff costs have been calculated using the mid-point of the salary scale for that grade and account for non-wage costs such as pensions, National Insurance and security clearance.
- IT costs have been sourced from Home Office IT and previous charges/quotes.
- Estimates of accommodation costs were provided by Home Office Property Group.
- Remaining costs such as travel, stationery, and conferences were provided by the relevant bodies, and used to make extrapolations.

OPTION 2 – Legislate

COSTS

The best estimate of the total discounted cost of these policies above the baseline over the 10 year period is **£3.2m** (present value). A discount rate of 3.5% has been applied to this cost, in accordance with HMT Green Book guidance.

The predominant cost is the setting up, maintenance and on-going staffing costs of the OCDA. These costs have been informed by detailed volumetric analysis of anticipated communication data requests volume. The transition cost is spread over 2017/18 and 2018/19 and the average annual

cost is hereafter stable. The Government anticipates that the "go live" date of the OCDA will be from July 2018. The table below presents a detailed picture of the expected costs.

Table 1 – Summary of Estimated Costs for Option 2

	Transition Cost (2017/18 & 2018/19)	Average Annual Cost (excl Transition)	Total Over 10 Years
Facilities (Discounted)	£452,467	£104,404	£1,287,703
Staff (Discounted)	£6,729,847	£3,528,322	£34,956,422
IT (Discounted)	£3,416,359	£493,864	£7,367,270
Project Team (Discounted)	£3,036,665	-	£3,036,665
Optimism Bias	£3,408,835	£1,031,648	£11,662,015
Total (Discounted & 25% contingency/Optimism Bias)	£17,044,174	£5,158,238	£58,310,075

For the management team, the Government assesses that there will be the need for one Senior Civil Servant as a Senior Manager and 4 Grade 7 Managers. It is estimated that approximately 68 FTE of Authorising Officers will be required; broken down between 10 SEOs, 46 HEOs and 12 EOs. There will also be a supporting admin team of 7 FTE split between 2 EOs and 5 AOs. The other costs include the cost of the facilities, the required IT, stationary and travel.

Optimism bias of 25% has been applied to the total not the component costs.

There is no expected cost on the Criminal Justice System as this is only a change to a current process.

BENEFITS

The key benefit of this option, which is non-monetised, is the upholding of the capability through the full retention of communications data. Without this, public authorities would only be able to acquire data that is held by telecommunications and postal operators for their own business purposes. This would lead to a significant loss in capability causing an adverse impact on terrorism and criminal investigations, and wider investigations such as locating missing persons.

Home Office analysts have estimated that the portion of capability lost through this would be substantial. Every major counter-terrorism investigation by MI5 over the last decade has used communications data and if this was lost, there would be significant capability loss for cases where data was not already held. Communications data is not only used in counter terrorism investigations or against serious crime, its usage allows the police to mitigate threat to life in a number of situations such as vulnerable missing persons. With limited access in these cases, police forces would not, for example, be able to prevent loss of life where communications data has provided location data when a vulnerable person. Subsequently, there is a considerable benefit through the retention of the full suite of the UK's data retention regime

The monetised benefit from the OCDA is the lessening of the burden on the LEAs of authorising communication data requests. By centralising the process of authorising communications data requests, this will allow for LEAs to re-allocate the time spent currently on authorisation to other activities.

The Government estimates, through analysis showing the need for IP Act training for current LEA authorising officers, that there are currently 4,338 active LEA authorising officers. It is assumed that they spend 2% of their current time on authorisations. This gives a current LEA FTE on authorisations of 86.76. It is further assumed that 75% of these applications are authorised by superintendents (£104,265 per annum) and 25% by inspectors (£71,909 per annum). This gives an annual cost to

the LEA's of **£8,344,195**. This is therefore the annual benefit of the OCDA as all authorisations, aside from a minimal proportion of urgent cases, will now be handled through the OCDA thus saving this cost to LEAs. As the go-live date of the OCDA is expected to be July 2018, the Government have calculated 9 months of savings in FY 18/19 and the full savings every year subsequently.

SUMMARY

Overall, there is a positive Net Present Value (NPV) of **£3.2m** over the next 10 years. This is back ended as a result of the high upfront costs of setting up the OCDA followed by the resource saving once the Office is into normal operation through the lessening of the burden on LEAs. However, as the benefit of the retention of the data regime and subsequent capabilities is non-monetised, this is a significant understatement of benefits and NPV of the policy option.

Option 2 - Regulate	
Costs over 10 years (£m in present value)	£58,310,075
Benefits Over 10 Years (£m in present value)	£61,464,511
Net Present Value (NPV)	£3,154,436
Benefit-Cost Ratio (BCR)	1.05

Business Impact Target

There is no expected cost or benefits to civil society or businesses in scope of the Business Impact Target. The Government is committed to full cost recovery for telecommunications operators and postal operators. As there is no expected impact on business through guaranteed full cost recovery and the size of businesses involved, there is no need for a small and micro-business assessment (SaMBA).

F. Risks

OPTION 2 – Legislate

There are risks involved in setting up the new independent body for the authorisation of communications data requests. The main risk is that the procurement of premises, recruitment and training of staff, as well as the development of the necessary IT systems for the OCDA may take longer than expected.

G. Enforcement

No changes will be made to the enforcement of the Investigatory Powers Act 2016. As is currently the position, only those companies issued with a notice will be required to retain data. The regulations are not intended to introduce any new requirements for communications companies, or place any new burdens on them.

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	£58.3m (PV over 10 years)	£61.5m (PV over 10 years)
		Non monetised benefit maintenance of the existing data retention regime and

		the subsequent benefit to counter-terrorism and serious crime investigations, and wider cases

Source: Refer to the costs and benefit section

I. Implementation

The Government recognises the importance of complying with EU law; as such, the relevant provisions in the Data Retention and Acquisition Regulations will come into force as soon as possible. Implementation of the provisions relating to independent authorisation of communications data requests will be dependent on the time it takes to set up the OCDA. The task of setting it up is significant. It involves the procurement of premises, recruiting and training new staff, and the development of the necessary IT systems and processes which will allow OCDA staff to electronically consider applications from over 600 public authorities. It is anticipated that the OCDA will begin considering applications from July 2018.

J. Monitoring and Evaluation

The application of the new provisions will continue to be scrutinised on an ongoing basis by the Investigatory Powers Commissioner, an independent member of the judiciary responsible for oversight of the use of Investigatory powers by all public authorities, who will provide yearly reports on the exercise of powers within the Act. The Investigatory Powers Tribunal will continue to provide a right of redress to any individual who believes they have been unlawfully surveilled.

K. Feedback

The Government will consider any public submissions made as part of the consultation process.