Title: Data Retention and Acquisition Regulations **IA No:** HO0319 **RPC Reference No:** **Lead department or agency:** Home Office **Other departments or agencies:** FCO, NIO, Cabinet Office, NCA, MPS, GCHQ, MI5, SIS, MOD, wider law enforcement, specified other public authorities	**Impact Assessment (IA)** **Date: June 2018** **Stage:** Final **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** N/A	**Business Impact Target Status**
-£17.8m	£0	£0	N/A	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 (CD) is vital to public safety and national security. Following litigation in respect of the Data Retention and Investigatory Powers Act 2014 (DRIPA), legislative changes are required to the current regime (the Investigatory Powers Act 2016) to ensure compliance with EU case law. The UK courts have ordered these changes be made by 1 November 2018. Without change the current regime would be declared unlawful and public authorities would not have access to a substantial amount of CD which would adversely affect their ability to prevent and detect crime and safeguard vulnerable people.

What are the policy objectives and the intended effects?

The objective is that public authorities, law enforcement and intelligence agencies, can continue to lawfully access CD, when necessary and proportionate to do so.

The intention is to use CD to help keep the public safe from terrorism, criminality and to protect vulnerable people.

The new provisions will give the Investigatory Powers Commissioner power to 1) authorise most CD requests by most public authorities, 2) narrow the crime purpose for which certain types of CD can be retained and acquired to tackle serious crime, and 3) provide safeguards for the retention and acquisition of CD, including independent authorisation CD 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. This significantly limits the amounts of CD available to the authorities and may increase the risk to the public from crime and terrorism. This does not meet the Government's objectives to keep the public safe from terrorism, criminality and to protect vulnerable people.

Option 2: (the Government's preferred option). Legislate to amend the Investigatory Powers Act to introduce additional safeguards and independent authorisation for the acquisition of CD. This would help strengthen the authorities ability to protect the public.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** 04/2020

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

I have read the Impact Assessment and I am satisfied that (a) it represents a fair and reasonable view of the expected costs, benefits and impact of the policy, and (b) that the benefits justify the costs.

Signed by the responsible Minister: Ben Wallace Date: 26th June 2018

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/A	**High:** N/A	**Best Estimate:** -17.8

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low		3		
High				
Best Estimate	13.2		7.8	67.1

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

The main monetised costs are the set up and ongoing costs of the Office for Communications Data Authorisation (OCDA) which, sitting under the IPC's remit, will have the power to authorise CD requests. This transfer of power has a transition cost of £13.2 million spread across 2017/18, 2018/19 and 2019/20. The ongoing costs commence in late 2018/19, with steady state running costs from 2019/20 at £7.8 million.

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			7.4	49.3

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

The transfer of responsibility of the authorisation of CD requests to the IPC (OCDA) will result in time and resource savings for law enforcement agencies. This is estimated at a saving of **£49.3 million** over the 10 years in present value terms.

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

The main 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 is a significant benefit.

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 CD. Public authorities, law enforcement and the intelligence agencies would only have access to CD 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 in 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: N/A	**Benefits: N/A**	**Net: N/A**	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). This Act, 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.

On 30 January 2018, the Court of Appeal held that DRIPA was incompatible with EU law on the grounds that it did not provide for independent authorisation of the acquisition of communications data, and because access to data for the purpose of preventing or detecting crime was not limited to serious crime. Similarly, on 27 April 2018, the Divisional Court held that the IPA is incompatible with EU law, for the same reasons as DRIPA.

A.2 Groups Affected

UK wide:

- 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 policeand 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 to legislation were consulted as part of the policy development process. The Government has consulted extensively with the law enforcement and intelligence communities, 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 publicly consulted on the changes proposed in response to the CJEU judgment. Several changes were made to the legislation and Code of Practice as a result. Where there are no changes, the Government has explained why it considers the regime already addresses the requirement of the CJEU's response. The consultation closed on 18 January 2018, and a Government response was published on 28 June 2018.

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.

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, in the area of criminal justice:

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.

Govt intervention is required to provide legislation compatible with EU legislation so to ensure continuity of access to CD

Therefore the Government proposes to amend the Investigatory Powers Act 2016 through Regulations made under section 2(2) of the European Communities Act 1972, which permits the Secretary of State to amend primary legislation by Regulation to implement EU law obligations.

It is important that any changes support the 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 Regulations ensure that the Secretary of State can continue to lawfully require telecommunications operators and postal operators to retain communication data. This will allow public authorities, including law enforcement agencies and intelligence agencies, to have continued access to communications data that is crucial in the fight against terrorism and criminality, and protect vulnerable people. The powers can only be used when it is necessary and proportionate to do so and are subject to strict safeguards.

The Regulations will give power to the Investigatory Powers Commissioner (IPC) to authorise most communications data requests. The IPC will manage this regime with a body of staff to be known as the Office for Communications Data Authorisations (OCDA). The Regulations will also restrict the crime purpose for which certain data types (events data) can be retained and acquired to 'serious crime' plus offences with aggravating features such as those involving violence or where the communication was integral to the offence.

The 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 internal 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.
- Add additional considerations that must be taken into account by the Secretary of State before a retention notice is given.

D. Options

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

Public authorities would only be able to lawfully 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 would become a lottery with capability highly variable across telecommunications operators and postal operators.

Option 2 Amendments to the Investigatory Powers Act to 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 Regulations create a new power for the Investigatory Powers Commissioner (IPC) to authorise communications data requests. The IPC will

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 Regulations 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 12 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.

- **Internal authorisation for urgent cases:** the CJEU 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 all 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:** the Regulations will replace magistrate approval of local authority applications with authorisation by OCDA which will report directly to the IPC

- **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 operator or postal operator.

E. Appraisal (Costs and Benefits)

GENERAL ASSUMPTIONS & DATA

- The calculation of economic costs and benefits are in line with HM Treasury Green Book guidance. The appraisal period is 10 years and includes discounting at 3.5 per cent.
- The costs outlined below are in 2017/18 prices, excluding VAT.
- Optimism bias (OB) has been applied to costs as mitigation against projects and programmes being over optimistic about project costs and duration.

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.
- 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

Transition costs (monetised)

Costs to the public sector
Set up costs of the OCDA include facilities, staff, IT and the project management team.

Estimates of facility costs were provided by Home Office Property Group.

Staff costs have been calculated from the volume of staff multiplied by the relevant staff wage. Staff wages uses 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.

For the project management team, the Government assesses that there will be the need for one Senior Civil Servant, one Grade 6 Senior Manager and 5 Grade 7 Managers, 4 SEO, 2 HEO and 1 EO. Project management team costs are calculated from the volume of staff multiplied by the relevant staff wage.

Transition costs are spread over 2017/18, 2018/19 and 2019/20, and total £13.2 million, which is £12.9 million over 10 years in present value (PV) terms.

Ongoing costs (monetised)

Costs to the public Sector

Ongoing costs include facilities, staff, training and IT.

Estimates of facility costs were provided by Home Office Property Group.

The expected volume of communication data requests was used to model the staff required.
It is estimated that approximately 69 FTE of Authorising Officers at EO Grade will be required as well as 14 HEO team leaders. There will be additional senior operational staff including a Chief Operating Officer and security lead, with the team consisting of 1 Grade 6, 2 Grade 7s, and 7 SEOs. There will also be a supporting admin team of 25 FTE split between 1 Grade 7, 4 SEOs, 5 HEOs, 1 EO and 6 AOs who will work on non-operational roles. There will also be a Chief Executive who will be a Senior Civil Servant. Staff costs are calculated from the volume of staff multiplied by the relevant staff wage, total £5.9 million per year.

IT costs have been sourced from Home Office IT and previous charges/quotes.

The ongoing costs commence in late 2018/19, with steady state ongoing costs from 2019/20 at £7.8 million each year. This is £54.2 million over 10 years in present value (PV) terms.

Table 1 – Summary of Estimated Costs for Option 2 (£m, 2017/18 prices, excl. VAT, incl. OB)

Category	Transition Cost (2017/18, 2018/19 and 2019/20)	Average Annual Cost (excl Transition)	Total Over 10 Years
Facilities	2.6	0.7	8.6
Staff	0.1	5.9	48.9
Recruitment	0.3	0.0	0.3
Training	0.4	0.1	1.1
IT	5.3	1.1	14.9
Project Team	4.4	0.0	4.4
Total Costs	**13.2**	**7.8**	**78.2**
Total Costs (Discounted at 3.5%)	**12.9**	**54.2**	**67.1**

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

BENEFITS

Ongoing Benefits (monetised)
The policy will reduce the number of CD requests authorised internally thus freeing up authorising officer time that can be re-allocated and spent on other activities.

In law enforcement agencies (LEAs), the Government estimates there are currently 4,300 active authorising officers.

It is assumed that they spend 2 per cent of their current time on authorisations. This gives a current LEA FTE on authorisations of 86.76. It is further assumed that 75 per cent of these applications are authorised by superintendents (£104,265 per year) and 25 per cent by inspectors (£71,909 per year). This gives an estimated annual cost to the LEA's of £8.3 million.

All authorisations apart from a proportion of urgent cases (estimated at 11%), will now be handled through the OCDA thus saving this cost to LEAs. Therefore the final annual efficiency saving will be **£7.4 million.**

The ongoing benefits commence in April 2019 and total £7.4 million in each year, at a present value (PV) of about £49.3 million over 10 years.

Table 2 – Summary of Estimated Benefits for Option 2 (£m, 2017/18 prices, excl. VAT)

Category	Average Annual Benefit (excl Transition)	Total Over 10 Years
LEA efficiency savings	7.4	59.4
Total Benefits (Discounted at 3.5%)		49.3

Ongoing Benefits (non-monetised)

Public
The main benefit of this option, which is non-monetised, is maintaining the capability to require the retention of communications. 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, adversely affecting a wide range of investigations, including those into terrorism, fraud, child abuse and efforts to find missing persons.

Criminal Justice System
There is a benefit of magistrates' time savings as the Regulations will replace magistrate approval of local authority applications with authorisation by OCDA. This will not result in cashable savings but represents savings in the opportunity cost of magistrates' time currently spent authorising local authority applications.This will also apply to Scotland and Northern Ireland however due to availability of data, this benefit has not been monetised.

Optimism Bias

The following levels of optimism bias has been applied to the estimated costs as mitigation against projects and programmes being over optimistic about project costs and duration, sourced from Home Office Finance and IT.

Table 3 – Optimism Bias summary, 2018, (%).

Category	Optimism Bias (%)
Facilities	20
Staff	10
Recruitment	20
Training	25
IT	20
Project Team	0

Sensitivity Analysis and Scenarios
Sensitivity analysis has been developed for facilities, IT costs and the monetised benefits of LEA efficiency savings.

LEA efficiency savings
As detailed above in the Benefits section, it is assumed that LEA authorising officers spend 2 per cent of their current time on authorisations. Monetised benefits are driven by this assumption and relative salaries. If LEAs actually spent 2.8 per cent of their time authorising applications then the **NPV will increase from -£17.8 million to £0, therefore break-even in monetary terms.**

SUMMARY

Overall, there is a negative Net Present Value (NPV) of **-£17.8m** over the next 10 years. This is due to the high upfront costs of setting up OCDA, particularly staff and facilities. This is largely offset by the resource savings once OCDA is into normal operation by 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.

Table 4 – Summary table, 2018, £ million.

Option 2 - Regulate	£ million
Costs over 10 years (£m in present value)	67.1
Benefits Over 10 Years (£m in present value)	49.3
Net Present Value (NPV, £m)	-17.8
Benefit-Cost Ratio (BCR)	-0.74

Business Impact Target

As the Government provides full cost recovery for telecommunications operators and postal operators under a retention notice, there is no overall impact to civil society or businesses as the EANDCB is £0. There is no impact to small and micro-businesses and therefore no small and micro-business assessment (SaMBA).

F. Risks

OPTION 2 – Legislate

There are risks involved in setting up OCDA. 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

Table H.1 outlines the costs and benefits of the proposed changes.

Table H.1 Costs and Benefits, £ million.		
Option	**Costs**	**Benefits**
2	£67.1m (PV over 10 years)	£49.3m (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
NPV		-£17.8m

Source: Home Office internal analysis.

I. Implementation

The Government recognises the importance of complying with EU law. The Divisional Court has set a deadline of 1 November 2018 for the legislative amendments to be made to those aspects of the regime the Government has accepted does not comply with EU law; namely in relation to

serious crime and independent authorisation. The court has accepted that the practical implementation of the independent authorisation of communications data requests will take longer. It is a significant task that involves the procurement of premises and recruiting and training of new staff to consider applications from over 600 public authorities. As such, it is currently anticipated that the OCDA will begin considering applications by April 2019.

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 annual 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.

To meet objectives it is important that the changes result in compliance with EU law. This would be achieved through the successful set up of OCDA which is able to handle the current level of CD applications. It is also important that communications data requests for crime are restricted to 'serious' crime.

A key evaluation measure for the policy changes would be the absence of a successful legal challenge once the new Regulations are in place.

K. Feedback

On 30 November 2017, the Government held a public consultation on proposed changes to the regime and on the code of practice. The consultation closed on 18 January 2018. There were 794 responses received, of which 716 were a direct result of a campaign run by the digital campaigning organisation Open Rights Group, which encouraged its supporters to submit their views based on areas of concern expressed by Open Rights Group. The remaining 78 submissions were made by academics, members of the public, legal representatives, public authorities, telecommunications and postal operators, media groups, oversight bodies and civil society groups.

The responses received provided useful and constructive feedback. A summary of the feedback and the Government response can be found at:
https://www.gov.uk/government/consultations/investigatory-powers-act-2016