

Title: DATA RETENTION LEGISLATION IA No: HO0126 Lead department or agency: Home Office Other departments or agencies: Law Enforcement, Security and Intelligence agencies	Impact Assessment (IA)		
	Date: 27/06/2014		
	Stage: Development/Options		
	Source of intervention: Domestic		
	Type of measure: Primary legislation		
	Contact for enquiries: Public line/inbox		

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 Two-Out?
-£8.4m	£0	£0	No
			NA

What is the problem under consideration? Why is government intervention necessary?
 The need for legislation follows a European Court of Justice judgment, which declared the European Data Retention Directive invalid (although it did also acknowledge that data retention is of the utmost importance to public security). The judgment has left us needing to ensure that communications companies in the UK carry on retaining this key information (known as communications data) so that it continues to be available when it is needed by law enforcement and others to investigate crime and protect the public. Without this Bill, vital evidence from telephones and the internet that is needed by the police on a day to day basis might be lost. More crimes, including the most serious such as child sexual exploitation, may go unpunished.


What are the policy objectives and the intended effects?
 It will simply preserve the status quo by ensuring that there is a functioning data retention regime with a clear basis in law that acknowledges the ruling. But it will not create any new powers, rights to access data, or obligations on communications companies that go beyond those that already exist.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)
 1. No legislation/do nothing.
 2. Legislation to recreate the mandatory data retention regime of the Data Retention (EC Directive) Regulations 2009 addressing the European Court Judgment where possible.

 Option 2 is the preferred option, as it will address the policy objective.

Will the policy be reviewed? It will be reviewed. If applicable, set review date: 01/2016					
Does implementation go beyond minimum EU requirements?				Yes	
Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base.		Micro Yes	< 20 Yes	Small Yes	Medium Yes
What is the CO ₂ equivalent change in greenhouse gas emissions? (Million tonnes CO ₂ equivalent)				Traded: N/K	Non-traded: N/K

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: 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'
 Baseline case - zero cost.

Other key non-monetised costs by 'main affected groups'
 Baseline case - zero cost.

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'
 Baseline case - zero benefit

Other key non-monetised benefits by 'main affected groups'
 Baseline case - zero benefit

Key assumptions/sensitivities/risks **Discount rate (%)**
 If a successful legal challenge leads to the loss of the mandatory data retention regime, then there would be implications for retention and acquisition of CD from business data or held under other legislation. Reduced access to CD in key cases is likely to necessitate greater reliance on other more expensive (and intrusive) investigative techniques such as surveillance, which could possibly total £millions each year.

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	NA

Summary: Analysis & Evidence

Policy Option 2

Description: Option 2 - Legislation to recreate the mandatory data retention regime of the DRD, addressing the European Court Judgment where possible.

FULL ECONOMIC ASSESSMENT

Price Base Year 2014	PV Base Year 2014	Time Period Years 5	Net Benefit (Present Value (PV)) (£m)		
			Low:	High:	Best Estimate: -£8.4m

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low			
High			
Best Estimate	-£22m	£8.3m	£8.4m

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

Compared to option 1, option 2 presents costs. Those shown above are the estimated cost of retention and access to data held under the DRR plus that of additional safeguards. The relevant infrastructure within Communications Service Providers etc already exists and the costs involved would in large part remain to be incurred with respect to CD from business data and retained under other legislation. The cost will continue to be funded by HMG, as will additional costs on the Information Commissioner's Office.

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

Compared to option 1, option 2 (i.e. as under the existing DRR) has greater potential implications for privacy – see more detail in a separate Privacy Impact Assessment. However, option 2 introduces safeguards intended to mitigate these impacts and address, insofar as is practicable, points raised by the ECJ ruling. There may also be CSP familiarisation costs, which will also be borne by HMG.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low			
High			
Best Estimate	Not Quantified	Not Quantified	Not Quantified

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

Direct financial benefits arise from the support that communications data provides to investigations into financial crimes, and any resulting seizure of criminal assets. This will provide benefits over option 1. These benefits already exist under the DRR and will be protected under this option. This option, for example, breaks-even should only £1.68m of the total annual recovery of criminal profits of £150m by the NCA flow from that agency's access to CD retained by means of the DRR.

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

CD is used in a wide range of criminal prosecutions and threat to life investigations. It means that more resource-intensive and intrusive investigative methods do not need to be deployed. This option will provide benefits over option 1. These benefits already exist under the DRR and will be protected under this option. It breaks even, for example, if (based on monetised values for specific crimes) use of CD retained under the DRR was instrumental in preventing (by successful prosecution of offenders) 43 sexual offences pa.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5%
<p>Assumptions and risks are detailed in the evidence base.</p> <ol style="list-style-type: none"> 1. Assumption that without enhanced legislation, a successful legal challenge could cause the loss of the mandatory regime 2. Risk of being perceived as ignoring the ECJ judgment 3. Potential reduction in HMG funding in this area 		

BUSINESS ASSESSMENT (Option 2)

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

Evidence Base

Background

Communications data (CD) is the context not the content of a communication: who was communicating; when; from where; and with whom. It includes the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It does not include the 'what' – i.e. the content of any communication – such as the text of an email or a conversation on a telephone. Communications data is defined in the Regulation of Investigatory Powers Act 2000 and is legally distinct from a communication's content.

Communications data is a key tool for modern policing and has been used successfully for many years. Information about communications activity was used in 95% of all serious organised crime investigations handled by the Crown Prosecution Service between July 2012 and February 2013. And it has been used in every major Security Service counter-terrorism investigation over the last decade.

It has also played a significant role in the investigation of a very large number of other serious and widely reported crimes, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman, the 2007 Glasgow Airport terror attack, and the murder of Rhys Jones.

Where an investigation starts with an internet communication, such as in online child sexual exploitation cases or identifying the location of people at risk of imminent harm, communications data will often be the only investigative lead. If this data is not retained, these cases will go unsolved.

Existing legal framework

The EU Data Retention Directive (Directive 2002/58/EC) passed into EU law in March 2006. This required European Member States to implement legislation into their own national law requiring communications companies to retain specific communications data sets for retention periods between 6 and 24 months.

Domestic retention of data is governed by the UK Data Retention (EC Directive) Regulations (DRR), passed by parliament in 2009, which are based on the European Data Retention Directive, as well as other legislation – notably, on a voluntary basis under the Anti-terrorism, Crime and Security Act 2001 (ATCSA). Other data may also be held by Communication Service Providers (CSPs) for business purposes.

Access to communications data by law enforcement and intelligence agencies (and other relevant public authorities) is primarily regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA places strict rules on when, and by whom, and for what purpose, data can be obtained. It provides authorities with a framework for acquiring communications data that is consistent with the European Convention on Human Rights (ECHR), ensuring that it is only accessed where it is necessary and proportionate to do so for a specific investigation.

The processing of personal information, including communications data, and the storage of personal data by industry is also subject to the Data Protection Act 1998 (DPA).

Problem under consideration

The need for legislation has been prompted by a European Court of Justice judgment, which declared the European Data Retention Directive invalid – while also acknowledging that data retention is a valuable tool in law enforcement investigations of the utmost importance to public security.

In the wake of the judgment, it is the Government's position that the UK Data Retention (EC Directive) Regulations 2009 remain in force. Communications Service Providers in receipt of a notice under the Regulations have been informed that they should continue to observe their obligations as outlined in any notice. However, given that the Directive which they implement has been declared invalid, there is a risk that in a worst case scenario, without a new legal basis being put in place, a legal challenge to the 2009 Regulations will be successful.

This Impact Assessment has been drafted based on the risk of this worst case scenario being realised, and should not be considered to be prejudicial to the Government's position that the DRR remain in force.

Rationale for intervention

As a result of the fact that the domestic Regulations are based on the European Directive, this judgment has made it highly desirable to put beyond any doubt the legal basis on which CSPs in the UK retain this key information so that it continues to be available when it is needed by law enforcement and others to investigate crime and protect the public.

Failing to do so would mean that, in the "worst case" event of a successful legal challenge an effective data retention regime in the UK would not longer be possible. In particular communications data would not be available to law enforcement unless it was kept by CSPs for business purposes – for certain key data types, such as location data or device information, this is normally no longer than three months, and sometimes much less.

Without these powers, it would be harder or impossible to investigate a range of crimes effectively. This includes:

- Murder – those who conspired to assist the killers of Rhys Jones were caught using evidence from mobile phones that proved they were associating at certain key times and places.
- Sexual exploitation – the men who groomed young girls in Rochdale were prosecuted in part through mobile phone call evidence which showed their association with each other and contact with victims.
- Drugs – a gang operating in Merseyside, Lancashire, Glasgow and South Wales in 2011 was found with 30kg of drugs and £37,000. Mobile phone call and text evidence was

used to determine the gang's hierarchy and identify key individuals. This resulted in the arrest of two gang members not identified using normal surveillance techniques.

- Door step fraud – a gang who conned an 85-year-old were prosecuted by evidence they had called the victims repeatedly from their mobile phone.
- Locating Vulnerable People – mobile phone location data was used to direct a search by Mountain Rescue and locate an elderly man with medical conditions who had gone missing following a hospital appointment.

Although it is difficult to be definitive about the impact of not requiring companies to retain data, a major recent Europol investigation into online child sexual exploitation (known as Operation Rescue) gives an indication. Of 371 suspects identified in the UK, 240 cases were investigated and 121 arrests or convictions were possible. In contrast, of 377 suspects identified in Germany, which has no such data retention arrangements, only seven could be investigated and no arrests were made.

The analysis and estimates set out in this Impact Assessment are based on the risk of the loss of the mandatory regime, and the subsequent need to ensure the continued availability of this data.

Policy Objective

It is our objective to simply preserve the status quo by ensuring that there is a functioning data retention regime with a clear basis in law that also addresses, to the extent practicable, the points raised in the ECJ judgment. We do not intend to create any new powers, rights to access or obligations on CSPs that go beyond those that already exist.

By creating a robust legal framework the Bill ensures that this critical information, which has been available in the past, will continue to be available to law enforcement when it is needed, subject to robust safeguards and oversight.

Groups Affected

The groups affected by this legislation will be:

- Communications Service Providers (CSPs);
 - Law Enforcement Agencies (LEAs);
 - Security and Intelligence Agencies (SIA);
 - Other designated Public Authorities using communications data;
 - The Interception of Communications Commissioner and the Information Commissioner;
- and

- 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.

Policy Options

Two policy options have been considered:

1. No legislation/do nothing.
2. Legislation to recreate the mandatory data retention regime of the Data Retention (EC Directive) Regulations 2009, addressing the European Court Judgment where possible.

Option 1 – No legislation / do nothing

In the wake of the judgment, the UK Data Retention (EC Directive) Regulations 2009 are considered to remain in force. Communications Service Providers in receipt of a notice under the Regulations were informed that they should continue to observe their obligations as outlined in any notice.

As stated above, this Impact Assessment has been drafted on the basis that at some point the DRR may be subject to legal challenge, and that in a worst case scenario, this challenge would be successful. Were such a challenge successful, the mandatory regime might be lost. As a result, vital data would no longer be retained for appropriate access by law enforcement and other agencies.

Following the loss of the mandatory regime, the data available would amount to data retained for business purposes, and that retained voluntarily under the ATCSA. Not all communications service providers are willing to retain data voluntarily, and would be even less so in the absence of a parallel mandatory regime.

Providers not retaining data voluntarily would delete their data as soon as business needs had been met. While the companies may hold subscriber data (such as their customers' names and addresses) and some service use data (such as their billing records) for an extended period, more specific traffic data relating to individual communications (such as location data or device identifiers) is unlikely to be kept for any more than three months – and often far less than this. These data types are often crucial to investigations that involve electronic communications.

As the “do nothing” option represents the baseline approach, this assessment estimates zero costs and benefits.

A situation where the Government was no longer able to require communications service providers to retain communications data would lead to a rapid degradation of the operational capabilities of our law enforcement and intelligence agencies. The use of communications data within investigations would also be complicated by inconsistencies between CSPs (i.e. some have data, but others do not as they lack a business need), and, over time, criminals might be expected to migrate to companies with more limited retention periods.

The Government has considered carefully possible alternatives to the continued use of communications data in the investigation of crime and has concluded that there is no comparable like-for-like alternative. Directed surveillance (i.e. surveillance in a public place) and intrusive surveillance (i.e. surveillance in a private place, such as a home) do not provide essential historical information required in criminal investigations when investigating a crime that has already occurred. Nor would they provide rapid, accurate information of the kind available through communications data. They also involve greater intrusion into privacy and are much more costly. For example, maintaining twenty-four hour surveillance coverage of even one individual involves multiple officers and administrative staff working around the clock. This option does not assume as part of the baseline that any of these costs would be incurred.

A wide range of criminal and threat to life investigations and prosecutions – including investigations into murder and terrorism – will be jeopardised. More crimes would go unsolved and the public could be put at risk. The Government may be perceived as failing to ensure the capabilities of law enforcement agencies. Such a scenario would also be contrary to a Government commitment in the Strategic Defence and Security Review¹ to maintain communications data capability.

The impact on law enforcement of a lack of comprehensive data retention is illustrated by the experiences of Germany, where data retention measures were annulled in March 2010. According to federal and state police, in 44.5% of the cases involving requests for historical data traffic data, there was no other means of conducting the investigation and, following the annulment, 30% of criminal cases collapsed.²

Option 2 – Legislation to recreate the mandatory data retention regime of the Data Retention (EC Directive) Regulations 2009, addressing the European Court Judgment where possible

This option would involve restoring the status quo, by recreating the mandatory data retention regime of the DRR using domestic legislation. It would address the opinions of the ECJ judgment where practicable to do so.

The cost estimates represent the difference in those between option 1 and option 2, estimated over the relevant period and subject to discounting to generate a present value. It follows Treasury “Green Book” methodology.

The costs reflect the secure decommissioning of systems that CSPs have developed to meet their DRR obligations, and the subsequent change costs for CSP business systems to support their ongoing disclosure obligations. Maintaining the current standard/speed of response in an environment without data retention stores would be technically more complex, leading to costs that could offset the reduction in retention costs. Such parameters have been considered and reflected in the analysis.

If the mandatory regime is retained there will not be any costs from decommissioning and modifying systems, which would have somewhat offset any cost savings from a reduction in data volumes retained.

¹ www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf

² http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf

The wider potential implications (in terms of the need for potentially greater reliance on other more intrusive and resource intensive means of investigation) should existing access communications data be lost have already been highlighted.

Costs therefore amount to £8.4 million (PV over 5 years). This includes additional costs relating to the Information Commissioner's Office (ICO), amounting to £320,000.

The 5 year time period has been chosen because proposals covering this area will be re-examined in connection with any future proposals to address the communications data capability gap. This is likely to take place within five years.

In reality, the infrastructure to support the retention and storage of data by Communications Service Providers, and the secure and reliable transmission of data, already exists. It is current Government policy to reimburse 100% of costs for storage of data required to be retained under the legislation. The current mandatory regime is simply being replaced and there are therefore no plans to change this policy. Familiarisation costs, and any measures introduced to address the ECJ judgment, will continue to be funded by the Government.

Compared to option 1, option 2 also presents benefits. This approach would allow mandatory retention to continue as before and the ability of law enforcement to obtain communications data would be unaffected. They would continue to be able to investigate crime, protect the public and ensure national security. At the same time, the risk of any subsequent legal challenge would be reduced. It would also strengthen what is already recognised as one of the world's best oversight and authorisation systems. The Government commitment in the Strategic Defence and Security Review to maintain communications data capability would also be upheld.

We have undertaken a "break-even" analysis which illustrates the scale of monetary and non-monetary benefit which would be required for the measure to secure a positive net present value. For this option to break even, the costs of £8.4 million would need to be met following implementation.

This option would break even at the point at which the use of retained communications data led to the seizure of criminal assets totalling £1.68 million per annum. This should be read in conjunction with the fact that the National Crime Agency, which relies heavily on retained communications data in its investigation of serious and organised crime, recovers over £150 million of criminal profits each year, and denies access to even larger amounts – £500 million in 2012/2013.³

Similarly, using monetised values for specific crimes⁴, retained communications data would need to be instrumental in avoiding (by means of successful investigation, disruption and prosecution of offenders) 1 homicide or 43 sexual offences per annum. This should be read in conjunction with the fact that in the year ending December 2013, in England and Wales there were a total of 551 homicides and 60,894 sexual offences recorded.⁵

In reality such estimates could be made across the spectrum of offences to which CD is used to help tackle. For example, information about communications activity was used in 95% of all

³ Serious Organised Crime Strategy, Home Office, October 2013

⁴ From 'The economic and social costs of crime against individuals and households 2003/04', Home Office, 2005, inflated to 2013 prices using Green Book methodology

⁵ Crime in England and Wales, Year Ending December 2013, Office for National Statistics.

serious organised crime investigations handled by the Crown Prosecution Service between July 2012 and February 2013.

Summary and conclusions

Our policy intention is to maintain the ability of the law enforcement, security and intelligence agencies to obtain communications data in the absence of the Data Retention Directive.

Option 1 was discounted because, in anything other than the short term, it would fail to meet the policy intention. The loss of the mandatory regime following a successful legal challenge would mean that, in time, less data than is currently available could be accessed for law enforcement purposes, representing a retrograde step.

We believe that the implementation of Option 2 would meet our policy objectives. This option represents the most secure way of restoring the status quo and ensuring the continued ability of law enforcement to obtain communications data.

Imposing this option does have costs when compared to the “do nothing” approach. However, we believe that continued access to retained data by law enforcement would mean that this option would more than breakeven.

In reality, the infrastructure to support the retention and storage of data by Communications Service Providers, and the secure and reliable transmission of data, already exists. These costs are already borne by the Home Office. Any costs arising as a result of addressing the ECJ will also be borne by the Home Office.

It is important to note that creating the mandatory regime is not the same as actually imposing obligations upon providers. There are a number of steps that would be required before a CSP would find itself subject to a notice. These are set out in full in Annex A.

On this basis, we intend to introduce legislation to recreate the mandatory data retention regime of the Data Retention (EC Directive) Regulations 2009 while also addressing ECJ opinions regarding the previous regime.

Annex A: Effect on Industry

As under the DRR, the legislation is intended to ensure that no public communications provider is either advantaged or disadvantaged by the continued requirements to retain communications data, or the provisions for reimbursement of additional costs.

The creation of a new mandatory regime will not impose the obligation to retain data on all communications providers. Only those subject to a notice will be required to retain data. As under the DRR, the Home Office will enter into discussions with communications companies prior to them being issued with a notice. However, under the new legislation this consultation with industry will become a mandatory requirement. These consultations will include discussion of:

- The best method of storing the data. This will vary depending on the circumstances of each company; however, key considerations in each case will include data security and the availability of data for law enforcement.
- The timing of when the company is able to become compliant with any notice. This will involve balancing the needs of law enforcement with the ability of the company to deliver the solution.

The infrastructure to support the retention and storage of data by Communications Service Providers, and the secure and reliable transmission of data, already exists. It is current Government policy to reimburse 100% of costs for storage of data required to be retained under the legislation. The current mandatory regime is simply being replaced and there are therefore no plans to change this policy. This process will therefore continue as before. Familiarisation costs arising as a result of addressing the ECJ's opinions will also be borne by the Home Office.

Annex B: Effect on Competition

As under the DRR, the legislation is intended to ensure that no public communications provider is either advantaged or disadvantaged by the continued requirements to retain communications data, or the provisions for reimbursement of additional costs. The existing notice-based approach, prior consultation, and cost recovery mechanisms outlined above, all of which already exist, will minimise any implications.

Annex C: Small Firms Test

As under the DRR, under replacement legislation there is the potential for small and micro firms to have obligations placed upon them. However, the notice-based approach and prior consultation already outlined will allow the implications and mitigations for any small or micro firms to be discussed, and the cost recovery mechanisms will cover any additional costs. As our policy intention is to simply maintain the status quo, there will also be no additional impact on small or micro firms.

Annex D: Human Rights Considerations

The UK already has one of the most stringent communications data oversight and authorisation systems in the world. In addressing the ECJ's concerns, where practicable, the new legislation will go even further in safeguarding human rights.

Further safeguards will include:

- Specifying further requirements around what information Ministers must consider before issuing a data retention notice on a communications service provider.
- Amending the set period for which data is retained from 12 months to a maximum of 12 months (allowing for shorter periods if there is lesser need)
- Limiting access to retained communications data to RIPA, court orders and certain other limited circumstances.
- Ensuring that specific data security requirements must be specified in a notice to each CSP when it is issued, rather than in commercial arrangements as at present.
- Ensuring the legislation specifies the duties of the Information Commissioner so he can oversee all of the relevant aspects of the retention of data (including when this is destroyed and integrity of data).

We consider that these new safeguards, in addition to those already existing, provide a rigorous check against the risk of disproportionate interferences with individuals' right to privacy.

A more detailed description of the impact on privacy is set out in a separate Privacy Impact Assessment.

Annex E: Enforcement, sanctions and monitoring

Currently, the monitoring of access to communications data is conducted by the Interception of Communications Commissioner. This will continue.

Under new legislation, we will clarify that the Information Commissioner's Office (ICO) will have responsibility not just for the security of retained data, but also the destruction and integrity of retained data.

Further monitoring surrounds the use of grant agreements for costs covered by the Home Office. The companies subject to mandatory retention may need to be reimbursed for valuable equipment.

This will continue to be monitored and subject to audit by the Home Office and HM Treasury under this legislation. Through this audit regime, we will ensure any potential element of business benefit is identified. If the company decides to make use of any identified business benefit, then they would be required to provide appropriate contributions to the cost of the data retention solution.

Obligations placed on CSPs under this legislation (including obligations to maintain the security of data) can be enforced by civil proceedings brought by the Secretary of State. However,

continuing to adopt a cooperative approach will mitigate the requirement for sanctions, with the Home Office paying any additional costs that the CSPs incur to ensure that they are not disadvantaged.

Annex F: Implementation and delivery plan

Following Royal Assent of primary legislation, the Government will seek to take forward the consequent secondary legislation in autumn 2014. This will include regulations that set out the detailed safeguards that will accompany the regime.

Meanwhile, the content of any prospective notices will be negotiated with the CSPs identified as processing data of interest to law enforcement. This consultation will be based on a range of factors, including those set out in Annex B.

Upon approval of the new regulations, the agreed notices will be considered by the Secretary of State and issued to those where she deems such a requirement to be necessary and proportionate.

Annex G: Post-implementation review

We will continue to record – on an exception basis – evidence from law enforcement and intelligence agencies to demonstrate both difficulties and benefits arising from this legislation.

The legislation will be re-examined by Parliament within a set time period and replaced or amended as necessary. This re-examination is likely to take place in connection with future proposals in order to address the communications data capability gap. Capabilities are continuing to degrade as a result of new internet-based technologies. As a result, an increasing and significant proportion of communications records that could be useful to operations are not available to the police and intelligence agencies (at the required timeliness or quality). This has a direct impact on the investigation of crime in this country and on our ability to prosecute criminals and terrorists. Any future legislation taken forward in this area could re-examine the issues relating to mandatory data retention. The Prime Minister has made clear that the wider issue of communications data retention, including the matters dealt with in the Draft Communications Data Bill in 2012, will need to be considered early in the next Parliament (in 2015-16).

There will also be an obligation on the Home Secretary to keep under review notices issued to service providers.

Annex H: Diversity Impact

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

There have been a number of rounds of public consultation in the area of access and retention of data. This includes on the Data Retention Regulations 2007 and 2009, the draft Communications Data Bill in 2012, the Regulation of Investigatory Powers Act 2000, and the Anti-Terrorism Crime and Security Act 2001.

The Draft Communications Data Bill also underwent Pre-Legislative Scrutiny by a Joint Committee of both Houses, and the Intelligence and Security Committee (ISC). They reported on 11 December 2012 and 5 February 2013 respectively.

This policy replicates the provisions in the existing DRR, on which there was a consultation in 2009. As our policy intention is to simply maintain the status quo as under the DRR, we have not undertaken consultations on this scale. However, we have consulted with law enforcement and intelligence agencies, other public bodies including the Information Commissioner, and CSPs.

Creation of the new Retention Code of Practice, as well as amendments to the Acquisition and Disclosure Code of Practice, will be preceded by public consultations.

Annex J: Environmental Impact

It is not known if pursuing option 2 will have an environmental impact. There are likely to be a number of both positive and negative impacts. For example, this could include the environmental impact of continuing data storage. In the alternative, there may be impacts arising from having to pursue other investigative techniques. These impacts have not been explicitly calculated.