EXPLANATORY MEMORANDUM TO

THE DATA RETENTION (EC DIRECTIVE) REGULATIONS 2009

2009 No. 859

1. This explanatory memorandum has been prepared by the Home Office and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 These draft Regulations are intended to complete the transposition of Directive 2006/24/EC into UK law. They require public communications providers to retain certain categories of communications data, which they generate or process, for a minimum period of 12 months.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None

4. Legislative Context

4.1 The draft Regulations complete the transposition of Directive 2006/24/EC, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. They relate to internet access, internet e-mail and internet telephony, as well as mobile and fixed line telephony. They revoke, and supersede, the Data Retention (EC Directive) Regulations 2007 (SI 2007/2199) which transposed the parts of Directive 2006/24/EC relating to mobile and fixed line telephony.

4.2 Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (ATCSA) already provides a legal basis for the retention of communications data in the UK for certain purposes. Parliament approved a voluntary code in connection with this in 2003. In addition, the Data Retention (EC Directive) Regulations 2007 made the retention of communications data relating to mobile and fixed line telephony mandatory. The draft Regulations will make the retention of communications data relating to internet access, internet e-mail and internet telephony, as well as mobile and fixed line telephony, mandatory rather than voluntary.

4.3 Section 106 of the ATCSA makes provision for the Secretary of State to make arrangements for payments to public communications providers in specified circumstances. Under the voluntary code of practice, the Home Office has maintained a policy of reimbursing public communications providers for additional costs incurred through retaining and retrieving communications data in line with the voluntary code. It has maintained this policy in relation to data retained in accordance with the Data Retention (EC Directive) Regulations 2007. The Impact Assessment (attached at Annex A) has identified the importance of ensuring that the draft Regulations are cost neutral to industry. Provision has therefore been made in the draft Regulations to

enable reimbursement of any costs incurred by public communications providers as a result of complying with them.

4.4 A transposition note is attached at Annex B to provide clarity on how the articles in the Directive relate to the draft Regulations. The Directive was examined and cleared by the European Scrutiny Committee at their meeting on 18th January 2006 (Report no 26872). The Directive was considered in Dossier 12660/05 and was cleared by Sub-Committee F of the House of Lords on14/12/2005.

5. Territorial Extent and Application

5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

The Minister of State for the Home Department, Vernon Coaker, has made the following statement regarding Human Rights:

"In my view the provisions of the Data Retention (EC Directive) Regulations 2009 are compatible with the Convention rights."

7. Policy background

- ***What is being done and why***

7.1 Communications data, which does not include the contents of communications, has proved valuable for law enforcement purposes over many years. Lawful access to communications data allows investigators to identify suspects and their 'hidden' means of communication, trace their criminal contacts, establish hierarchical relationships between conspirators, place them in specific locations at specific times, identify their banks and those engaged in laundering their criminal finances and assets both in the UK and abroad, and can confirm or disprove suspects' alibis.

7.2 In murder cases especially the analysis of communications data gives an insight to the victims' movements and details of people they had contact with, using communications equipment, prior to their death. In other cases, communications data can corroborate the testimony of victims, in particular those subject to sexual assault where the offender claims prior contact with the victim. It is regularly used by the police to assist Her Majesty's Coroner in establishing the activity of a deceased person prior to their death where no crime has occurred. The Child Exploitation and Online Protection Centre, set up by the Government just over two years ago, is completely reliant on the retention of internet-related data by public communications providers to be able to carry out its function of protecting our young citizens by identifying sexual offenders in the online environment.

7.3 Given the essential role communications data plays in assisting law enforcement agencies in protecting our citizens and bring offenders to justice, the Government has for some years sought to ensure that it is retained and made available

to appropriate public authorities lawfully, consistently and efficiently. This has been achieved through Part 11 of the ATCSA and its associated voluntary code since 2003, and, in respect of mobile and fixed line telephony, through the Data Retention (EC Directive) Regulations 2007 since they came into force in 2007. The draft Regulations are a further step in this process.

8. Consultation outcome

8.1 The draft Regulations have been subject to a 12 week public consultation exercise which concluded in October 2008. During this exercise, Home Office officials met with a broad range of public communications providers and their trade associations, the Association of Chief Police Officers, the intelligence agencies, privacy lobbyists and other individuals. A total of 54 responses were received. Many responses were from members of the public who were opposed to the Directive on principle but did not offer suggestions on the wording of the draft Regulations (24 out of 54 responses). Public communications providers welcomed the Government's approach subject to five main concerns, which are addressed below.

8.2 First, draft Regulation 5 has been amended to remove a provision which would have enabled the Secretary of State to vary the period for data must be retained under the Regulations by notice.

8.3 Second, draft Regulation 9 has been amended to ensure that all statistics required to be collected under Directive 2006/24/EC are also required to be collected under the draft Regulations.

8.4 Third, draft Regulation 10 has been amended so that the Secretary of State must issue a notice to any public communications provider required to retain data under the Regulations. Under the amended version of draft Regulation 10, the Secretary of State must issue such a notice to a public communications provider unless the data to which the Regulations apply are retained in the UK in accordance with the Regulations by another public communications provider.

8.5 Fourth, several responses to the consultation exercise expressed concern about how the draft Regulations ought to be interpreted in practice. The Government undertakes to establish an "implementation group". This will develop guidance to assist in the implementation of the draft Regulations.

8.6 Finally, a number of responses queried the meaning of the term "e-mail". The Government confirms that the term "email" has the same meaning as "electronic mail" which is defined in the Privacy and Electronic Communications (EC Directive) Regulations 2003, transposing Directive 2002/58/EC into UK law. Both terms therefore refer to "any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

9. Guidance

9.1 The "implementation group" referred to above will develop guidance to assist in the implementation of the Regulations so that the new obligations which they impose are fully understood and complied with.

10. Impact

10.1 The impact on business, charities or voluntary bodies is cost neutral.

10.2 The impact on the public sector is £46.58 million over three years.

10.3 An Impact Assessment is attached to this memorandum.

11. Regulating small business

11.1 The legislation applies to small business.

11.2 To minimise the impact of the requirements on firms employing up to 20 people, the approach taken is that such firms will only be required to retain data under the draft Regulations if the Secretary of State issues a notice to them requiring them to do so. In addition, all communications service providers which incur additional costs as a result of the draft Regulations will be reimbursed in accordance with draft Regulation 11.

12. Monitoring & review

12.1 Article 14 of Directive 2006/24/EC requires the Commission to submit to the European Parliament and Council an evaluation of the Directive and its impact with a view to determining whether it is necessary to amend its provisions and in particular the types of data or the retention periods which it details. The "implementation group", which the Government undertakes to establish, will, in addition to assisting in the implementation of these Regulations, monitor and review their effectiveness and impact and will assist the Government in formulating a submission to the Commission giving notice of any amendments considered necessary.

13. Contact

Andrew Knight (Home Office, Room P5.37, 2 Marsham Street, London, SW1P 4DF, Tel No: 0207 035 4848, or email: commsdata@homeoffice.gsi.gov.uk) can answer any queries regarding the instrument.

Annex A – Impact Assessment

Summary: Intervention & Options

Department /Agency:	Title: Impact Assessment of The Final Transposition of the EU Data Retention Directive	
Stage:	**Version:** 1	**Date: 10 February 2009**
Related Publications: Final Transposition of Directive 2006/24/EC: relating to the retention of communications data.		

Available to view or download at:

http://www.homeoffice.gov.uk/documents/cons-2008-transposition

Contact for enquiries: Andrew Knight **Telephone:** 0207 035 4848

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

The Police, Security and Intelligence agencies and additional public authorities rely heavily on communications data to undertake their law enforcement and public safety functions. For long running investigations there is a danger that this vital data will be erased by the communications company and therefore no longer be available to assist law enforcement. This European Directive was designed to make the retention of communications data by communications companies mandatory, so it will continue to be available for law enforcement.

What are the policy objectives and the intended effects?

The Directive represents a transition from the current voluntary regime in the UK, to a framework which mandates minimum requirements for retention of internet-related data across EU Member States. This will create greater certainty that communications data will be available to support long running investigations, which tend to be those into murder, serious sexual offences and terrorism. Retaining this data will better enable law enforcement organisations to build stronger prosecution cases (providing evidence in court) and also to prevent serious offences before they happen.

What policy options have been considered? Please justify any preferred option.

1) Stop work on internet data retention. 2) Continue with voluntary data retention. 3) All communications providers to retain data. 4) Selected communications providers to retain data.

Option 4 was preferred. This gives the law enforcement community the full benefit of retained data, subject to existing strict access provisions, whilst minimising the number of communications companies that need to implement this Directive and reducing the cost to the taxpayer. This option also minimises the possibility of any EU infractions proceedings.

When will the policy be reviewed to establish the actual costs and benefits and the achievement of the desired effects? The review of the EU data retention Directive will take place in September 2010 and the UK is contributing to that review. The UK will be providing costs and benefits as part of that process.

Ministerial Sign-off For final proposal/implementation stage Impact Assessments:

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) the benefits justify the costs.

Signed by the responsible Minister:

Vernon Coaker

Date: 11th February 2009

Summary: Analysis & Evidence

Policy Option:	Description: Option D "Transpose Directive but minimise duplication" or Option A "Do nothing".

COSTS

ANNUAL COSTS		Description and scale of **key monetised costs** by 'main affected groups' The Home Office will bear all costs relating to the design, development and installation of Data Retention Facilities with communication companies sufficent to implement the directive requirements to capture defined sets of communications data. Resource will continue to be met be public authorities on a per use
One-off (Transition)	**Yrs**	
£ 30.35m	3	
Average Annual Cost (excluding one-off)		
£ 2.21m		**Total Cost** (PV) **£ 46.58m**

Other **key non-monetised costs** by 'main affected groups' n/a

BENEFITS

ANNUAL BENEFITS		Description and scale of **key monetised benefits** by 'main affected groups'
One-off	**Yrs**	
£ n/a		
Average Annual Benefit		
£ n/a		**Total Benefit** (PV) **£ n/a**

Other **key non-monetised benefits** by 'main affected groups' The retention of internet communicatations data enhances the ability to; prevent and detect serious crimes including national security, murder and sexual offences, to provide evidence to prosecute offenders for those crimes and to eliminate suspects from enquiries.

Key Assumptions/Sensitivities/Risks Assumption: That the number of companies that carry communications data remains stable and that the growth in communications related data remains in line with forecasts.

Price Base Year 2008	Time Period Years 8	**Net Benefit Range** (NPV) **£ 0**	**NET BENEFIT** (NPV Best estimate) **£ 0**

What is the geographic coverage of the policy/option?	UK wide
On what date will the policy be implemented?	01 April 2009
Which organisation(s) will enforce the policy?	Home Office
What is the total annual cost of enforcement for these	£ 133,000
Does enforcement comply with Hampton principles?	Yes
Will implementation go beyond minimum EU requirements?	No
What is the value of the proposed offsetting measure per year?	£ 0
What is the value of changes in greenhouse gas emissions?	£ 0
Will the proposal have a significant impact on competition?	No

Annual cost (£-£) per organisation (excluding one-off)	Micro	Small	Medium	Large
Are any of these organisations exempt?	No	No	N/A	N/A

Impact on Admin Burdens Baseline (2005 Prices)				(Increase - Decrease)
Increase of	£ 0	Decrease of	£ 0	**Net Impact**	**£** 0

Key:	**Annual costs and benefits: Constant Prices**		**(Net) Present Value**

Evidence Base (for summary sheets)

[Use this space (with a recommended maximum of 30 pages) to set out the evidence, analysis and detailed narrative from which you have generated your policy options or proposal. Ensure that the information is organised in such a way as to explain clearly the summary information on the preceding pages of this form.]

Rationale

1. 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.

1.1. We refer collectively to this type of data as communications data. The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content. It includes the manner in which, and the method by which, a person or machine communicates with another person or machine.

1.2. For many years communications data has been used by investigators to identify suspects, establish their contacts, and the relationships between conspirators, and place them in a specific location. Communications data is used in numerous other ways, including assisting investigation of suspects' interaction with victims and witnesses and also in support of a suspect's alibi.

1.3. The EU institutions recognised the importance of retaining communications data to be used by law enforcement agencies in their work protecting the public, detecting crimes and prosecuting offenders.

1.4. Last year we consulted on our plans to transpose the final part of the European Data Retention Directive. This final part of the Directive, which relates to internet data, follows the first part of the Directive which required retention of data related to fixed and mobile communications. The UK implemented the required legislation in October 2007 to transpose into UK law the first part of the Directive.

1.5. In our consultation last year, we provided a number of examples of how internet communications data is used in to help law enforcement. The following is one of those examples, from he West Yorkshire Police where internet related data had assisted their officers to identify and arrest a team of armed robbers.

Operation Backfill was an investigation into a series of armed robberies where high value motor cars were advertised for sale for "strictly cash only". The advertisements were posted on a website. When potential customers met up with the persons purporting to sell the cars they were held up at gun point. The police started an investigation which examined the criminals' use of the internet. The investigators acquired internet

related data from the service provider which indicated the use of a laptop and premises from where the suspects had logged onto the internet when posting the advertisements. The suspects were arrested;

1.6. The retention of communications data in the UK has been recognised as a valuable and important measure for a number of years. The UK Government first introduced legislation on communications data retention in 2001. The Anti-Terrorism, Crime and Security Act 2001 (ATCSA) included at Part 11 provisions for a voluntary regime for the retention of communications data by communications companies. This scheme started in 2003 and involved a number of key communications companies being paid to retain their data to be accessed by the police, security and intelligence agencies and additional public authorities under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.7. The maximum retention period under ATCSA was 12 months, whereas the EU Directive allows for retention periods between 6 and 24 months. We are proposing a standardisation of all retention at 12 months. The business case for 12 month retention is based upon our experience of how communications data is used by law enforcement to investigate crimes.

1.8. Prior to 2003, public authorities making use of communications data had to rely solely on the data routinely retained by communications companies for their own purposes. Many public communications providers retain data about communications generated or processed on their network or by the use of their services. They use this data for a variety of business reasons, including invoicing their customers, service development, site management and prevention of fraud but as soon as these business needs have been met, without legislation requiring its retention the providers would delete it. Such deletion would mean that many long running investigations would not able to access the communications data needed. It is important to remember that long running investigations are generally the most serious including murder, serious sexual offences, terrorism and child abuse.

1.9. In the consultation document we outlined the work of the Child Exploitation and Online Protection (CEOP) Centre. CEOP would be key users of retained communications data in their work working to reduce harm and the risk of harm to children. An example in the consultation document (repeated below) demonstrates the links between offences on the internet and abuse.

CEOP received intelligence from the FBI that an individual using internet email had sent a movie file of a woman sexually abusing a 4 month old baby girl. The log-on IP address for this account was found to be registered to a male from Northampton.

Further enquires established a girlfriend of the individual had three children all less than 4 years old. After an investigation both were convicted of the serious sexual abuse of the children. The children had been found in conditions of neglect, described by an officer as utterly filthy, unsanitary and unfit for human residence.

1.10. Without intervention to enable the retention of internet related communications data it is likely that many investigative leads, such as the one provided by the FBI, could not be acted upon.

Policy Objectives

1.11. Our policy intent is to ensure communications data is retained by communications companies for one year for the purpose of enabling the detection and prevention of crime, particularly serious offences such as murder, serious sexual offences, human trafficking and terrorism. We believe the benefits to society from retaining communications data (including internet data) provide significant and compelling reasons for taking action.

1.12. We aim to minimise the impact upon the communications industry and work with them to implement effective solutions.

1.13. We have a commitment to implement this Directive as a Member State of the European Union. Failure to do so is likely to result in infraction proceedings. Any such infraction proceedings would be costly for the UK to fight and are unlikely to be successfully defended.

Options

2. Four options were considered during the consultation and are detailed below;

- Option A - “Continue with ATCSA” (i.e. no change to the status quo)
- Option B - “Do Nothing” (stop data retention activities)
- Option C - “Apply the Directive to all Communication Providers”
- Option D - “As option C but minimise duplication of the retention of the same data sets across different providers”

The costs, benefits and drawbacks are summarised after Option D.

Option A - “Continue with ATCSA”

2.1. This option would see the current data retention programme under ATCSA continuing without completing the Directive. It is likely the UK would face infraction proceedings for failure to implement the Directive, although unlike option B it would support to some degree the policy intent.

2.2. The data sets included within the Directive are largely the same as those included under ATCSA. In other words the Directive will make the UK’s otherwise voluntary scheme mandatory. Some companies are reluctant to be seen to volunteer to retain data, but are happy to do so if compelled by legislation. For this reason continuing with this option will not yield all the benefits of transposing the Directive.

Cost reimbursement

2.3. The existing legislation in the UK places a duty on the Secretary of State to ensure that arrangements are in force to make appropriate contributions towards communications providers who have incurred costs as a consequence of retaining communications data in accordance with the Act (Section 106 of ATCSA) and with regulation 10 of The Data Retention (EC Directive) Regulations 2007. However, given that the majority of other Member States have indicated that they do not intend to reimburse communications providers for additional costs, we considered whether or not the UK should change its position with regard to this. We compared

the effectiveness of our model with others and concluded the current reimbursement presented clear benefits, not least of which is the ability to be selective over the communications companies that retain data.

2.4. In relation to Option A the decision not to reimburse would significantly reduce the number of communications companies volunteering under ATCSA and therefore the benefits of the programme would be reduced.

Option B - “Do Nothing”

2.5. During the consultation, many respondents suggested the “Do Nothing” option should be adopted because of concerns about human rights. Many of these respondents’ concerns focussed on the proportionality of access to communications data by law enforcement, rather than the retention of data by communications companies being considered under this policy. We discuss those human rights considerations more fully below (see annex).

2.6. This option would not address the policy intent. It is also likely the UK would face infraction proceedings for failure to implement the Directive.

Cost reimbursement

2.7. Although a large element of the storage would be avoided under this option there would be some negative cost elements. Under both ATCSA and the European Data Retention Programme, better systems to retrieve data in response to a law enforcement request are being introduced. Without the introduction of those better retrieval systems the cost of retrieval (borne by law enforcement) will rise and it is likely that the time taken to resolve time sensitive enquiries will also rise. This will have a negative impact on the police and other law enforcement agencies ability to respond to crimes such as kidnapping.

Option C - “Apply the Directive to all Communication Providers”

2.8. Under option C the UK is unlikely to face infraction proceedings and the policy intent will be realised. This option would see every communications company retain the relevant data irrespective of whether it had been retained elsewhere. We anticipate that this option would be by far the most expensive and would affect around 100 times more organisations that option D.

Cost reimbursement

2.9. This option would be the fairest to reduce the level of cost reimbursement. However, there might be difficulties introducing such a measure since the early adopters, those who have already implemented systems, would have received reimbursement already and it is likely that there would be criticism from other sectors of the communications industry over unfair treatment. It is also likely that many communications companies would seek to implement the minimum possible, upsetting the more cooperative approach that we have tried to maintain. In such circumstances it is likely that the result would be less than ideal, in that the data might not be easily understood or be made available without undue delay, which is a requirement of the Directive.

Option D - “As option C but minimise duplication”

2.10. The Directive applies to all public communications providers. However, within the Directive, Recital 13 declares that data should be retained in such a way as to avoid being

retained more than once. We discussed this with the Commission in early January 2007 and again in 2008, and the Commission raised no concerns about interpreting this recital to minimise the impact on communication providers. A range of options is available which seeks to capture the data required from different parts of the industry, while minimising duplication.

2.11. In order to avoid duplicative storage of data, we have tried to reduce the number of public communication providers required to retain communications data whilst continuing to aim for full retention of communications data in the UK. Our engagement with industry and law enforcement agencies has confirmed that such an approach is possible. For example where a mobile network provider's services are sold by another provider, that second provider will not be required to retain copies of itemised bills as that same detail will be retained within the scope of the Regulations by the mobile network provider. The European Commission has raised no concerns with this interpretation of Recital 13.

Cost reimbursement

2.12. Reducing or removing reimbursement would make Option D difficult to implement. It is likely that we would face challenges from those who were required to retain data. It is possible that some companies might alter their practices to avoid being required to retain data and this would have a disproportionate effect on the availability of data for law enforcement use. As with Option C those companies already receiving reimbursement would be at an advantage compared to those who would not be reimbursed.

A summary of the costs benefits and drawbacks is included in the table.

	Options	Costs	Benefits/drawbacks
A	**As above but proceed with ATCSA voluntary retention for internet**	£25.65m capital, £12.23m resource over 8 years • This does not include an estimate for the cost of potential infraction proceedings.	• Appropriate data will be available to support the investigation, detection and prosecution of serious crime. • Infraction proceedings will not be avoided.
B	**'Do nothing'** continue with EU DRD fixed and mobile	• £3.5m capital • £7.75m resource over 8 years remain to be spent on EUDRD fixed and Mobile • not including an estimate for the cost of potential infraction proceedings.	• Some data will be available for the investigation, detection and prosecution of serious crime – but the data available will depend on the policy of individual businesses.
C	**All public communications providers must retain data.**	£68.44m capital, £39.40m resource over 8 years	• Appropriate data will be available to support the investigation, detection and prosecution of serious crime. • Infraction proceedings will be avoided.
D	**Duplicative storage of communications data is avoided**	£30.35m capital, £16.23m resource over 8 years EUDRD internet data retention including the cost of continuing with the fixed and mobile project	• Appropriate data will be available to support the investigation, detection and prosecution of serious crime. • Infraction proceedings will be avoided.

Responses to consultation

3.1. Many respondents to the consultation were concerned the measures would not be effective in reducing crime. However, other respondents, including those from law enforcement bodies suggested otherwise. Human rights group Liberty stated;

> *"The consultation gives a range of examples demonstrating the importance of communications data retention. We agree that communications data records can prove a valuable crime detection and prevention tool."*

The full response from Liberty is available on the their website at http://www.liberty-human-rights.org.uk/pdfs/policy08/comms-data-directive.pdf

3.2. Some concerns were raised that the retained data might not be stored secure and for that reason the "Do nothing" option should be chosen. We have maintained security of retained data as a high priority under ATCSA and the first part of the Directive, and this would continue through the final transposition. We intend to use an independent regulated audit firm to ensure data retention solutions proposed by the communications companies are proportionate. In addition the Information Commissioner Office will be the supervisory authority for data protection purposes.

Summary and conclusions

4 Our policy intentions are to ensure communications data is available for one year within communications companies for the prevention, investigation and prosecution of crime and protection of national security. The implementation is important to mitigate the risks associated with a decline in communications data over longer running investigations. We are also required to implement this Directive as a Member State of the European Union.

4.1 Option D is the preferred solution. Option B was discounted as it represents a retrograde step. If Option B were chosen, in time less data than is currently available could be accessed for law enforcement purposes. This is in direct opposition to our policy aims. Consideration of privacy concerns were foremost in proposing Option B, but as outlined in the Annex the potential for impact on privacy and other human rights has been mitigated and therefore we do not believe those concerns are sufficient to justify selection of option B.

4.2 Option C was discounted because this blanket imposition of requirements would lead to a large amount of duplication of stored data and therefore nugatory investment. It would be more difficult to be sure that data standards (including security standards) were adhered to and the cost of implementation would be significantly higher than any other Option for no additional benefit.

4.3 Option A (continue with ATCSA) does not achieve the full benefit of the policy that we would wish to pursue. Some companies are happy to retain data but only if compelled to do so. Option A does not transpose the Directive and therefore this compulsion would not occur. It is also likely that under this option the UK would attract infraction proceedings. The cost difference between this option and Option D is relatively small, but Option D will provide a significantly greater level of data retention. For these reasons Option A was rejected in favour of Option D.

4.4 By implementing Option D, we aim to avoid duplicative storage of data and therefore minimise the impact on industry and the cost to the public purse whilst at the same time maximising the data available for law enforcement. We have confirmed during the consultation stage that such an approach was viable. The European Commission have raised no concerns with this interpretation of Recital 13. We believe that Option D is best suited to meeting our policy objectives. We aim however to engage fully with the European Commission in their review of the Directive and will be monitoring the implementation of the Directive into the UK in terms of compliance and effectiveness. Results will be fed into the review of the Directive in 2010.

4.5 In the Government's assessment, the cost of imposing these requirements is justified by the benefits to society and our legal commitment to implement the EU Directive. By reimbursing industry for the burden that this would otherwise impose, the Government hopes to mitigate any potential competition and small business impacts and aims to ensure that it is funded in an equitable fashion. We therefore intend to transpose the Directive utilising option D.

4.6 On this basis, we intend to transpose the internet-related aspects of the Directive using Regulations under the European Communities Act of 1972 with Regulations to allow the Government to work cooperatively with the industry to ensure that appropriate;

- retrieval mechanisms are in place;
- allow Government to reimburse public communications providers for additional costs;
- make provisions to avoid duplicative retention of communications data and

require communications data to be retained for a period of 12 months;

Specific Impact Tests: Checklist

Use the table below to demonstrate how broadly you have considered the potential impacts of your policy options.

Ensure that the results of any tests that impact on the cost-benefit analysis are contained within the main evidence base; other results may be annexed.

Type of testing undertaken	*Results in Evidence Base?*	*Results annexed?*
Competition Assessment	Yes	Yes
Small Firms Impact Test	Yes	Yes
Legal Aid	No	No
Sustainable Development	No	No
Carbon Assessment	No	No
Other Environment	No	No
Health Impact Assessment	No	No
Race Equality	Yes	No
Disability Equality	Yes	No
Gender Equality	Yes	No
Human Rights	Yes	Yes
Rural Proofing	No	No

Annexes

Annex A: Effect on Industry

A1. The proposed Regulations are designed to ensure that no public communications provider is either advantaged or disadvantaged by the requirements to retain communications data or the provisions for reimbursement of additional costs. Particular attention has been given to ensuring that the Secretary of State is able fully to audit payments made for additional costs, to ensure that competition is not distorted and that there is no contravention of State Aid regulations.

A2. We propose that the reimbursement of costs remains restricted to expenditure that public communications providers have incurred through putting in place additional capability that is uniquely for the purpose of providing for the retention and disclosure of communications data to authorities empowered to access it under the Regulation of Investigatory Powers Act (RIPA) 2000.

A3. The highly competitive market in the UK means that without reimbursing additional costs, those public communications providers receiving high volumes of disclosure requirements from RIPA authorities would be disadvantaged relative to other public communications providers in the UK.

A4. Rather than reimbursing additional costs for retention and disclosure, or expecting industry to bear full costs of the proposals, we have also given thought to the option of requiring industry to bear the costs of retention but reimbursing additional costs for suitable retrieval solutions for those public communications providers who receive the highest volumes of requests. The work conducted under ATCSA and the Data Retention (EC Directive) Regulations 2007 suggests that retention and retrieval mechanisms are so intertwined that it would be difficult to introduce such measures without potentially introducing an advantage to public communications providers who receive the highest volumes of requests. This is because there is a risk that those providers who received funding for a suitable retrieval solution may unintentionally be subsidised for retention costs because it is difficult to separate this out from a retrieval solution.

A5. To avoid the potential distortion of the UK market and to smooth the transition from our legislation under ATCSA (where it relates to the retention of internet-related data) to the draft Regulations that implement the final phase of the Directive, we propose that we continue reimbursing additional costs for both the retention and disclosure of all communications data.

A6. The costs covered by the Directive (and those covered under RIPA) will be subject to audit by an independent regulated audit firm. The cost of preparation for

this audit procedure is itself included in the cost recovery regime. The companies who implement data retention solutions may have valuable equipment provided to them. Through the 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.

A7. We will transpose the Directive in a way that minimises the amount of additional information that is stored, but, do so in a way that does not remove requirements from one company simply to transfer them to another. Similarly, it is important to ensure, through the audit regime, that there is no element of opportunity for a business benefit in those companies who are reimbursed.

A8 Prior to the issuing of a notice the Home Office will enter into discussions with the communications company to determine;

- whether there is a need for the communications company to do anything at all – in many instances the current retention policy of the company will be sufficient to meet the needs of the Directive, in other cases the data will be already be held by a different communications company and again there will be no need create an additional store of data.
- What the best method of storing the data will be. This will vary depending on the circumstances of each company; however key considerations in each case will be data security and availability of data for law enforcement.
- The timing of when the company is compliant with the Directive. This will involve balancing the needs of law enforcement with the ability of the company to delivery the solution.

Annex B: Effect on Competition

B1 We believe the measures outlined above will minimise the impact on industry; however it is also necessary separately to consider possible effects on competition. We have considered whether there is any likely impact on the number or range of suppliers. We have spoken to the communications industry and we have found it is unlikely compliance with the Directive will either directly or indirectly limit the number or range of suppliers. In particular we found no support for a view suggesting this Directive, as we intend to implement it in the UK, would pose barriers to entry into the communications market.

B2 Consideration has been given to the ability of suppliers to compete and also to the incentives to compete vigorously. The measures do not impede the ability of suppliers to generate new business or restrict the manner in which firms conduct their business.

Annex C: Small Firms Test

C1. The EU Directive does not distinguish between sizes of communications provider required to retain data. However the measures outlined above will minimise the effect on small firms. Through reimbursing public communications providers for additional costs in complying with the proposed Regulations and by interpreting Recital 13 to minimise the number of public communications providers who must retain communications data, we believe that we will avoid a disproportionate impact on small firms.

C2. During the last 5 years of voluntary retention under ATCSA and in the initial EU data retention under the completed part of the Directive we have worked with different companies, including small firms and have incorporated a number of particular requirements into our ways of working. These particular requirements might include paying in advance of delivery or working with two or more companies to build a joint solution. We have worked with some smaller companies that have chosen to outsource their data retention to minimise that company's involvement. We will continue to seek to work with the communications industry to implement data retention in a way that reduces the impact.

C3. We have contacted a number of small firms involved in the supply of communications to discuss what this Directive would mean for them. From those discussions we have concluded there would be no greater (or disproportionate) impact on the small firms.

C4 The Data Retention Directive only applies to data that is already generated or processed by way of a business process with the aim of having that data stored. For a small firm this is limited to increasing the capacity of storage for data that is already kept, but only where the data is not already held by another company. Often a small company resells access obtained from a larger company's communications network or facility and that larger company will keep all the data details of communications made. In this scenario the small company would just need to keep account details, which are generally those details which are ordinarily retained for normal business purposes in any case.

Annex D: Human Rights Considerations

D1. The Directive provides flexibility with regard to the period for which communications data must be retained. Under our existing legislation (ATCSA), a retention period of 12 months was adopted. The 2003 consultation paper on the Code of Practice for Voluntary Retention of Communications Data considered three factors in assessing the proportionality of the retention period:

- degree of intrusion involved into an individual's private life
- strength of public policy justification
- the adequacy of the safeguards in place to prevent abuse

D2 The 2003 consultation paper concluded that 12 months is the optimal trade-off between law enforcement requirements and the associated interference with individuals' right to privacy. We do not believe that the period of time for which data must be retained is a significant driver of financial costs. We do not believe that the proposed regulations alter the balance of these factors compared to the 2003 analysis.

D3. A key aspect of debate, both during the public consultation on, and Parliamentary debate about, the Code of Practice for Voluntary Retention of Communications Data, and also during the debate about the Directive within the European Council and the European Parliament, has been the impact, or potential impact, that retention of communications data has on individuals' human rights. The retention period has been considered as a significant factor in determining proportionality; however we do not propose to alter the retention period of 12 months.

D4 Some commentators have suggested that data retention will lead to greater acquisition of communications data by the police, law enforcement agencies the security and intelligence agencies. It is important to state that access to communications data is governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and no changes to the safeguards set out in that Act are planned.

D5. RIPA stipulates that access to communications data must be necessary to achieve one of the purposes set out in the Act. RIPA also sets out in law the requirement for a "designated person" within each public authority to consider the proportionality of the access to communications data in relation to the right to respect for the privacy of individuals.

D6. More detailed guidance is provided by the Acquisition and Disclosure of Communications Data statutory code of practice. The designated person is obliged to balance the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by a relevant public authority. Further, the code of practice outlines how the "actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation" should also be considered as part of the proportionality test.

D7. Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation, or is in any way arbitrary will not be proportionate. The impact of these measures on human rights has already been

considered (RIPA in 2000, and the Code of Practice in 2007). We do not propose to alter the statutory mechanisms through which data is accessed.

D8. Under RIPA, the Interception of Communications Commissioner, currently Sir Paul Kennedy, has oversight of the process of access to (Acquisition) communications data. His office conduct regular inspection visits of public authorities who obtain communications data. There is a process to record any errors that occur and these are outlined in a published annual report. We do not propose to change the oversight mechanisms. The Investigatory Powers Tribunal exists for anyone to bring a complaint. We do not propose to change this.

D9. We consider that the safeguards set out in RIPA provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy. The implementation of this Directive does not alter the balance in that debate.

Annex E: Enforcement, sanctions and monitoring

E1. Under RIPA the monitoring of access to communications data is conducted by the Interception of Communications Commissioner. This will continue. The proposed regulations make provisions for any audit that may be reasonably required to monitor a claim for reimbursement.

E2 The Directive makes no provisions for imposing sanctions on those public communications providers who do not comply with the requirements. However, by adopting a cooperative approach whereby additional costs are paid to ensure that no public communications provider is disadvantaged, we believe that our measures will be sufficiently enforced. This assumption is supported by our experience of working cooperatively with industry under ATCSA and the Data Retention (EC Directive) Regulations 2007.

E3. As part of our monitoring mechanisms to inform the annual reports to the Commission on the effectiveness of the implementation, we will seek to identify cases where requests for data could not be met. This data will inform the plans for reviewing the implementation of the Directive. If the statistics provide sufficient indication of non-compliance, we will review the need to introduce primary legislation to allow for the introduction of sanctions.

Annex F: Implementation and delivery plan

F1 We need to have appropriate legislation in place to take account of internet-related data by 15 March 2009. The draft Regulations will replace the Data Retention (EC Directive) Regulations 2007 and will incorporate the requirement for the

retention of communications data in relation to fixed line telephony, mobile telephony, internet access, internet email and internet telephony.

F2. The Home Office plans an incremental approach building on the current retention within communications companies involved with ATCSA and progressively working to cover the data required by the Directive. The implementation will be guided by an "Implementation Group" to be made up of a representatives of law enforcement, police, Government and the communications industry.

F3. During the implementation of this Directive opportunities will be taken, where appropriate, to maximise efficiencies within the existing processes. This will include automating workflow processes for companies that deal with large volumes of RIPA notices, in this way reducing the administrative overhead within those companies.

F4. The proposed Regulations will apply throughout the United Kingdom.

Annex G: Post-implementation review

G1. Included in the Directive is a requirement to report annually to the Commission on the cases in which information was provided to the competent authorities in accordance with applicable national law, viz

- the number of occasions when data retained in accordance with these Regulations has been disclosed in response to a request;
- the time elapsed between the date on which the data were retained and the date on which transmission of the data were requested; and
- the number of occasions when a request for lawfully disclosable data retained in accordance with these Regulations could not be met.

G2. The arrangements that we propose to put in place with industry will include the provision of statistics. Additionally, we will continue to record - on an exception basis - evidence from law enforcement and intelligence agencies to demonstrate both difficulties and benefits arising from these regulations.

Annex H: Diversity Impact

H1. The impact of the chosen option on a broad range of Diversity issues has been considered. As the measure does not affect end users in the way that they currently use their communications services, there is no diversity impact.

Annex I: Consultation

I1 The proposed regulations have been drafted in accordance with option D and have been subject to public consultation. The consultation ran for three months up until 31 October 2008. The consultation is available to view on the Home Office website at www.homeoffice.gov.uk/documents/cons-2008-transposition . The Government response to the consultation is being published to accompany this revised impact assessment.

I2. A total of 54 responses were received to the consultation, from which we learnt;

- Public communications providers were in general positive about the draft Regulations.

- Many responses were received from members of the public (24 out of 54). These were typically opposed to either the EU Directive or to data retention itself rather than the Government's approach to implementing the Directive. Many respondents had confused issues of access to communications data by public authorities with the retention of communications data these Regulations seek to provide for. Access to communications is controlled by RIPA and many of the points raised in relation to human rights are already provided for within RIPA and the related code of practice for Acquisition of Communications Data. Those human rights considerations implemented under RIPA have been restated in this document for completeness.

- Some respondents from industry wanted greater clarity over who the regulations applied to. In response the Government has proposed new wording in the Regulations.

- Industry gave detailed and reasoned support to continue the current cost recovery regime. Some respondents suggested that taxpayers' money should not be used for this purpose, linking this to privacy concerns rather than the Government's implementation plans.

- Many respondents agreed that the provisions in the draft Regulations will enable Government to manage the impact and ensure that there is no detrimental effect on competition.

- An issue concerning copyright infringement was raised. Companies alleging that their copyrights have been infringed (for example, through illicit music and movie downloads) are able to apply to the courts to grant orders requiring public communications providers to disclose data identifying their customer/s by resolution of the IP address. The Government recognises the concerns raised regarding copyright infringement cases. The Home Office is working with Ministry of Justice and the Interception of Communications Commissioner to provide guidance for the courts on how these cases should be handled, and separately the Government intends to provide more effective remedies for rights holders.

Annex B – Transposition Note

Article	Objective	Implementation	Responsibility
1.	Defines the subject matter and scope of the Directive.	No action required	
2.	Definitions	Regulation 2	Secretary of State
3.	Member States will adopt measures to ensure that the data are retained	Regulations 3 and 4	Secretary of State
4.	Retained data will be accessed only by competent national authorities in accordance with national law.	Regulation 7 in conjunction, primarily, with the Regulation of Investigatory Powers Act 2000	Secretary of State The Interception of Communications Commissioner is responsible for keeping under review the exercise of the powers conferred by the Regulation of Investigatory Powers Act 2000 in relation to the acquisition and disclosure of communications data.
5.	Defines categories of data to be retained.	The Schedule to the Regulations	Secretary of State
6.	Data defined in Article 5 shall be retained for not longer than 24 months and not less than six months.	Regulation 5 specifies a retention period of 12 months	Secretary of State
7.	Data shall be protected at the same level as the data on the network.	Regulation 6	Secretary of State The Information Commissioner will monitor the application of the provisions of the Regulations with respect to the security of stored data
8.	Data shall be provided to competent authorities without undue delay.	Regulation 8	Secretary of State
9.	A Public Authority shall monitor application of the Directive.	Regulation 6	Secretary of State The Information Commissioner is the Supervisory Authority designated for the purposes of Article 9 of the Data

			Retention Directive
10.	Specified statistics must be provided to the Commission on a yearly basis.	Regulation 9	Secretary of State
11.	Amendment to 2002/58/EC	Does not require transposition	Secretary of State
12.	Extending the retention period beyond 24 months.	Does not require transposition	Secretary of State
13.	Penalties for inappropriate access to data	Article 13 is not transposed in these Regulations, as its requirements are met by the Data Protection Act 1998	
14.	Commission will submit evaluation of Directive to the European Parliament not later than 15 September 2010.	Does not require transposition	
15.	Provision of a transposition note and the option to postpone aspects of the implementation relating to internet access, internet telephony and internet e-mail.	In 2007, the UK opted to postpone the transposition regarding internet-related data. These Regulations now transpose the Directive in its entirety.	Secretary of State
16.	Entry into force	Does not require transposing	
17.	Addressees	Does not require transposing	