

**Home Office Consultation:
Protecting the Public in a Changing Communications Environment**
- BT response

Executive summary

1. BT is pleased to offer these comments on this consultation document. We have been an active participant in previous consultations and in the debates that have followed their publication. We will continue to work with Government and others to reach a position where the UK's interests in protecting the public and the commercial and legal positions of companies handling Communications Data (CD) can be reconciled.
2. This response provides comments on each of the questions in the consultative document. However, the document has significant gaps in terms of definitions and explanations of what Government intends as next steps. Many of our comments are, therefore, in the form of questions where we believe Government needs to provide further clarity.
3. The value of this work is well understood and we work with Government and law enforcement agencies under existing rules. However, these proposals represent a significant step change for Communication Service Providers (CSPs) from their current data retention activities, either for their own business needs or to comply with the Data Retention Regulations. In particular, the proposals include extending requirements to non-UK data and to third parties, which may or may not be located outside the UK, as well as extending the processing that CSPs would undertake from retention to also piecing together CD.
4. The proposals would outsource data collection, processing and retention to CSPs rather than building a central Government database and could result in significant brand, reputation and customer relationship issues for CSPs.
5. It is also clear from the document that retaining data on the scale proposed would raise significant issues of proportionality, especially in view of the fact that only a fraction of the data might be used. Moreover, finding the pieces of information that might prove to be useful to the relevant authorities from amongst the mountain of data that will be available to them will be no easy task – the proverbial "needle in a haystack" question.
6. Further detail is required on many aspects of the proposals to enable BT to fully identify and evaluate their implications. Should Government decide to continue with its plans (and these may be premature whilst the scope of the Data Retention Directive has yet to be fully established), we look forward to further dialogue with the Home Office and others in order to ensure that a common understanding of what is being proposed can be reached, and a practical and sensible way forward can be developed.

Responses to Questions

Question 1:- *“On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?”*

7. We believe that the availability of appropriate CD has made a demonstrable contribution to the ability of public authorities to pursue activities relating to the protection of the public.

Question 2:- *“Is it right for Government to maintain this capability by responding to the new communications environment?”*

8. The consultation document demonstrates that the environment in which CD exists is changing because of new technologies and the way people use them. To that extent it is perfectly legitimate for Government to be considering how, if at all, it needs to react to that situation. Maintaining an ability to deal with CD in the new environment is logical. So, if the question is whether in terms of principle it is right to maintain a capability then we agree. However, the proposals in the consultation document are, in many instances, extensions of current capability and we are not convinced that a case has been made to do this.

Question 3:- *Do you support the Government’s approach to maintaining our capabilities? Which of the solutions should it adopt?*

Question 4:- *Do you believe that the safeguards outlined are sufficient for communications data in the future?*

9. BT’s responses to these two questions are combined in the following paragraphs. In most cases, these responses take the form of questions about the scope, definitions, processes, etc. that Government has in mind.

10. Scope

Summary - The consultation has not defined data types that would be in scope. It suggests much of this would be third party data (including offshore data) but it is not clear what data types are intended or what processing would be required of CSPs to make it more usable for public authorities. Given the absence of definitions of the additional data types to be retained, any assessment of the size of the task that CSPs could face can only be speculative.

- It is not clear what is covered under the existing Data Retention Regulations in terms of internet access, internet email and internet telephony data. Therefore, it is impossible to know with any degree of certainty what shortfall in the current arrangements it is that Government is hoping to address through these proposals. Does

Government have an estimate of volume of data in scope to be retained and the scale of the databases required to capture, retain and process for disclosure? Using just one current application as an example, the Home Office itself, in its fact sheet, says that 137 billion Instant Messages were sent in the UK in 2007, with an expected 3% growth rate per year. It is difficult to assess the impact of new requirements on individual CSPs without such volume forecasts or estimates.

- The proposals anticipate CSPs capturing so-called third party data which, in the ordinary course of business, a CSP would not generate or generally process. How does Government intend to ensure that the capturing of this data by CSPs does not contravene any existing domestic or local laws, or expose them to liabilities? Does Government intend to limit the scope of third party data capture? For example, will it be limited to the access network only or is the intention to extend it to traffic on backbone networks including foreign traffic incidentally passing through the UK?
- The distinction between CD and content may not be clear when dealing with internet (payload) data. It is likely that there will be significant instances where CSPs would need to process content to extract CD even if that content were subsequently to be discarded. How does Government intend to deal with this issue to ensure precision in what is CD and that the inevitable processing of content by a CSP is lawful?
- It is suggested that CSPs would additionally be required to carry out significant processing of the “raw data” such as data matching and other processing to make it more readily usable by potential recipients. Clarity is needed about exactly what is being proposed as this is a significant step change in itself from anything CSPs are required to do today.
- Many third parties potentially in scope would not be UK companies and it is unlikely that a CSP would have any contractual relationship in respect of the services provided to end users in the UK. How does Government intend to ensure such processing is lawful and to reconcile conflicts of law and policy pertaining to these third parties’ willingness to allow their data to be processed in this way?

11. Privacy and Purpose

Summary - Any new legislation would need to be compatible with the UK’s privacy and human rights obligations. Security of the data, purpose limitations, the legitimacy of techniques necessary to acquire CD on third party services and the use of this data would need to be carefully considered. Any increase in data retained by CSPs will increase their data privacy compliance burden. The current disclosure regimes would need to be reviewed and perhaps overhauled to be fit for purpose if CSPs are to hold a more extensive range of data on behalf of Government.

- There is a delicate balance to be struck between privacy and security and this may be a reason why a Government central database has been ruled out in favour of separate CSP databases. The need to strike this balance is not avoided, however, by outsourcing data collection, processing and retention to CSPs.
- The legality of CSPs doing any of the proposed processing of “raw data” which is referred to under Scope will need to be established.
- CSPs would have no separate interest or legitimate reason for generating or processing CD related to third party data. Is Government anticipating that CSPs would be the data controllers? If so then it would be a huge additional burden for CSPs in, for example, creating and maintaining the necessary security, technology and processes.
- There have been some concerns expressed around the use of DPI techniques, and Government needs to address these as part of this consultation.

In addition;-

- ECHR compliance will need to be established in relation, for example, to Article 8¹ (privacy and confidentiality) and Article 10² (freedom of expression) which protect individuals and companies. How is proportionality and necessity to be established?
- The Data Retention Regulations made under the Data Retention Directive do not make it clear under what circumstances retained data may be disclosed for purposes other than the investigation and prosecution of serious crime.
- There is no clarity on this “purpose limitation” and there is disparity between the Directive, the implementing legislation and UK practices on disclosures under RIPA, PACE and use for civil purposes made under a Court order requiring such disclosure for many and diverse reasons.
- This will further exacerbate unresolved issues under the Directive and, in view of this, does Government intend to restrict use of CD retained under this proposal and, if so, to whom will it be disclosed and for what purpose?
- Does Government consider that the current disclosure regime is fit for the additional purpose of regulating the capture, retention and disclosure of this CD? Or does Government intend to amend existing disclosure legislation?
- If Government were to be the data controller, it would be Government who would have to make the decision as to whom data is disclosed. Government would be answerable to both the public and the regulator(s) for the security and purpose to which this data is put. Where CSPs are the data controllers of the data, it is the CSPs who must consider whether disclosures are lawful. Even if in receipt of a Court

¹ Article 8 right to respect for private and family life, home and correspondence

² Article 10 right includes freedom to receive and impart information and ideas without interference by public authority and regardless of frontiers

Order, PACE Order, Notice or Authorisation requiring them to disclose, CSPs must consider whether or not to appeal the decision, in particular where the relevant data is not held for business purposes.

- In addition, does Government intend for the CD captured and disclosed under these proposals to be available for evidential use in prosecuting offenders?

12. Oversight issues

Summary: Oversight of data processing, retention and disclosure is currently split between different regulators and it may be more efficient and effective to have one regulator with overall oversight.

- There are a number of UK Commissioners with oversight of data processing involving the capture, retention and disclosure of communications data. For example;-
 - the Information Commissioner (ICO) is an independent authority set up to protect personal information (and to promote access to official information). The ICO also has responsibility for ensuring the security of data under the Data Retention Regulations;
 - the Interception of Communications Commissioner has oversight of the interception warrants, acquisition and disclosure of data and where there is a requirement for data to be de-encrypted;
 - the Office of the Surveillance Commissioner provides oversight of Part III RIPA (encryption) in addition to the conduct of covert surveillance and covert human intelligence sources by public authorities.
- This complex structure might be further complicated by these proposals. How does Government intend to properly regulate and give oversight of these proposals when put into practice?
- Considering the debate about shifting the burden on to CSPs as a way of overcoming the political and privacy issues, how does Government intend to ensure that CSPs do not become quasi public authorities directly subject to such legislation as Freedom of Information?

13. Compatibility with EU Legislation

Summary: The human rights and privacy issues arising from such proposals may not align with EU or other UK legislation. The test of proportionality and necessity of purpose would need to be considered and met for such data collection and use.

- Existing legislation would prevent CSPs from capturing data that they do not generate or process in the ordinary course of their businesses as potentially unfair processing and unlawful. How does Government intend to amend legislation to deal with this and so that is compatible and in compliance with existing domestic and European legislation?

- Compatibility with the E-Commerce Directive's Article 15 (prohibition on Member States from imposing a general obligation to monitor), including the implications of exposing CSPs to increased liabilities if monitoring obligations are introduced, will need to be established.

14. Technology

Summary: The scope of the data types and processing envisaged will impact on CSPs. For example, are existing capabilities scalable, where and how would de-encryption take place, and how automatic will retrieval need to be? As technology develops, CSPs would have to ensure the ability to extract data types which could potentially inhibit product development and may involve higher costs to the business.

- Does Government intend to define how the solution is to be designed and implemented? CSPs must not be put in a position where they cannot be transparent about what data they are capturing and on whom. Does Government propose to make public the techniques used to comply with these proposals?
- How are the definitions of what is in scope in terms of CD to be captured and kept up to date to reflect changing technology?
- CSPs will need to know how relevant authorities wish captured data to be presented to them. Would CSPs be required to perform complex searches, relational database processing, etc. and how would this be compatible with the current privacy and disclosure regimes?
- The service protocols employed between an end user and a third party service provider are commonly proprietary to the third party, are not under the control of the CSP and a CSP has no need to understand them in order to deliver communications. This presents fundamental problems for the capture and interpretation of third party communications data by CSPs.

15. Commercial/Costs

Summary: There are likely to be direct and indirect costs to business in retaining and processing this data. Whilst there is no commitment to pay even direct costs, the HO, in line with usual Government practice, has been prepared to pay for data retention and disclosure on a cost recovery basis. The impact on the competitiveness of UK companies and "UK plc" needs to be considered, especially in the current economic environment.

- The application of the value for money test in relation to costs involved in retaining data will be important. All CSPs under an obligation to capture, retain and disclose data should be treated in the same way.
- Will cost recovery extend to the cost of complying with data protection legislation, for example in responding to data subject access requests, where the statutory fee of £10 does not cover the costs of complying within timescales even today?
- Does Government anticipate auditing systems and the ongoing operation of any CSP's systems in relation to cost recovery?

- Has Government considered the possibility of a broader economic impact on the UK economy if the proposals result in discouraging service providers establishing in the UK?
- There is potential for a large increase in the carbon footprint arising from extra equipment, accommodation, etc. required. What carbon footprint is Government prepared to tolerate for the activities associated with the capture, retention and disclosure of this communications data?
- How does Government plan to cover the cost of evolving technology, replacing systems, and keeping them up to date?
- Inherent to the proposals is an increase in the volume of data that CSPs will be required to retain and this will increase CSPs' costs. We will need answers to the questions we raise above under Scope and Technology in order to assess the potential cost impact.
- The likely impact on competition of any proposal needs to be considered, but this will only be possible when Government has provided clarification on a number of key issues, e.g. scope, on whom the obligation falls (including a satisfactory model for establishing or allocating responsibility for retaining data), the nature and standards of the retained data and the cost reimbursement model.

end