RETENTION OF COMMUNICATIONS DATA

TITLE

1. Voluntary retention of communications data by communications service providers for the purposes of national security or the prevention or detection of crime or the prosecution of offenders.

PURPOSE AND INTENDED EFFECT OF THE MEASURE

Issue and objective

2. **Issue**: Communications data is an important investigative tool: it allows investigators for example to establish links between suspected conspirators (itemised bill) or to ascertain the whereabouts of a given person at a given time, thereby confirming or disproving an alibi (cell site analysis). Data is distinct from content: taking the example of a mobile telephone call, data includes the originating/destination telephone line, and the time and place of the call, whereas content is what was said during the conversation.

3. There are currently no provisions for communications service providers to retain communications data for the purposes of the law enforcement, security and intelligence agencies. Under the Telecommunications (Data Protection and Privacy) Regulations 1999, service providers are obliged to erase or anonymise data which is not needed for specific business purposes (e.g. management of billing and traffic, customer enquiries, prevention or detection of fraud and marketing of telecommunications services). The Regulation of Investigatory Powers Act 2000 regulates access to communications data by authorised public authorities, but makes no provisions to ensure that such data is available when public authorities request it.

4. **Objective**: This legislative proposal is intended to ensure that communications service providers have a clear legal basis for retaining communications data for law enforcement purposes, and that public authorities have a clear picture of what data is being retained and for how long.

5. This objective will be achieved by means of a voluntary code of practice which will be admissible in legal proceedings as evidence that the data has been retained for the

purpose of preventing and detecting crime and prosecuting offenders. The Secretary of State will have reserve powers to impose a mandatory code of practice by order if the voluntary arrangements are considered not to be working satisfactorily.

Risk Assessment

6. Changes to the business model are leading to a reduction in the amount of data which is needed for billing purposes (e.g. pre-pay/ subscription/ "always on"). Combined with pressure from the privacy lobby, this is leading to a decrease in data retention overall. The risks associated with data retention fall in four main areas: security, civil liberties, domestic competition and international competition.

Security

7. Communications data have played a vital part in the terrorist investigations relative to the events of 11 September 2001. Future investigations would be seriously hampered by a lack of available data.

Civil Liberties

8. Data relating to specific individuals under investigation will only be available if data relating to the communications of the entire population is retained, since a criminal's data cannot be distinguished from anyone else's at the time of collection/retention. Mass retention has obvious civil liberties ramifications (even though this is data, not content, and retention, not access). A balance must therefore be drawn between security and privacy.

Domestic competition

9. Equally, there are risks to communications providers. Retaining and retrieving data is expensive and may require the development of new systems. Marginal costs will vary according to the retention specification: the longer the period and the broader the definition of data affected, the higher the costs. Smaller or niche-market firms might suffer disproportionately from a blanket requirement. However, there has already been considerable investment in retention capability across the industry: a report produced for the Home Office estimated that £20 million had already been spent in tailor-made systems, developed by the industry for law enforcement purposes.

International Competition

10. Concern has been expressed that the UK's competitiveness in the e-commerce market might suffer. However, we are not the only country to address this issue. In

the EU, France, Germany, Belgium, the Netherlands, Denmark and Italy either have or are on the point of introducing retention policies. Consistency in approach under the Third Pillar has been proposed and further negotiations will follow.

11. For these reasons, the legislative proposal is for a voluntary code of practice which will specify a maximum recommended period for the retention of data. This period is expected to be twelve months (it will not be more); it has not been specified on the face of the bill since the start date of the retention period will vary for different types of data (e.g. point of collection/transfer/cancellation). This level of detail will be worked up in the code of practice.

OPTIONS

12. Three options have been identified:

Option 1: Self-regulation
Option 2: Voluntary code of practice, and individual agreements
Option 3: Mandatory code of practice

ISSUES OF EQUITY AND FAIRNESS

13. None of the identified options would seem likely to discriminate against any particular element of society.

BENEFITS

14. The proposed provisions for the Bill reflect Option 2. This option appears to offer the best compromise between the conflicting risks of security, privacy and competition.

15. Option 2 will provide a framework for negotiation between the two groups of parties affected by the issue of data retention: the security, intelligence and law enforcement agencies and the communications service providers. It will ensure that the needs of law enforcement are addressed, without corralling communications service providers into an arrangement which is disadvantageous for their business interests. It also has the advantage of a high level of flexibility: agreements between the Government and individual service providers can be tailored to the business practices of each service provider.

16. The other two options have clear disadvantages: Option 1 would be unlikely to preserve the necessary data and may result in unequal implementation of the proposals. It would not give a clear role to the law enforcement community in negotiating the code of practice.

17. Option 3 would risk imposing substantial costs on industry which would severely impact business. Its advantages for the law enforcement agencies would be total clarity about what data is retained across the industry; and for communications service providers, less vulnerability to civil liability if they retain data longer than is needed for their own business purposes.

QUANTIFYING AND VALUING THE BENEFITS

18. Security and liberty are notoriously difficult to quantify, although highly valued. Similarly with competition, it is hard to state what the quantitative impact of the proposals will be on companies' competitiveness.

19. In terms of international competition, these provisions are in line with legislation being introduced in other EU countries. UK business should not suffer unduly in comparison to competitors operating abroad as a result of these provisions.

COMPLIANCE COSTS FOR BUSINESS, CHARITIES AND VOLUNTARY ORGANISATIONS

Business sectors affected

20. The legislative proposals affect three key business sectors: public telecommunications operators, international simple voice resale providers, internet service providers, and postal carriers. Given the rapid development of technology in the telecommunications sector, it is expected that other groups will be affected in the longer term as technological innovations are introduced into the communications marketplace.

21. **Public telecommunications operators** (PTOs) are licensed under Sections 7 and 8 of the Telecommunications Act 1984, and their systems designated as public telecommunication systems under Section 9. They include some cable companies and mobile operators. In total they number around 280, although most of the market share is held by less than a dozen operators.

22. **International simple voice resale providers** (ISVRs) are licensed under Section 7 of the Telecommunications Act, and buy bulk international line space from PTOs to resell the calls. 570 were licensed by the Department of Trade and Industry as of November 2001, of which around 60% are currently active in the market.

23. **Internet service providers** (ISPs) are also licensed under Section 7 of the Telecommunications Act. The Internet Service Providers Association lists around 100 members, although not all of these are ISPs; and the London Internet Exchange lists over 80. In total there are now over 300 operating in the UK.

Compliance costs

24. Technically there will be no compliance costs since the proposal is for a voluntary code of practice. However, the Government hopes that retention periods will increase both as a result of industry negotiations during the consultation process and due to the increased protection from civil liability afforded by a statutory code which is admissible in legal proceedings.

25. Retention costs fall into three categories: technical investment, technical running costs and staff costs. If service providers are asked to retain more data for longer periods, they may need to invest in new systems to hold and retrieve the data. These systems will then have associated running costs. Managing the process will also require the time of engineering staff and senior managers who will be diverted from their core business functions. There may be associated recruitment and training costs, together with increased time spent assisting the agencies or in court verifying data produced as evidence.

26. Some of these costs are already incurred by service providers retaining data for their own business purposes, for which substantial retention capabilities may already exist.

27. Estimates vary upwards from £9m per annum across the industry. The costs to internet service providers are anticipated to be greater than those for public telephone operators, and have been estimated to be on average in the region of a few hundred thousands pounds per year for each provider.

28. However, the situation varies greatly from one firm to another according to infrastructure and retention practices. Therefore, the provisions and any

compensation will be dealt with on a case by case basis: there would not be a "one size fits all" arrangement.

Total compliance costs

29. If the number of requests for access to communications data increases as a result of these provisions, this might lead to an increase in public authority spending on accessing communications data (a cost-recovery scheme is currently in operation). Alternatively, the number of requests could be capped by putting an upper spending limit on the budget for communications data requests.

30. The provisions placing a duty on the Secretary of State to put in place arrangements to compensate communications service providers for the costs of adhering to the code of practice or any agreements are consistent with similar provisions in the Regulation of Investigatory Powers Act 2000.

RESULTS OF CONSULTATIONS

31. Full consultation will take place in the context of drawing up the code of practice: the Secretary of State will have a statutory duty to consult with industry before issuing it.

32. Initial meetings with industry representatives about the Government's proposals have already taken place: they met with a cautious welcome. A report on current data retention practices in industry was commissioned before the events of 11 September and has just reported. It gives a good picture of the complexity of the issue. There is also on-going consultation in the form of the Government Industry Forum and the Association of Chief Police Officers' Telecommunications Industry Liaison Group. Further presentations have been planned with law enforcement agencies and communications service providers respectively.

SUMMARY AND RECOMMENDATIONS

33. Option 2 offers the best solution in terms of offering clarity to both service providers and law enforcement about the lawful basis for retaining communications data and its availability, without having the high cost implications of Option 3.

34. Its main benefit lies in its flexibility, and adaptability to the business practices of each communications service provider by means of individual agreements. It can only

work with industry co-operation, which the Government anticipates to be forthcoming, based on experience to date.

ENFORCEMENT, SANCTIONS, MONITORING AND REVIEW

35. A reserve power to introduce a mandatory code of practice under secondary legislation, subject to affirmative resolution, will also be put forward. This power will be subject to a review every two years, and discarded if no longer felt to be necessary.

Contacts:

Michael Gillespie
Organised and International Crime Directorate
Queen Anne's Gate
50 Queen Anne's Gate
London
SW1H 9AT
Michael.Gillespie@homeoffice.gsi.gov.uk