ISPA response to joint Committee on the draft Communications Data Bill

About ISPA

The Internet Services Providers' Association (ISPA) is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and seeks to actively represent and promote the interests of businesses involved in all aspects of the UK Internet industry.

ISPA membership includes small, medium and large Internet service providers (ISPs), cable companies, web design and hosting companies and a variety of other organisations. Our members may be affected by the Communications Data Bill in various ways. ISPA currently has over 215 members, representing more than 95% of the UK Internet access market by volume. ISPA was a founding member of EuroISPA.

We have been involved in the area of communications data for many years, including the development of data retention provisions under both the Anti-Terrorism Crime and Security Act (2001) and the Data Retention (EC Directive) Regulations 2009 and ISPA members have great experience in handling RIPA requests.

Introduction

1. ISPA members accept that law enforcement agencies should have reasonable access to communications data in order to help in the detection and investigation of serious crime and to safeguard national security. However, any communications data regime needs to be workable for the industry and capable of earning user trust, as well as be proportionate and balance the requirements of law enforcement with both the level of intrusion in to users' privacy and the cost and burden placed upon communication service providers (CSPs).

2. We believe that the current regime performs fairly well, in particular the dedicated expertise in the Single Point of Contact System (SPOC), which has provided for an effective means of structuring the relationship between law enforcement authorities (LEAs) and CSPs. The current system also ensures that the costs that CSPs incur when they comply with requests can be reimbursed so that CSPs continued investment in innovation and service development has not, so far, been adversely impacted by data retention requirements. This also acts as a safeguard to ensure that law enforcement to only requests data where the cost can be justified. It is crucial that these elements continue as part of any future communications data regime.

3. As an association representing a variety of CSPs, ISPA has particular experience and knowledge of costs and burdens placed on CSPs. Below we will argue that a great deal of uncertainty surrounds the proposals and the main changes should be viewed as significant extensions to current capabilities. We have grouped our comments according to the themes raised in the Committee's call for evidence.

4. Industry needs clearer and more detailed information on what the proposals will actually mean in practice for different CSPs. They will have a significant impact on how the UK Internet is run and our members need to fully understand how this will affect them. We would urge the Committee to address the points summarised below with Government so that the whole data retention process is clear and proportionate.

Summary of main points

5. We accept that law enforcement should be able to access communications data in a changing communications environment, but this has to balance the requirements of law enforcement, privacy of users and the impact on business. It is not clear if the Draft Bill achieves this.

6. We welcome that cost recovery is included in the Draft Bill as it ensures a more effective system and reflects the fact that our members do not gain from retaining and disclosing communications data.

7. The Draft Bill has the potential to put the UK at a competitive disadvantage and destabilise the market, with the UK seen as a less attractive and more onerous place to do business digitally, affecting both inward investment and services being made available. In challenging economic times we question whether this should be a government priority.

8. In our view the Draft Bill amounts to a significant extension of the current capabilities and should be viewed as such. This is particularly true of the powers to capture and retain third party data and the filtering arrangement.

9. Due in part to the lack of detailed information made available, we are yet to be convinced that the proposals technically possible on the scale envisioned or that foreign CSPs will provide the necessary information to UK law enforcement.

10. The changing definitions of CSP and communications data have the potential to include a wider range of CSPs and data than previously.

11. Far too much discretion is given to the Home Secretary without the necessary Parliamentary oversight to ensure that significant changes proposed are proportionate and necessary. Parliament should be told what data will be retained, for what purposes and make sure that the necessary safeguards are in place to balance the differing interests of law enforcement, users and businesses.

General comments / requirements of law enforcement

12. ISPA members fully understand that the communications landscape is changing and that this warrants a review of the current communications data regime. However, we feel that that the Draft Bill is missing crucial detail, principally because of the number additional requirements that could be introduced by order, notice and regulations. A great deal more work needs to be done to explain what the current proposals will mean in practice. Whilst we understand that concerns about security and confidentiality may limit what can be revealed publicly and what can and cannot be written on the face of the Draft Bill, we feel that the current level of information makes it hard to undertake an adequate, in-depth assessment of the proposals. To help us fully understand the implications of what is being proposed, we would urge the Committee to seek as clear information from the Home Office as possible on what the Draft Bill will mean in practice for all involved.

13. The Home Office argues for law enforcement to be able to 'maintain' access to communications data as technology and ways of communicating evolve. However, it is not clear that the proposals in the Draft Bill merely maintain current capabilities in a changing environment. For example, the obligation to generate data that is not required for business purposes, the requirement to capture and retain data of a third party and the extended definition of CSP represent significant changes. We question whether such extensive additional powers are proportionate and necessary and whether less intrusive alternatives might be more appropriate.

14. On this basis, we believe that the Draft Bill would in fact extend existing capabilities in that it would require CSPs to retain data that they would otherwise not retain for business purposes and capture and retain data about services they do not own or operate. This could create a capability to track relationships and interactions between individuals in multiple contexts and across multiple online environments where they meet.

15. In comparison with other Western countries the proposals are far reaching and beyond current norms. It could set a precedent for similar legislation elsewhere so it is important that the Draft Bill is fully scrutinised and explained as clearly as possible. How the proposals fit with the Government's wider goals of making the UK a digital hub to help boost growth and its support of the Internet freedom agenda is unclear.

Costs

16. It is currently difficult to determine with any accuracy the costs of the proposals to ISPA members but we note that the Home Office's cost estimates and risk assessments are made on the basis of optimistic assumptions. We would encourage the Committee to test these assumptions. There appear to be three key elements:
    1) costs incurred by CSPs;
    2) ability to bring overseas providers into the retention regime; and
    3) the continuing development of communications services.

Costs incurred by CSPs

17. The costs that will be incurred by CSPs could be significant but there is insufficient detail to determine whether the Home Office's assessment of £859 million is correct. ISPA believes, however, that the key costs related to the retention element of the proposals will be due to the Home Office and not CSPs. This is because the final costs will primarily be dependent on the retention notices issued by the Home Office to CSPs, which will specify the technology that CSPs will be required to deploy and the amount of data they are requested to retain.

18. We strongly welcome the Home Office's commitment to maintaining the current system of cost recovery for CSPs. CSPs do not gain from retaining and disclosing communications data. It is for this reason that we hope that the Committee endorses Parliament's support for the cost recovery system and we encourage Committee members to go further and ensure that the cost recovery for CSPs is guaranteed on the face of the Bill. This would provide a long-term guarantee that would bar future Governments from transferring retention costs to CSPs and thereby jeopardising investment of CSPs in network infrastructure and services.

19. The requirement to capture and retain data types which are not required for business purposes or to collect data relating to third party services is likely to impact the way CSPs build and operate their businesses. This is not why ISPs run their networks and is technically very complex. This obligation could force our members to redesign their networks based on the obligation to retain, rather than on commercial interest or economic effectiveness. Furthermore, there is a concern for small and start-up tech companies that they may be brought into the regime at any moment. This could severely impact on innovation, affect current and new business models and divert resources away from business investment and discourage international companies from choosing to base themselves in the UK. The Home Office should be able to offer certainty to CSPs about who and what is in scope and how the process may come about.

20. The estimated costs seem to be based on a number of assumptions. In the interests of transparency, and to enable Parliament and the wider public to understand the whole process, further detail should be provided on how the figure of £859 million was calculated. The accuracy of these estimates is important to an assessment of the overall proportionality of the Draft Bill. Not only must the costs be accurately assessed but industry must be assured that the costs of complying with the eventual obligations can be fully recovered. We therefore query whether contingency plans are in place for a situation where it becomes clear that the money that has been allocated turns out to be insufficient (e.g. because the need to retain third party data exceeds expectations).

Ability to bring overseas' providers into the retention regime

21. Two of the key elements of the new proposals are the extension of retention requirements to providers outside the UK and the ability to require UK CSPs to retain data of third party providers. According to comments made by the Home Office, these two proposals are closely interlinked as the third party data retention requirement would only be used if overseas providers were unwilling to comply with an order to retain data in the first instance. The ability to bring overseas providers into the retention regime will therefore have a significant impact on overall costs as the capturing of the relevant overseas data via UK providers would be the least cost efficient solution.

22. There is a concern over how these requirements will be viewed in other countries and possibly copied. Asserting UK jurisdiction on overseas providers is a significant step and it is not clear that this is a proportionate, necessary or realistic policy step. We do not feel that the Home Office has provided a compelling case for such sweeping powers and it is not clear that less radical alternatives (such as reforming Mutual Legal Assistance Treaties) have been fully explored. We would encourage the Committee to explore this further.

The continuing development of the communications industry

23. At present Government estimates that there is a 35% gap in communications data availability which, if the proposals are introduced, could be reduced to 25%. It is unclear how the baseline (i.e. 100% of data) for this assessment has been derived, how it will develop with new forms of communications and whether it will stay at the currently estimated level. It is not certain whether the data contained in this gap is not already available to LEAs but is not currently requested properly. We further question whether the proposals are justified and represent value for money for only a 10% increase in current capabilities. Developments in the communications industry are difficult to predict and there is little explanation in the consultation document of how the Government has taken account of this in the estimation of costs.

Level of intrusion into users' privacy

24. ISPA members believe that any intrusion into users' privacy should be kept to a minimum and be proportionate and necessary in order to avoid a situation where average users feel inclined to change their online behaviour in response to the proposals. The Draft Bill should be viewed within the wider debate around privacy and use of data online, which is based on a system of trust and a trend towards greater transparency. The level of intrusion is actually not fully explained or understood because a great deal of the detail remains unclear.

25. The filtering capabilities that the Draft Bill includes could present additional risks to privacy. As an additional third party is being included in the disclosure of private data, it could become an additional attack vector for malicious agents looking to obtain information about individuals. There also exists the possibility for legal representations being made by other parties via the courts to access data retained for the purposes of civil cases or as defence material in other cases.

26. Questions of intrusion, proportionality and necessity arise in relation to the retention of and access to data. The scope, definitions and also the presence of appropriate safeguards proposed by the Draft Bill will play an important part in determining the answer to these questions.

Scope & Definitions

27. Whilst the Draft Bill appears to make only a minor change to the definition of 'communications data' it potentially has a substantial impact. The introduction of the new term 'telecommunications operator' and the inclusion of overseas providers effectively makes a significant change compared to the established definitions of 'public communications providers' under the Regulation of Investigatory Powers Act 2000 (RIPA) or 'communications providers' under the Anti-Terrorism Crime and Security Act 2001 (ACTSA).

28. The Draft Bill's term 'telecommunications operator' refers to a person who controls or provides a telecommunications system, or provides a telecommunications service and will thus cover, among other things, social networking providers, webmail and instant messaging.

29. If the definition of communications data is applied to these wider areas, for example, then it becomes clear that these providers will not only be required to retain new types of data (compared to a 'traditional' CSP) but that these data types also have the potential to be far more revealing and intrusive than the data that is currently being retained for law enforcement purposes. For example, the draft Bill defines 'subscriber data' as "information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person." Social networks often ask their users for information about their gender, religion, relationship status etc. which should not only be considered as very personal information but is also information that is currently not retained for law enforcement purposes.

30. A further challenge of definition is determining what within a communication application constitutes communications data and, as such, would need to be retained, as opposed to data that would need to be collected through lawful intercept. Within communications applications such as social networking services or online gaming, the differentials between what would traditionally constitute Internet 'traffic' and 'content' become less distinct. The Committee should consider whether communications data can be reliably extracted from content data in this scenario.

31. In addition to changing definitions, the Draft Bill extends the scope geographically by requiring overseas providers to retain data or by making this data accessible via UK CSPs. The Home Office says that these new retention requirements only cover data relating to UK citizens or people staying within the UK during the time for which the data is requested, yet the requirement provides access to a wider data set than this. The Committee should consider whether such a broad power is necessary and proportionate if the policing need is much narrower.

32. The precise data types as well as the proportionality and feasibility of the proposed extension to the scope of the data retention regime merit further investigation by the Committee. Until this is known, the impact of the proposals cannot be accurately quantified by Parliament or CSPs.

Safeguards and Enforcement

33. Higher levels of intrusion would warrant the introduction of new safeguards and additional oversight mechanisms. As we argued earlier, this should be applied to both the retention of and the access to communications data. As others may focus more on access to data, we will focus on the retention of data.

34. Oversight of data retention should take place on multiple levels. Parliament plays a key role in this and we welcome that the Committee has been given the opportunity to scrutinise the current proposals in the form of a Draft Bill. We are concerned, however, that numerous requirements in addition to those on the face of the Draft Bill could be introduced by orders, notices and secondary legislation, i.e. with limited parliamentary oversight. For example, the data types that CSPs would have to retain would only be specified in notices by the Secretary of State, without further scrutiny. As currently drafted, the current Draft Bill would put a great deal of power into the hands of the Home Secretary and to ensure that the retention of data is proportionate, Parliamentary oversight needs to be robust.

35. It is proposed that oversight would be provided by the Interception of Communications Commissioner's Office (IoCCO) and the Information Commissioner's Office (ICO). The proposals of the Draft Bill lead to a

situation in which CSPs would be required to retain much larger volumes of commercially sensitive data with a corresponding increase in burdens to store and manage it appropriately, including securing and restricting access to it, for law enforcement purposes authorised by the Draft Bill. The Committee must be satisfied that, whatever proposals are passed by parliament the IoCCO and ICO are sufficiently resourced to address these issues. They must also have the necessary powers and access to information they would need to perform their oversight roles effectively. We would also welcome clarification on what proposed role Ofcom will have in the process.

36. The Committee will be aware that the EU Data Retention Directive (EUDRD) is under review, and there is a potential for the period of retention to be reduced. Any reform or changes to the wider communications data landscape should be flexible and allow for developments in Europe to be reflected in the UK.

Technical aspects of the Draft Communications Data Bill

37. The Draft Bill raises serious concerns about technical feasibility which have yet to be explored in detail.

38. Requiring companies to generate data specifically and only for law enforcement purposes or to capture and retain data about third party services sounds simple but they are technically very complex and difficult propositions. We would like to dispel the idea that existing equipment can be easily reconfigured to capture and retain third party data. DPI and such technology can be used by ISPs for legitimate traffic management processes, but it does not follow it could be repurposed to fulfil the requirements set out in the Draft Bill. We are yet to be convinced that current hardware can handle the volume of traffic that moves across service provider networks at this level.

39. There is a further concern that the in-line devices that would be placed into the network are vulnerable to hackers and criminals and prone to cause single points of failure. Since the Draft Bill and the backstop powers rely heavily on such complex technical solutions, we would encourage the Committee to consider whether this approach could be technically feasible or cost effective to implement.

40. The Draft Bill contains powers for law enforcement to use a filtering arrangement to match individual's various communications across different platforms. Again, we feel more information is required to better understand what this will mean in practice and whether more safeguards need to be put in place to safeguard privacy. By extending the value chain and analysing data from multiple sources rather than from the source itself, as the filter is expected to do, the reliability of the data could be compromised and its evidential and intelligence value lost.

41. In terms of the utility of capabilities proposed, ISPA is concerned that they would be evaded not only because users will increasingly turn to encrypting traffic, but also by the prospect that it will become the norm and be built in as standard by third parties, i.e. even where users haven't specifically decided to encrypt. This would impair the ability of CSPs to manage traffic on their networks, as it would all appear as a stream of different encrypted communications streams with no easy way to differentiate the content within those streams. In addition, we are yet to be convinced how third party data could be reliably extracted from encrypted traffic.