Investigatory Powers Bill – ISPA response

About ISPA

1. The Internet Services Providers' Association (ISPA) is the trade association for companies involved in the provision of Internet Services in the UK with around 200 members from across the sector. ISPA represents a diverse set of companies, including those that provide access to the internet, host websites and data of individuals and business and other cloud-based or over the top services.

Introduction

2. We have been involved in the area of communications data for many years, including the passing of the Regulation of Investigatory Powers Act (RIPA), the development of data retention provisions under both the Anti-Terrorism Crime and Security Act (2001) and the Data Retention (EC Directive) Regulations 2009. Most recently we responded to the Joint Committee on the Draft Communications Data Bill and the Data Retention and Investigatory Powers Act. A number of our members are subject to obligations under RIPA and associated legislation. We most recently responded to the Investigatory Powers Review and our response can be found here. We gave oral evidence to the Committee in November and this response builds on this earlier session.

ISPA's approach

3. ISPA has long been supportive of the creation of a new legal framework to underpin investigatory powers. It is widely acknowledged that the existing laws are too complex for legal experts let alone the public or policy-makers to understand, oversight arrangements have not kept pace with the application of law and various courts and tribunal found issues with the current arrangements.

4. We start from the position that a limited set of authorities should have reasonable access to investigatory powers to investigate and prosecute crime and safeguard national security. This has to be in compliance with the law, effective, feasible and minimise the impact on business. The Investigatory Powers Bill provides a crucial opportunity to update a hugely complex array of existing surveillance laws.

ISPA's 5 pre-publication tests for the Investigatory Powers Bill

5. Ahead of publication of the Draft Investigatory Powers Bill we published a checklist of some of the key tests that the Bill needs to pass to ensure an effective outcome. These tests were:
    1. Full, extensive Parliamentary scrutiny and consultation with all stakeholders
    2. Effectiveness on a technical and public policy level
    3. A stable framework that complies with all relevant legal obligations
    4. Adequate balance of powers, oversight and transparency
    5. Full consideration of impact on business

6. Of these 5 tests, three are of particular relevance in the context of the Science and Technology Committee's inquiry:
    1. Full, extensive Parliamentary scrutiny and consultation with all stakeholders
    2. Effectiveness on a technical and public policy level
    3. Full consideration of impact on business

7. The Investigatory Powers Bill is a large and highly complex piece of legislation. The in-depth scrutiny that is required to do justice to such an important proposal can only be achieved if there is a clear understanding of its scope, aims and implications. This requires the provision of a sufficient amount of time to deliberate the proposals and straightforward and detailed explanations of the aims and powers of the Bill. In this context we would like to highlight one of the five principles – clarity and transparency – that was set out by the independent reviewer of terrorism legislation, David Anderson QC, in his report on investigatory powers. We are concerned that the Government has, yet again, set an expedited timetable for the consideration of the Bill and that, in some instances, the Government has been unwilling to provide a sufficient amount of detail to allow in-depth scrutiny of the Bill. However, we strongly support the Committee's inquiry as a welcome attempt to provide Parliament with a better insight into the Bill.

8. It is important to consider that the Bill needs to work on technical as well as a public policy level and that the two are closely interlinked. Public policy aims need to be supported by technical capabilities but equally technical capabilities, e.g. the addition of 'Internet Connection Records', needs to be conducted within a public policy framework that ensures a just and proportionate application both now and in years to come. Again the Committee will play an important role in ensuring that technical considerations are factored into parliament's scrutiny of the Bill. It is not unreasonable to say that a thorough analysis of the technical aspects has been absent in this area in previous parliamentary discussions.

9. The consideration of technical aspects is also relevant to ensuring that the impact of the Bill on businesses is fully considered. Therefore, it will be important to consider direct as well as indirect effects. For example, the Bill will have a direct impact on those providers that will be served with a retention notice or an interception warrant but it may also affect a decision by businesses on whether they should base themselves in the UK, what kind of hardware to use and the procurement of digital security products from UK businesses.

Consideration of technical issues in the Draft Investigatory Powers Bill

10. An assessment of the technical issues in Draft Investigatory Powers Bill needs to take place on two levels:
    1. Technical feasibility, i.e. is it technically possible to implement the provisions of the Bill
    2. Technical application, i.e. how can the provisions of the Bill be used and what results can be achieved

Technical feasibility

11. Broadly speaking, it should be possible to find technical solutions to implement the provisions of the Bill. However, this is subject to time – service providers may need to develop specific solutions and approaches – and budgets – some of these solutions may be highly complex and difficult to implement. In this context it is worth stressing the importance of a cost recovery process for service providers. Cost recovery not only ensures that providers are not commercially disadvantaged but it also acts as an important safeguard by providing a clear link between public expenditure and the exercise of investigatory powers. It is for these reasons that we are concerned that the Bill merely guarantees a partial recovery of costs which could undermine this safeguard and put providers at a commercial disadvantage.

12. It is also worth pointing out that the Bill goes beyond the current legal framework in that that providers will no longer only be required to retain data that is or will be generated for business purposes. Clause 71(8)(b) refers to "collection, generation or otherwise" which suggests that providers may be required to specifically generate data, i.e. it may require providers to change their business operations or make changes to their business model. This in turn may have a particular impact on small and medium-sized companies.

13. Finally, it is important to note that the internet, online services and telecommunications are based on a complex interplay of networks and services. Changes within one part of the infrastructure or value chain may have an impact on other parts which usually encourages businesses to share operational information with each other. Some of our members have expressed concern that provisions in the Bill which limit the ability of providers under notice to share information may have unintended consequences.

14. Overall, ISPA believes that it is likely that it will be technically possible to implement the provisions of the Bill. However, this may be associated with significant costs and it remains for Parliament to determine whether the operational advantages of the data that is being generated justify the public expenditure and interference with the rights of businesses and individuals. There are also doubts whether the impact assessment fully covers all the possible applications of the provisions in the Bill due to the broadly drafted powers (see below).

Technical application

15. It is important to note that a detailed assessment of how the provisions of the Bill will be implemented on a technical level and what can be achieved by using them is not possible at the current stage. Many of the provisions and particularly some of the definitions of the Bill are drafted so broadly that it is unclear how they can be implemented and used. Whilst we are aware that there are limitations as to what can be revealed publicly due to security considerations, we are concerned that some aspects of the Bill are not fully understood and thus not properly scrutinised. While the Government has provided explanations on how it intends to interpret some of the provisions (e.g. in fact sheets and speeches), it is worth stressing

that these explanations are not legally binding and that future governments could change the stated use of a provision without further consultation and scrutiny of the impacts on businesses and consumers. Accordingly, we would welcome a more tightly drafted and more easily digestible Bill. At present, there is real possibility that the powers in the Bill are overly broad and that its impacts on the UK economy are not fully understood.

Service provider definitions

16. The Draft Investigatory Powers Bill makes is difficult to determine what kind of providers could be covered by the various provisions (e.g. communications data retention, interception, equipment interference). We understand that individual providers cannot be named due to security concerns. However, we would welcome a clear explanation of what type of providers and services fall within the various definitions of the act. For example:
    - Clause 1 of the Data Retention and Investigatory Powers Act requires a "public telecommunications operator to retain relevant communications data" while the Draft Investigatory Powers Bill merely uses the term "telecommunications operator". This effectively extends the reach of the Bill to private networks, e.g. private company networks or even the communications services within the House of Commons.
    - The terms "telecommunications service" is extended in the Investigatory Powers Bill to cover the "provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system", i.e. it may cover actions that are not generally regarded as a communication, e.g. the saving of a document in the cloud.

17. Overall, we are concerned about the unclear and potentially wide-ranging definition of providers and services that are covered by the Bill. The Government has stressed publicly that it has drafted the Bill in consultation with a number of operators that are likely to be served a data retention notice but the powers of the Bill could easily be applied to a whole range of other providers and services whose input has not been considered. We would welcome further information as to the type of providers and the services likely to be covered by the Bill.

Communications data definitions

18. The Home Secretary has described communications data as "simply the modern equivalent of an itemised phone bill"[1], an assessment which we regard as mischaracterisation because communications data that relates to modern communications service is far more revealing about an individual's life or behaviour than an itemised phone bill. David Anderson QC came to a similar conclusion in his report, and the Joint Committee on the Draft Communications Data Bill also suggested that "a new hierarchy of data types

[1] https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

needs to be developed". The Investigatory Powers Bill addresses this through the creation of events and entity data which is a welcome step. However, we urge Parliament to undertake a close assessment of whether the distinction is drawn appropriately and whether the access requirements and safeguards are appropriate for the level of intrusiveness.

Internet connections records

19. Internet Connection Records (ICRs) are a new concept that has been introduced by the Government alongside the Draft Investigatory Powers Bill. Whilst we understand the challenge of trying to identify who is accessing a communications service, we have two concerns with ICRs:
    1. ICRs are not currently retained or held by service providers for business purposes, i.e. they are an artificial construct that, depending on how the definitions of the Bill are interpreted, will require services providers to produce large volumes of new data sets.
    2. The Investigatory Powers Bill does not provide a clear definition of ICRs making it difficult to assess what data could fall under the definition and what impact the colleation of this data may have on businesses and consumers. More details on this are provided by Graham Smith of Bird&Bird in his written evidence to the Committee.

20. Overall, this makes an assessment of either the technical or the public policy impact of ICRs very difficult but it is very likely that the retention of ICRs will be technically very difficult and expensive although not impossible.

Communications Data Request Filter

21. Clause 51 provides for a filtering arrangement for communications data. This capability was also proposed in the Draft Communications Data Bill and the Joint Committee that considered the Bill came to the following conclusion:

> *"The Request Filter will speed up complex inquiries and will minimise collateral intrusion. These are important benefits. On the other hand the filter introduces new risks, most obviously the temptation to go on "fishing expeditions". New safeguards should be introduced to minimise these risks. In particular the IoCC should be asked to investigate and report on possible fishing expeditions and to test rigorously the necessity and proportionality of Filter requests"*

22. We largely agree with this assessment. The request filter effectively creates a single distributed database of communications data that is retained in the UK. This database not only allows for simple searches but also complex profiling queries. As such it is a very powerful tool that makes the complex analysis of communications data more easily achievable for public authorities.

23. Accordingly, it will be important to ensure that it the request filter is built in such a way that it provides reliable results but also that the use of the filter is subject to appropriate proportionality tests. This will

need to take into account that the request filter interferes with the rights to privacy of all people whose data is considered as part of a query and not just those people whose data is included in a result. Moreover, there is a need for tight safeguards to ensure that the powerful Communications Data Request Filter is not abused. Compared to the Draft Communications Data Bill, the Draft Investigatory Powers Bill includes a number of improvements, mainly the new Clause 8 offence of knowingly or recklessly obtaining communications data without lawful authority and the creation of a new Investigatory Powers Commissioner. It remains for Parliament to decide whether these improvements are sufficiently strong to address the Joint Committee's concerns and to ensure that the Request Filter is used proportionately.

Encryption

24. Encryption is an essential tool to ensure the security of data and electronic communications. It is widely used by corporations such as banks, is an essential element of the Government's cyber-security strategy and increasingly used by individuals who handle sensitive information or have a general interest in protecting their privacy online. While the Guide to Powers and Safeguards in the Draft Investigatory Powers document states that the "draft Bill will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA" we urge the Committee to investigate this area in more detail. This is for two reasons:
    1. The provisions relating to encryption may be applied to new kinds of services or providers that were not envisioned when the current rules were drafted
    2. End-to-end encryption is nowadays more common than when the current rules were drafted

25. With this in mind more information needs to be provided on how the application of Clause 189 (4)(c) would impact providers and services that are widely used by citizens and corporation in the UK. For example, it is unclear how a service provider that offers its customers an end-to-end encryption communications service and thus does not have any access to the encryption keys would be able to comply with a request for the removal of electronic protection. This in turn may also lead to a situation where providers that are based in the UK are commercially disadvantaged compared to their non-UK competitors that are not subject to the same requirements (either because requirements do not apply to them or because they are unenforceable).

Impact on SME and the UK's position as a leading Digital Economy

26. To conclude, we wish to reiterate the impact the Bill could have on the UK's digital economy. David Anderson QC recommended a new law in this area that is comprehensive and comprehensible. We would argue that the Draft Investigatory Powers Bill is certainly comprehensive but would question whether it is comprehensible. We believe that this is partially a result of the Government's attempt to future-proof the Bill, but we are concerned of the impact of over broad and difficult definitions on industry as a whole and particularly smaller and medium-sized enterprises. Several of our smaller and medium-sized members have already voiced concerns about what would happen if the powers were applied to them and it is likely that

the UK cyber-security and hosting providers may be put at a commercial disadvantage if their customers do not fully understand how UK services may be affected by the Bill.

27. Overall we believe that a more tightly drafted Bill, updated on a regular basis with input from stakeholders and parliamentary approval (e.g. via secondary legislation), could be as effective as the current Bill while providing parliamentarians, citizens and industry with a better idea of the powers and impacts of the Bill. This could further be combined with an appeals process for providers that are served with a retention notice that is independently judged rather than stopping with the Secretary of State.