Contents

1. Summary of key points and recommendations

Full, extensive Parliamentary scrutiny and consultation with all stakeholders

- The Investigatory Powers Bill is a large and highly complex piece of legislation. ISPA is concerned that the Government has set an expedited edited timetable for the consideration of the Draft Bill and has failed to reveal the level of detail that would be required to scrutinise the Bill in depth and properly assess its impact on businesses, customers and citizens both inside and outside of the UK.
- With a more meaningful consultation process that would have involved a wide cross section of the internet community, the Draft Bill could not only have been improved and made easier to understand, but its cost assumptions could also have been put on a robust basis.
- In order to future proof the Draft Investigatory Powers Bill, the Government has built a significant amount of stretch into the Bill – in addition to a more tightly drafted bill, draft of the codes of practices and secondary legislation should be made available at an early stage, ideally, alongside the introduction of the actual Investigatory Powers Bill, to aid Parliament, the public and industry in their scrutiny of the Bill.

Effectiveness on a technical and public policy level

- ISPA has strong concerns that the Bill, as it is currently drafted, does not provide for an effectively tight policy framework and that future governments could change the use of a provision (as stated by the current Government) without further consultation and scrutiny of the impacts on businesses, customers and citizens.
- It will be difficult but possible to implement the provisions of the Bill but this is subject to possibly long time scales and large budgets. 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.
- The interplay between changing definition and existing powers clearly needs to be considered. The Government should explain in more detail what kind of services and providers are likely to covered by the Bill and how they will be affected (particularly in the context of developments such as the Internet of Things). Unless we are provided with further detail on necessity and proportionality, we are also inclined to remove that extension of private networks from the Bill.
- A more detailed and clear explanation of ICRs is necessary before an in depth assessment can be made
- The request filter is a very powerful tool that makes the complex analysis of communications data more easily achievable for public authorities. It remains for Parliament to decide whether these improvements are sufficiently strong to address the concerns raised by the Joint Committee on the Draft Communications Data Bill and to ensure that the Request Filter is used proportionately.
- Provisions on encryption exist in the current law but the Investigatory Powers Bill allows for the application of these powers to new kinds of services and providers that were not envisioned when the current rules were drafted. We urge Parliament to closely and fully investigate the issue of encryption as there is a real risk that current provision undermines businesses that operate in the UK and the position of the UK as the leading digital economy.

A stable framework that complies with all relevant legal obligations

- It is of fundamental importance that the final Investigatory Power Act complies with all relevant UK and international laws or conventions. A failure to ensure this is likely to result in further successful legal challenges and thus in uncertainty for industry. In cases of legal uncertainty, we urge to err on the side of caution and to not include any provisions in the Bill that have the chance to lead to a successful legal challenge.

Adequate balance of powers, oversight and transparency

- ISPA urges Parliament to undertake a close assessment of whether powers and definitions, e.g. those relating to communications data are drafted appropriately and whether the access requirements and safeguards are appropriate for the level of intrusiveness. Parliament needs to ensure that the level of oversight is scaled up according to the intrusiveness of the powers. The default choice should be to maximise oversight where possible to ensure that users' trust can be maintained.
- Parliament needs to be aware the final Investigatory Powers Act will set an international example that may be followed by less democratic states which may have an impact on UK citizens and businesses.

Full consideration of impact on business

- When assessing the impact of the Bill on businesses it is important to look at the direct, as well as indirect effects, to expand this analysis beyond the UK and to consider monetary as well as non-monetary implications. Only a small set of providers have been consulted and indirect effects, particularly with relation to SMEs may not have been included in the Impact Assessment or full considered.
- The final Act Should enshrine full cost recovery for providers – The cost recovery provision ensures that providers are not commercially disadvantaged and acts as an important safeguard as it provides for a clear link between public expenditure and the exercise of investigatory powers

Conclusion

- 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. Such a Bill would, perhaps be less ambitious than the current draft, but it would provide law enforcement and the security services with up-to-date powers, limit the risk of a successful legal challenge and provide parliamentarians, citizens and industry with a better idea of the powers and impacts of the Bill.

2. 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.

3. Introduction

2. ISPA has long been supportive of the creation of a new legal framework to underpin investigatory powers and welcomes that a new draft bill has been put before Parliament for scrutiny. 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 the law and various courts and tribunals have found issues with the current arrangements.

3. 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.

4. 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

    In the remainder of our response we consider whether these five tests have been met.

4. Parliamentary scrutiny and consultation with all stakeholders

5. 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. "Clarity and transparency" was one of the five principles in the David Anderson QC report on investigatory powers and we are concerned that the Government has not only set, yet again, an expedited timetable for the consideration of the Draft Bill, but also has not revealed the level of detail that would be required to scrutinise the Bill in depth.

6. A key recommendation of the Joint Committee on the Draft Communications Data Bill was that further and substantial consultation was needed ahead of new powers being brought forward. Companies that are currently under a data retention notice (or are likely be to be served with one in the new regime) have been more comprehensively consulted than previously but this deeper level of consultation has not extended to the wider Internet industry. The Bill will not only affect companies that are currently under a data retention notice – some powers can be applied to almost any internet company and, in a fast growing market, some companies may be subject to a notice in the near future. With a more meaningful consultation process that would have involved a wide cross section of the internet community, the Draft Bill could not only have been improved and made easier to understand but it's cost assumptions could also have been put on a robust basis.

5. Effectiveness on a technical and public policy level

7. The fact that the Draft Investigatory Powers Bill is a highly technical piece of legislation should not be used as an excuse to delink considerations of public policy and technical viability. This needs to be done in two ways:
    1. Can the public policy goals of the Bill be implemented at a technical or administrative level?
    2. Does the Bill set an effective framework to ensure that its provisions do not go beyond the stated public policy goals?

Public policy considerations

8. We set out below that we believe that the Bill can be implemented at a technical and administrative level. However, we have strong concerns that the Bill, as it is currently drafted, does not provide for an effectively tight policy framework. The Government has provided explanations on how it intends to interpret some of the provisions (e.g. in fact sheets, explanatory notes and speeches by Government Ministers) but these explanations are not legally binding and future governments could change the stated use of a provision without further consultation and scrutiny of the impacts on businesses, customers and citizens.

9. In order to future proof the Draft Investigatory Powers Bill, the Government has built a significant amount of stretch into the Bill, resulting in a piece of legislation that is overly broad and whose impact on businesses, citizens and consumer is not fully understood.

10. We are aware that some detail will be provided in secondary legislation, codes of practices and in notices to service providers. We understand that the exact detail of the notices cannot be revealed but we believe that, in addition to a more tightly drafted bill, draft of the codes of practices and secondary legislation should be made available at early stage, ideally, alongside the introduction of the actual Investigatory Powers Bill, to aid Parliament, the public and industry in their scrutiny of the Bill.

Technical considerations

General 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 will need to develop specific solutions and approaches and the Committee has already heard evidence that the implementation of Internet Connection Records (ICRs) may only be completed in 2018
    - Budgets – The solutions are likely to be highly complex and difficult to implement. The cost estimates that have been provided by the Home Office require further scrutiny and the Committee has already heard that a single provider believes that they will take up the lion's share of the estimated costs.

    When considering the general technical feasibility, it is further worth noting that the technologies that are applied by different providers vary and that different providers thus face different costs. This becomes particularly important if it is decided that smaller providers who have not been consulted so far are included in the data retention regime in the future.

12. Overall, ISPA believes that it will be difficult but 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).

Definition of a service provider

13. The Draft Investigatory Powers Bill significantly changes the definition of services providers that are subject to the Bill. This is important as it:
    - Expands the number and types of companies that are subject to and affected by the Bill
    - Changes how existing (and new) powers can be used and implemented, thus effectively creating powers that previously did not exist in the law.

14. Some areas that we would like to point at specifically are:
    - 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 only applies to a "public 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 definition of a "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.

15. 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. It is not clear if this has been of a suitably detailed level to enable a full and clear assessment. Moreover, the powers of the Bill could easily be applied to a whole range of other providers and services whose input has not been considered, not least given the new extension to 'private' networks.

16. The interplay between changing definition and existing powers clearly needs to be considered the Government should explain in more detail what kind of services and providers are likely to covered by the Bill and how they will be affected.[1] Unless we are provided with further detail on necessity and proportionality, we are also inclined to remove that extension of private networks from the Bill.

Communications Data definition

17. The Home Secretary has described communications data as "simply the modern equivalent of an itemised phone bill"[2]. We regard this assessment as a 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 on investigatory powers and the Joint Committee on the Draft Communications Data Bill also suggested a "new hierarchy of data types 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 would appreciate further information on the Bill's definition that "'data' includes any information which is not data" and urge Parliament to undertake an in-depth assessment of how clearly the definition allow a differentiation between content and communications data

18. Another data type within the Bill is "related communications data" which potentially blurs the lines between intercepted content and communications data. The Bill provides the following definition of related communications data:
    i. "Can be logically extracted from the content of the communication;
    ii. Which does not, once extracted, reveal the meaning of the content of the communication; and

[1] Some areas that should be considered in this context are how the Bill will apply to the Internet of Things and machine-to-machine communications and what the privacy impact of this is.
[2] https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

iii. Can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which describes an event, or the location of any person, event or thing."

There does not seem to be any clear link between part iii of the definition and the specific communication, i.e. the persons, apparatuses, services or systems could be completely unrelated to the specific communication, e.g. if a database of customers was attached to an email, all the customers' email addresses could be treated as communications data rather than content

19. Overall, we urge Parliament to undertake a close assessment of whether the communications data definitions are drafted appropriately and whether the access requirements and safeguards are appropriate for the level of intrusiveness. The more blurred the lines between content and communications data become, the harder it will be to design and maintain technical equipment to meet this challenge.

Retention and generation of data

20. The Bill goes beyond the current legal framework in 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. There have also been suggestion that powers to require the generation of data are similar to third party data retention powers under the Draft Communications Data Bill and we would thus like further information on what exactly is meant by the "generation" of data.

Internet Connections Records

21. An Internet Connection Record is 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 three 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 collection 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 Science and Technology Select Committee.
    3. The large cost involved in being able to capture and store data associated with ICRs may not be fully met by the figures set out in the Impact Assessment.

22. Overall, this makes an assessment of either the technical or the public policy impact of ICRs very challenging but it is very likely that the retention of ICRs will be technically very difficult and expensive

although not impossible. A more detailed and clear explanation of ICRs is necessary before an in-depth assessment can be made.

Request filter

23. 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 this 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"*

24. 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.

25. 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

26. 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

27. 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 may be unenforceable overseas).

6. A stable framework that complies with all relevant legal obligations

28. The Committee will be aware that there have been a number of successful legal cases against the use and application of investigatory powers in the UK and EU. The Committee will further be aware of the debate around whether previous court case, particularly the *Digital Rights Ireland* case that was heard in the Court of Justice of the European Union (CJEU), set minimum principles. It has further been pointed out to the Committee that some of the provisions of the Draft Investigatory Powers Bill that have been described as existing powers have never been subject to Parliamentary scrutiny or a full legal assessment, thus putting a question mark on their legal compliance.

29. ISPA is not in a position to provide a clear assessment on these legal matters. However, we believe that it is it is of fundamental importance that the final Investigatory Power Act complies with all relevant UK as and international laws or conventions. A failure to ensure this is likely to result in further successful legal challenges and thus in uncertainty for industry.

30. If there is uncertainty about the legal compliance of powers in the Bill, especially in light of Court of Appeal referral of the Davis/Watson case to the CJEU[3], we would urge to err on the side of caution and to not include any provisions in the Bill that have the chance to lead to a successful legal challenge.

7. Adequate balance of powers, oversight and transparency

31. The Draft Investigatory Powers Bill is a highly intrusive piece of legislation and in some areas significantly increases the level of intrusion into the privacy of customers and citizens more widely. The Draft Bill also

[3] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/11/Davis-FINAL.pdf

attempts to strengthen the safeguards and oversight arrangements and we welcome a number of the measures, particularly the creation of an Investigatory Powers Commission. We also note that a limited judicial authorisation regime has been included in the Draft Bill, but are aware that concerns have been raised in relation to its limited application (e.g. exclusion of communications data) and the effectiveness of the double lock system. At present we are not in a position to provide a final assessment in this area but urge Parliament to ensure that the level of oversight is scaled up according to the intrusiveness of the powers. The default choice should be to maximise oversight where possible to ensure that users' trust can be maintained.

8. Full consideration of impact on business

32. When assessing the impact of the Bill on businesses it is important to look at the direct as well as indirect effects, to expand this analysis beyond the UK and to consider monetary as well as non-monetary implications.
    - A large and potentially expanding number of providers will be directly affected by the Bill, either because they will be served with a notice or a subject to other powers in the Bill.
    - An unknown number of business will be indirectly affected by the Bill and the clearest example is probably that UK providers of security services, hardware and software, but also UK data centres may find it harder to sell in overseas markets due to security concerns of overseas customers.
    - Overseas, non-UK, providers will also be affected as the Government intends to apply some provisions of the Bill extra-territorially which requires some providers to trade-off their own domestic against the UK law.
    - Both UK and overseas businesses may be impacted by other countries following in the footsteps of the UK by adopting similar (but possibly not democratically controlled) investigatory powers regimes, particularly because the UK plays such a leading role in the global digital economy.

33. As explained previously, only a small subset of the providers that will be impacted have been consulted ahead of the application of the Bill and it is not clear whether the indirect effects have been considered by the Impact Assessment. Moreover, 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.

Costs & Cost recovery

34. The Impact assessment that accompanies the Bill includes an estimated £247m in total and £170.4m in capex costs. This is significantly less than the £859m in the Draft Communications Data Bill. It was made clear during the oral evidence sessions that this figure was arrived at following high level discussions with

service providers, and that the true cost of implementing the obligations for a single large ISP would be in the high tens of millions. This is based on the need to procure new hardware to meet new obligations and the high costs of storing large volumes data that would follow. ISPA then expanded on this adding that for some smaller provider the figure could be in the region of £20-30m subject to the exact network requirements. With one single ISP stating in the oral evidence that it would take up the lion's share of the estimated costs, the robustness of the impact assessment is called into question.

35. The Draft Investigatory Powers Bill includes a system for providers to recover their costs. This cost recovery provision is important for two reasons:
    1. It limits the extent to which providers that need to comply with the relevant provisions are commercial disadvantaged.
    2. It acts as an important safeguard as it provides for a clear link between public expenditure and the exercise of investigatory powers and this provides an effective way for ensuring that powers are used where necessary.

36. At present, the Draft Bill only guarantees that the contribution of the Government to a provider's costs cannot be zero but we believe that, for the two stated reasons, it is important to enshrine full cost recovery on the face of the Bill. The current draft would enable future Government to scale back their contribution to costs and thus not only put providers at a commercial disadvantage but also risk undermining an important safeguard.

9. Conclusion

1. The Draft Investigatory Powers Bill is an extremely complex and wide-ranging piece of legislation and the information that has been provided so far makes it difficult to scrutinise the Bill in-depth. However, it is clear that the Bill will have a significant impact on providers, customers and citizens, both inside and outside of the UK. We are concerned that some of the provisions in the Bill are too wide-ranging and that the impact of these powers, particularly in the context of fast a changing communications and technology environment (e.g. the rollout of the Internet of Things), is not fully understood.

2. Industry fully supports the creation of a new legal framework for investigatory powers. This new Bill needs to be fully compliant with the law, be effective, feasible and minimise the impact on business and customers. 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. Such a Bill would, perhaps be less ambitious than the current draft, but it would provide law enforcement and the security services with up-to-date powers, limit the risk of a successful legal challenge and provide 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.