Briefing paper: Counter Terrorism and Security Bill

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.

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 responded to the independent review into investigatory powers. ISPA was not consulted by the Home Office prior to publication of the Bill.

Introduction

3. ISPA agrees that a limited set of authorities should have reasonable access to communications data to prosecute and investigate serious crimes and safeguard national security.

4. Focusing more closely on the proposals in the Counter Terrorism and Security Bill (CTSB), ISPA does not have an objection in principle with the aim of enabling law enforcement to better resolve IP data. However, we are concerned with the process that the Government has followed to bring about the current and recent reforms to the law.

5. This briefing paper outlines these points in greater detail and makes the following key points:

   - Whilst the communications data proposals of the Bill are limited, we are concerned that Government has again failed to consult extensively with relevant stakeholders and is artificially limiting the time that Parliament has to scrutinise the proposals.

   - After failing to pass the draft Communications Data Bill in 2012, the Government has adopted a piecemeal and expedited way towards reform of the law, thereby curtailing the chances of Parliament to scrutinise proposals effectively and holistically, limiting opportunities to consult affected parties.

   - The open-ended broad definitions included in the Bill, such as terms like "any other technical identifier" and new definitions of service providers, means that our members, the technical and operational experts, are unclear what powers the legislation may permit or prohibit. Government needs to be clear what kind of data will be classed as "other identifiers" and about the full scope of the definitions to ensure that the CTSB proposals can be properly understood and scrutinised.

   - Instead of proposing incremental changes to the law, which in and of themselves may not amount to a more intrusive regime but taken together may do so, Government should commit to no further extension of communications data capabilities until a full and comprehensive review has taken place in the next Parliament.

About the Bill

6. The Data Retention and Investigatory Powers Act (DRIPA) already requires Communications Service Providers (CSP) to retain certain types of communications data if they have been served with a relevant notice from the Home Secretary.

7. Chapter 2, Part 3 of the CTSB Bill extends the definition of communication data retained under DRIPA with the intention to enable law enforcement and other relevant authorities to better match a communication that is of interest to them with an IP address or other identifier.

8. The rationale for this change to the law is that some CSPs are currently unable to provide information that would allow law enforcement to determine whether a particular communication has been sent from or to a particular subscriber, e.g. because IP addresses are shared between multiple subscribers or devices. This is done for technical and operational reasons and CSPs do not have a business purpose for retaining information that allows them to match a communication that is transmitted across their network to a particular subscriber.

9. The Bill does not specifically mandate the logging of IP data and instead requires the logging of relevant internet data that may be used to identify, or assist in identifying, an IP address to a person or device. It is worth pointing out this data will not guarantee that a specific person or even a specific device will be identified. Therefore, it is somewhat misleading that the explanatory notes of the Bill generally refer to the identification of a user when they refer to the provisions of the Bill.

Process

10. The Government failed to pass the Draft Communications Data Bill in 2012. Since then, Government has made two attempts to bring about changes to communications data and interception regime. It has passed DRIPA under emergency procedures and is now proposing to add IP resolution via a fast-tracked legislative process. DRIPA and CTSB contain elements of the Draft Communications Data Bill.

11. Despite a clear recommendation from the Joint Committee on the Draft Communications Data Bill that "before re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups", industry does not feel that it has been adequately consulted on the detail of the proposals.

12. After the failure to pass the Communications Data Bill the plan to bring forward proposals to allow for IP-matching were trailed in the Queen's Speech 2013. This not only implies that the Government would have had sufficient time to consult with industry and other stakeholders, it also calls into question the need for adopting an expedited parliamentary process. This expedited process has ultimately curtailed the time that Parliament has to properly scrutinise the proposals.

13. Whilst the communications data proposals of the Bill are limited we are concerned that Government has again failed to consult extensively with relevant stakeholders and is artificially limiting the time that Parliament has to scrutinise the proposals.

Lack of clarity

14. The new provisions of the Bill have been described as IP matching or resolution. However, the powers that the Bill will provide are not actually specifically limited to IP addresses as they also allow for the retention of "other identifiers". The explanatory notes suggest that these "other identifiers" would be used to "resolve an IP address to an individual" but subsection (3)(b) does not actually specify this direct relationship between an IP address and "other identifiers".

15. Whilst Subsection (3)(c) outlines some limitations, e.g. the identification of websites visited by a user would not be allowed, ISPA is unclear about what kind of data and information would be included under the definition of "other identifiers".

16. According to the explanatory notes, the additional capabilities will possibly require the retention of port numbers and MAC addresses. This is likely to involve the retention of a very large volume of data for something the Home Office itself says is of only limited value, particularly as the legislation prohibits the communications service or website (known as weblogs) a user has accessed from being retained.

17. New definitions of internet access service and internet communications service are inserted without giving clear definitions and without proper parliamentary scrutiny. This has the potential to include any type of internet service and whilst we understand that law enforcement needs proper investigative powers, sufficient time should be given to Parliament to fully analyse and debate the implications of what constitutes an online communication. For instance, would saving a file on to a cloud hosting service constitute a communication?

18. Modern Internet communications mean it is possible to combine data points that are by themselves non-intrusive but taken together with other data can be used to build a more intrusive profile of an individual. Government needs to provide Parliament and industry with a better understanding of what kind of data will be classed as "other identifiers" and the full scope of the definitions to ensure that the CTSB proposals can be properly scrutinised.

A new approach

19. We note that once again powers are being extended with only limited opportunity to scrutinise. Since the passing of RIPA in 1999, we have seen a piecemeal approach to communications data with more and more powers added without a full and complete forward looking review and consultation.

20. In our recent submission to the Independent Review of Investigatory Powers we argued that rather than adding ever more new powers, there was a need to fully review communications data capabilities in light of the Snowden Revelations, the increased use of internet

communications and rulings calling into question the legal framework from Europe as a whole. We expect this review to be a priority for the Home Office in the next Parliament.

21. **Incremental changes to the law can, if assessed together, amount to a substantial change of the law and to an extension of powers over time. The piecemeal approach to regulation that we are seeing limits the chance to scrutinise and properly assess the impact of proposed changes to the law as a whole. Government should commit to no further extension of communications data capabilities until a full and comprehensive review has taken place in the next Parliament.**