DATA RETENTION AND INVESTIGATORY POWERS BILL: INTERCEPTION PROVISIONS PRIVACY IMPACT ASSESSMENT

Executive summary

1. This document sets out the Home Office's assessment of Privacy Impacts associated with the interception provisions in the Data Retention and Investigatory Powers Bill. The document:

- considers the privacy impact of the proposed legislation; and
- assesses whether the capabilities implemented through this proposed legislation will be compliant with the Data Protection Act 1998 (DPA) and Data Protection Principles (DPP).

2. As the new legislation will simply make explicit our current interpretation of Chapter 1, Part 1 of RIPA, we judge that there will be no impact upon privacy beyond that which currently exists.

The case for legislation

Rationale

3. When RIPA was enacted 14 years ago, it was intended to provide a legislative regime fit for the information age. Since then, it has kept pace with changing technology.

4. However, the increasing globalisation of the telecommunications market has brought about new challenges. The days when we all relied on a small number of domestic telecommunications companies to communicate with each other are in the past. Today, we use a wide range of communication methods sourced from a range of global providers to live our everyday lives. And so do those that mean to do us harm.

5. It is now part of everyday life for people in the UK to communicate using services such as social media, instant messaging and web-based e-mail provided by overseas companies. These companies may not have any physical infrastructure in the UK and the services they provide are innovative, diverse and ever expanding.

6. It is not, therefore, surprising that the nature of the national security threat has been affected by technological developments and diversification. In his open evidence to the Intelligence and Security Committee of Parliament in November last year, the Director of GCHQ (Sir Iain Lobban) stated: "*I think [technological change] has helped the terrorists. I think our job is harder, has got harder, is getting harder. If you think about what the internet does for terrorists, it gives them a myriad of ways to communicate covertly. It gives them a platform, to fund-raise, to radicalise, to spread propaganda. It gives them the means to plan, to command and control, to spread lethal ideas, to exhort violence*."

7. The changing nature of global communications means that suspects in national security and serious crime investigations are increasingly making use of communications services provided from overseas. RIPA imposes obligations on any company providing services to the UK to comply with warrants issued by the Secretary of State for the interception of communications. It has become necessary to clarify RIPA in order to put beyond doubt the obligations imposed on services provided from outside the UK. This is essential to the prevention of terrorism and the detection of serious crime.

8. It is important that the UK's ability to investigate terrorism and serious crime is not eroded by the globalisation of telecommunications. It is vital therefore that there is no doubt as to whether RIPA imposes obligations on the range of services that are inevitably used by terrorists and criminals in their attack planning and criminal activities.

9. Part 1, Chapter 1 of RIPA sets out the obligations imposed on service providers to ensure the agencies can intercept the communications of those who would seek to do us harm. The original statute places an obligation on anyone providing a service to customers in the UK, regardless of where the company's infrastructure is based. But the law now needs to be more explicit.

10. In the absence of explicit extraterritoriality, these companies have started to question whether the law, as it currently stands, applies to them. This represents a real risk to the national security of the UK. Whilst these companies have always been bound by RIPA obligations, we want to put the matter beyond doubt.

11. Interception is a vital tool for law enforcement and security and intelligence agencies and they are heavily reliant on it for intelligence gathering purposes. Any reduction in co-operation will have a serious impact on national security and the ability to prevent or detect serious crime. We need to ensure that there is no doubt that the legislation is intended to apply to companies who are based outside the UK, and that it captures the range of services that are inevitably used by terrorists and criminals in their attack planning and criminal activities. Legislation must address this risk as quickly as possible.

12. This legislation is not intended to extend the UK's reach around the world. Rather, it is to confirm that RIPA obligations in relation to interception apply to all companies providing services to people in the UK irrespective of where they are based. Legislation will allow UK intercepting agencies to continue to investigate threats to ensure they can keep the public safe. It will enable law enforcement agencies to continue to intercept the communications of a member of a serious organised crime group arranging the importation of arms or Class A drugs; to identify where the pick-up is going to take place so they can do something about it. It will enable security and intelligence agencies to continue to intercept the communications of a would-be terrorist planning an attack in the UK; to identify who he's talking to, what he's planning to do and when, and to disrupt the plot before it is carried out.

Overview of proposed legislation

13. The objective of this legislation is to put beyond doubt the fact that RIPA obligations in relation to interception apply to all companies providing services to people in the UK, irrespective of where they are based. This will maintain the ability of law enforcement and intelligence agencies to intercept the communications of those who wish to do us harm. It does not seek to extend the UK's reach or increase the powers of law enforcement and intelligence agencies beyond the original intention of RIPA.

Overview of current and planned safeguards

14. Interception is an intrusive power and is, quite rightly, subject to a strict authorisation and oversight regime. Interception may only be undertaken by a small number of law enforcement and intelligence agencies for a range of purposes specified on the face of legislation. An interception warrant can only be issued by the Secretary of State, who must be satisfied that the proposed action is both necessary and proportionate.

15. Independent oversight of the UK's interception arrangements is undertaken by the Interception of Communications Commissioner, who must be or have been a senior judge. The intercepting agencies are also accountable where appropriate to the Intelligence Services Commissioner, the Office of Surveillance Commissioners, and HM Inspectorate of Constabulary.

16. Intelligence activity is overseen by Secretaries of State, independent Commissioners, the cross-party Intelligence and Security Committee of Parliament (ISC) and held to account by the Investigatory Powers Tribunal. We consider that these safeguards provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy.

17. In addition, the Investigatory Powers Tribunal provides an independent forum for redress for those who think their communications have been unlawfully intercepted.

Privacy risks

18. As the proposals simply make explicit the current interpretation of Chapter 1, Part 1 of RIPA, there will be no new privacy risks associated with the interception provisions in this legislation.

Privacy impact statement

19. I have considered the possible privacy implications of proposed legislation on interception. As the proposals simply make explicit the current interpretation of Chapter 1, Part 1 of RIPA, there will be no new privacy risks associated with the interception provisions in this legislation.