

## **Informal Analysis of Impact of RIP Bill as presented to the House of Lords**

### **1. Introduction**

This paper presents views on key outstanding issues on the Regulation of Investigatory Powers (RIP) Bill as presented to the House of Lords. It builds on the informal analysis produced for the Bill when originally introduced into the House of Commons, reproducing comments made in that document where appropriate.

### **2. Overall Assessment**

#### **2.1 Business Impact**

The comments made in the original analysis regarding the impact on business and on the image of the UK as a good place to do business largely remain. In spite of a few significant changes, listed later, there are still areas of uncertainty for business. While the Regulatory Impact Assessment claims that this Bill does no more than place UK business in the same position as businesses in other major G8 countries, this is clearly not the case. As presented this Bill will discourage inward investment, and may even encourage those based in the UK to place their e-commerce investment outside the UK. The Home Office has repeatedly stated that these concerns will be covered in the planned Codes of Practice, and have indicated that they intend to apply the provisions of the Bill selectively. However, Codes of Practice are not legally enforceable (and drafts have yet to be seen), and there is no certainty that future governments will be so selective. Whatever statements this government might make about how they intend to implement this Bill, industry must assess the impact of the Bill on what future governments might impose using the provisions of the Bill as it stands.

EURIM continues to discuss the major issues with appropriate officials with the objective of getting further changes to the Bill accepted.

#### **2.2 Interception (Part I of the Bill)**

EURIM welcomes the change to Clause 12 to introduce the Order under Affirmative Action. It is regretted that no process has been introduced to allow Notices issued to individual service providers to be challenged.

A major issue is the scope of a “public telecommunications service” liable to be required to provide interception capabilities. More and more companies are introducing services to the public that exploit the internet, and replicate many of the services offered by ISPs and content service providers. There is general concern as to whether they are liable for a Notice to incorporate interception capabilities. Informal discussion suggests that only certain types of service (particularly those that enable persons to communicate) are intended to be covered (as appears to be the intent of paragraph (b) under “postal service”). However, the definition of “telecommunication system” in Clause 2 includes provision of “communications”, which is defined in Clause 72 as “(c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation and control of any apparatus”. This would seem to cover every form of service provision including web servers (thing to person), communication between processes and even remote activation of devices. While Clause 2 (3) excludes broadcast for general reception, this does not seem to exclude internet services such as web servers since they do not broadcast, but transfer information on the request of the caller. Words are needed to limit the scope of this definition if that is the intention of the government.

There remain serious concerns at the loose definition of communications data, the lack of any ability to challenge notices to provide such data, and the ease with which the scope of such data can be changed without explicit consultation.

For those considering investment in the UK, there will be unknown technical implementation requirements and costs to be included, which may constrain both the possible technical solutions and the legal framework within which services are provided. These uncertainties will tend to discourage such investment given that investment can easily be made in places where such uncertainty does not exist.

### 2.3 Access to Protected Data (Part III of the Bill)

The changes to Clause 46 (4) on the form of notices and to Clause 70 on excluding Part III from corporate liability are welcomed, as is the intent to seek plaintext from reliable sources. However the other major concerns remain.

In particular, the apparent broad definition of protected data goes far beyond that implied by statements in, for example, the Explanatory Notes. Clause 46 (1) lists the types of encrypted data in the possession of various authorities for which the keys (or plaintext) can be requested. However the definitions of Protected Data and Key in Clause 52 both imply that those authorities can also demand the means - such as passwords - to access systems that contain data. This could counter internal security controls and expose sensitive data unreasonably. Such sweeping powers would undermine the image of the UK as a safer place to do electronic business.

### 2.4 General

There is a general concern that commercial liability is not adequately addressed. It is essential that business can both maintain secrecy when required and honour its obligations of confidentiality to others. As written, the Bill does not create confidence that information and keys provided under due process will be adequately protected, and businesses are not protected from liability should information provided under due process subsequently result in a breach of confidentiality, or otherwise cause commercial damage through no fault of that business. This situation is exacerbated when a business is expressly prevented from informing others that a breach of their confidentiality has occurred. With businesses other than telecomms companies increasingly providing services, the need to demonstrate good practice in maintaining security (for example consistent with BS 7799) will require such action on any suspected breach of security. The Bill must take account of the need for such good corporate governance. While Codes of Practice could address these issues, they have no force in law and may not protect against liability claims.

As businesses hold more commercially sensitive information electronically, and find themselves subject to the provisions of this Bill, it is important that there are simple processes in place to enable the provenance of warrants and other forms of authority issued under this Bill to be established in real time. There are already examples where such forms of authority have been questioned, and forged documents are seen as a vehicle for those seeking to obtain information illegally. This may be a topic to include in the proposed Codes of Practice.

## 3. Analysis of the Bill

This analysis focuses on those aspects of the proposed RIP Bill that could affect the provision of and operation of information and business systems. It does not provide a legal view and does not address wider civil liberties and human rights issues. It is based on the earlier analysis of the Bill, but focuses on the key issues that are considered most urgently to need attention.

Throughout references are to the clauses in the Bill as presented to the House of Lords. Where appropriate and possible, ways in which the wording could be improved are suggested, with rough draft amendments in some cases.

### Regulatory Impact Assessment

These, while not strictly part of the formal Bill, provide interesting insights into how the Home Office sees the intended effects of the Bill.

#### *Part I*

“Issue and Objectives” shows, under Objective, that it is intended that all communications service providers will be affected. This is reinforced by comments in 5 (i), where anyone licensed under section 7 of the Telecommunications Act is considered included. This would appear to include most companies offering electronic services directly to the public, not just ISPs. The assessment assumes that ISPs are a distinct business sector, which is unlikely to remain the case for long. Note that the cost

compliance argument in 5 (ii) seems to imply that most businesses will outsource their ISP provision to third party companies. There is an urgent need to clarify what is meant by a service provider.

Note also that section 7, last paragraph, implies that UK industry would not be placed at a disadvantage as the requirements are equivalent to those required in the countries listed. This is not considered true.

## The Bill

### Part I

There is an urgent need to clarify what is meant by the definitions in Clause 2 (1) of a “public telecommunications service”, which provides a “telecommunications system” that facilitates “communications” which is defined in Clause 72 (1) very broadly to include communication between persons, persons and things, and between things. This set of definitions would seem to include every possible form of communication.

Clause 12 (2) enables the Secretary of State to issue notices to telecommunications service providers (as defined in Clause 2) to include specified interception capabilities in their systems. There appears to be no means of challenging the appropriateness of such a notice. Government officials have indicated that there would always be informal consultation with a service provider before a notice was issued, but we cannot rely on this being the case for all future governments, even if such an intention is written into the Codes of Practice. As written, this could place UK businesses at a severe disadvantage if unreasonable demands were placed on them. Businesses would need clear sight of the likely technical requirements, and costs of such notices before deciding whether to invest in UK based operations. The proposals in Clause 12 (2) don't seem to provide this.

Clause 20 (4) defines communications data very widely - and potentially includes data not directly related to communications at all (see 24 (4) (c)). Clause 21 (4) appears to require the service provider to obtain communications data asked for that the service provider does not normally retain or even collect regardless of the cost. Although Clause 21 (5) does include the test of proportionality, there appears to be no means to challenge any request for information once made other than by judicial review. Note that Clause 21 (2) (h) allows the Secretary of State to create new purposes for the collection of communications data that have nothing to do with law enforcement, or any other listed purpose via an order agreed under negative resolution. A possible form of words to address this last point could be to add to Clause 21 (2) (h) the words:

and laid before both Houses of Parliament. (i.e subject to Affirmative Action)

The test of reasonableness for the ability of the service provider to obtain the data required under Clause 21 (4) has been included as Clause 21 (7).

### Part II

There are privacy issues associated with this part. However, there appear to be no obvious issues with this Part affecting business raised to date.

### Part III

Clause 46 still includes, in subsections (d) and (e) the ability to seek access to information obtained by means other than via a warrant. This concern is reinforced by the inclusion in (2) (b) (ii) of a reason for seeking keys where information is “likely to be of value for purposes connected with the exercise or performance by any public authority of any statutory power or statutory duty”. The reasons listed in Clause 46 (3) seem to be adequate, and we *recommend that (2) (b) (ii) be deleted*. Alternatively, it may be sufficient to revise the process for issuing permissions relating to access to keys or plaintext to require at least, for example, the involvement of a judge (*Note: the preferred level of authority needs to be agreed before a definite proposal can be made*). This could be achieved by revising the relevant sub-clauses of Schedule I.

Clause 46 (1) coupled with Schedule 1 appears to enable permission to issue Clause 46 notices for certain types of protected data to be given by relatively low-ranking authorities with no judicial oversight. Furthermore, subsection 7 of Schedule 1 still appears to allow such permissions to exist

indefinitely where no expiry date is specified. Additional words could be added to Schedule 1 subsection 7:

(3) notwithstanding the requirements of (2), any permission given shall lapse 6 months from when it was granted unless it is explicitly renewed by the same or higher authority as originally issued it.

It is not clear that a valid defence under Clause 49 (3) (a) is that the person served with the Clause 46 notice is not technically competent to, or authorised to, provide the requested key(s) or plaintext (for example, their system was set up such that they did not have the access rights to extract the required information). A new sub-clause should be added along the following lines:

(d) that he was not technically capable of making the disclosure, or did not have the proper authority to do so.

Clause 51, Safeguards, does not oblige those requesting keys to make all reasonable endeavours to keep those keys secret. While Clause 51 (3) could be construed as requiring this, an explicit requirement to do so would create greater confidence. The following wording could be added to Clause 51 (3):

and appropriate technical and organisational measures have been taken against unauthorised or unlawful access to or disclosure of keys, these measures to be verifiable by independent inspection.

Clause 52 - sub-section (a) in the definitions of “key” and “protected data” are still unsatisfactory, and will create great concern in industry. Industry has always accepted that where information has been acquired that is unintelligible, the means to gain access to that information in intelligible form is desirable. Subsection (a) appears to allow authorities to demand passwords and other data associated with access to systems (including, for example, “root” passwords) on which electronic data resides in which they are interested. This has nothing to do with protected data. Indeed, there appears to be a direct conflict in that Clause 46 talks about protected information in the possession of various public bodies, but subsection (a) of these definitions talk about electronic data that “cannot be accessed”. It would seem sufficient for the definitions to include only subsection (b) in each case to meet the needs of Clause 46. An amendment could be raised that would:

In Clause 52 delete (a) from the definition of “key” and delete (a) from the definition of “protected data”.

Schedule 1 subsections 4 and 5 cover protected information acquired without a warrant or without the exercise of statutory powers - when it appears a Clause 46 notice can be served with no judicial permission or authority and little oversight. This creates an environment where there appears to be little real control over such notices. As mentioned earlier, this needs to be tightened up.

Chris Sundt  
Chairman, Electronic Security Working Party.

1 June 2000