

## **EURIM Working Party Minutes**

*Working party: 13-Secure E-Commerce*

*Ref: 00-WP13-Min02*

*Minuted by: Kate Norman*

*Date: 14/03/00*

*Tabled paper: Analysis of Impact of RIP Bill  
by Chris Sundt*

*Circulation: Secure E-Commerce WP;  
Bill Committee; HO officials.*

### **Minutes Of Consultation Meeting on the Regulation of Investigatory Powers Bill held at The Corporation Of London Marketing Suite on 14<sup>th</sup> March 2000**

1. The Chairman welcomed those present, in particular officials from the Home Office and DTI and Oliver Heald MP, who was one of the five EURIM Parliamentary members on the Bill Committee. Introducing the discussion, CS said that the purpose of the meeting was to consider the implications for business of the Regulation of Investigatory Powers Bill. EURIM endorsed the view that law enforcement should be supported in meeting its objectives to maintain an interception capability. Large sections of the Bill did not seem to our members to be contentious, but there were some aspects which we believed to be unsatisfactory from a business viewpoint. There were also some serious data protection issues.
2. CF, a Policy Manager on the Bill Team, outlined progress on the Bill, which had entered Committee Stage that morning. At the first outline session, particular interest had been expressed in Clauses 6 (which bodies could apply for interception warrants), 12 (costs and industry concerns) and 21 (communications data) and in Section 46 Notices.
3. The Bill was then reviewed in detail and comments made as follows:
4. Section 1 made it an offence to intercept via a “private communications system” Clarification was sought on the position of a corporation which was required by its regulator to monitor its staff’s activities. CF said the intention was that this contingency would be covered by the exception provided in Clause 4.2 for “lawful business practice”. There would be a consultation exercise to discover exactly what that was. He also referred to the Halford judgement which went to the Court of Human Rights and established that, because there was no way of authorising interception of private networks “in accordance with the law”, the UK was in breach of the European Convention on Human Rights.. Such interception, he said, had to be authorised. It was pointed out that the exception offered by Clause 4.2 did not make such monitoring lawful but merely stopped it being a criminal offence. If an employee felt wrong had been done, there would be a civil right of redress. It was agreed that, on the surface, the Bill appeared to provide adequate provisions for business in these areas but individual companies would need to check that their procedures were watertight.
5. Section 8, regarding types of warrants, greatly extended the range of organisations upon whom certificates could be served and there was concern that this included ISPs as well as telecommunications companies. CF confirmed that both “targeted” and “certificated” warrants could be issued to any service provider.

6. Section 12 gave substance to the ability of the Secretary of State to specify the interception capabilities to which ISPs would be subject. It was felt that 12(6) as drafted did not adequately express the intention that the process should be openly available and transparent.
7. Under subclause (2), when a notice had been served there was no process (other than judicial review) to appeal or complain on the basis that it was not reasonable. It would be possible for a law enforcement agency to make an open-ended request requiring the re-opening of archives. NH indicated that there had been a brief discussion of this during the Second Reading debate and ISPs were in fact being consulted to establish what was reasonable. It was considered it would be helpful to state this on the face of the bill. New ISPs were coming along all the time and different procedures being introduced. Whatever was agreed at this stage needed to include a mechanism for it to be changed over time and after consultation with those affected. This might require an external body with an obligation to review.
8. It was noted that much of the cost of compliance would come from the type of hardware and software that would have to be used. This could lead to pressure to buy particular expensive kits that were known to perform to the satisfaction of the authorities. Industry believed that the interception capability being called for was technically feasible but this had not yet been tested. It had, therefore, been suggested that the government needed, at this stage, a blank cheque to state the technical steps they would require. A preferable situation would be for this clause not to come into effect until the Secretary of State could satisfy the House that the technical situation was all right, after which the generic structure could be set out. Industry (and this included users) needed a means of vetting notices for technical viability and proportionality.
9. It was noted that many organisations that would be affected by these provisions had not realised this was the case and so had not responded to the consultation exercise leading up to the Bill. This had distorted the perceived reaction of industry and concern was expressed at the number of businesses who had still not seen that this was relevant to them. Those who had understood, were concerned at the onerous nature of the provisions and were already being deterred from providing planned services to electronic commerce.
10. Sections 20 and 21 dealt with access to communications data. There was concern over the definition of "communications data" which seemed to include data which was not directly related to communications. There was an issue on how long an ISP would have to keep communications data as much of it was personal data which the Telecommunications Data Protection Directive said should not be kept. It was confirmed that such retention would be deemed to be lawful retention within the Data Protection Act. The greater problem was that different parts of the Bill had different approaches and different impacts on privacy. Getting at encrypted data was regarded as a greater intrusion of privacy than was intercepting phone calls and it was understood that the ODPR had not received any assurances regarding this.
11. There was no requirement in the Bill for the Secretary of State to meet the cost of compliance and this was of major concern in terms of the UK's ability to attract electronic business. In most other countries, where exceptional costs were incurred in complying with this type of legislation, the government had an obligation to cover those costs. CF clarified that costs could be recovered in relation to communications data but confirmed

that, for the interception requirement, meeting costs was at the Secretary of State's discretion.

12. There was serious concern about liability protection should data disclosed under Part 1 result in a customer or other data subject being damaged if it were leaked.
13. There was a call for the means to enable someone served with a notice to check its validity in real-time. The most common way of gaining unlawful access to data was by pretending to have authority under a Bill such as this. Members had experience of senior people having been taken in by such fraudulent requests. Most people shown warrants had no way of testing their validity. Due diligence would require using a round-the-clock checking service to test the validity of a warrant. Under the old system only a very few organisations and individuals were involved so it was much easier to confirm their authority. The old procedures were no longer adequate. CF said that a code of practice was currently being written.
14. Further uncertainties arose from the fact that some type of data could be construed as either communications data or content and it was particularly important to clarify which category applied to digital signatures. CF was unable to give an immediate response and subsequently clarified that a digital signature would be part of the content of a communication.
15. Section 21 was considered to be too broadly worded, enabling almost any public sector body to get information for any purpose and there was concern that it would permit "fishing trips". A tighter system was needed for approving warrants for communications data. CF indicated that the purposes for which communications data could be acquired were similar to those in the Data Protection Act but the Bill put in some extra constraints. This Bill was concerned with the requirement to give access, whereas the DPA merely set out the procedures to be followed when access was requested.
16. Concern was expressed that the terms of this Bill could lead to difficulties with the United States leading to further trade disputes. Authorities were being given power to eavesdrop on Internet traffic and particular difficulty was envisaged if US operations based in London were intercepted under conditions that would not have been lawful if they were US based, notwithstanding the convention that if you operated in a country you obeyed its laws.
17. Part 2 of the Bill did not contain issues of direct significance to the business community and therefore was not discussed in detail. It was noted, however, that there would be more privacy protection when residential premises were under surveillance than when business premises were targeted.
18. Part 3 of the Bill was a revision of the part previously in the draft Electronic Communications Bill and it was agreed that this version was an improvement, having taken into account many of the previous criticism. The intentions were better but there were still some difficulties with the detailed wording. The crucial issues were in Sections 46 (defining who can ask for a key) and 49 (addressing the offence of not supplying a key).
19. Re Section 46, it was considered essential to be able to check validity as this was what opened up your security. Subclause 2(b)(ii) was thought to be too broad and should be

deleted. When this clause was linked with Section 52 on “protected” data, there were some alarming security implications if that meant that passwords or root keys could be demanded. A process was needed to record the state of all keys required and perhaps the face of the Bill should include a requirement regarding the security of keys in the possession of the authorities. It was understood that GTAC would do the decryption and that all keys would be at Thames House and it was expected that, with interception data, the normal situation would be the provision of plain text. A differentiation between storage type keys and session keys would be valuable.

20. Government had to demonstrate that this measure would be workable in practice. The requirement to provide communications data without the knowledge of the end user did not take account of the increasing trend for end-to-end encryption. It would be very difficult to get plain text in this situation.
  21. Concern was expressed at the lack of an expiry date for a S46 notice. There was too wide a range of people who could give permission. Relatively junior officials seemed able to raise notices of long duration.
  22. Regarding Section 49, the burden of proof issue was still on the table. There was uncertainty whether there was merely a requirement to keep a record of the state of the keys, or a need to keep the actual keys. If the latter were the case, when combined with Section 69, that could force companies into key escrow for their own protection.
  23. The use of private keys within a corporate system could present serious problems and where smart cards containing private keys were seized the owner would be deprived of all the (many) purposes of the card.
  24. Regarding S 52(2) there were issues relating to the definition of “possession”. Being able to use a key did not mean that the individual concerned also had access to the key itself. The use of the term “immediate” could mean access was not practical merely because of the number of people that had to be consulted before a key could be released. It was considered essential that there be a defence if a key did not exist or could not be extracted.
  25. There was a problem about the person on whom a notice could be served.. It had to be someone who was technically competent. Where the notice required secrecy this could be complex, since the only person capable of responding might not be in the company and could be outside the UK.
-