

The Internet Services Providers Association UK

Written Evidence to the All Party Parliamentary Internet Group

ISPA welcomes the opportunity to comment to the All Party Parliamentary Internet Group on issues arising from current legislation on hi-tech crime.

This submission will focus mainly on the Regulation of Investigatory Powers Act, the Anti-terrorism, Crime and Security Act and the Computer Misuse Act.

Regulation of Investigatory Powers Act (RIPA) 2000

RIPA was intended to streamline data disclosure mechanisms by introducing a single, effective procedure with robust safeguards to protect users in line with the Data Protection Act and the Human Rights Act. However, this has not yet been achieved and - two years after the Bill received royal assent the sections of the Act on disclosure have yet to be implemented –

- **Code of practice on data disclosure**

The Home Office has announced its intention to hold a wider debate on how best to balance privacy and public protection, with reference to the proposals postponed in June 2002, to extend the list of public authorities named in Section 22.

It is clearly a matter for the Secretary of State to judge the necessity and proportionality of extending this list. However, we do not share the view that this matter should be resolved before provisions which are already agreed by Parliament, industry and law enforcement alike are implemented.

ISPA recommends that Part 1 Chapter 2, and the associated Code of Practice and cost recovery mechanisms, be implemented as a matter of priority, thus making the authorities named on the face of the Act fully compliant with the applicable data disclosure provisions .

- **Access powers outside RIPA**

Implementing this section would go some way towards streamlining data disclosure mechanisms. However, ISPA believes that additional steps need to be taken before this objective is fully met. In particular, ISPA is concerned that there are no plans to repeal pre-existing powers to order disclosure retained by a number of public authorities. In practice, this will mean that certain authorities will have the ability to circumvent RIPA in terms of accountability, safeguards and costs. Indeed, many of these powers do not have robust codes of practice for disclosure which are comparable with the code proposed under RIPA Part I Chapter II. .

ISPA recognises repealing legislation is a time consuming process. **We would therefore recommend Government introduce a Memorandum of Understanding between these authorities and Government, which commits them to the use of RIPA procedures over any pre-existing powers they may have under other statutes.**

- **Single Point of Contact (SPOC) scheme**

ISPA fully supports the SPOC system which processes data disclosure requests from public authorities to communications service providers and would like to see it extended outside of the ACPO umbrella to include any public authorities added under Section 22 of RIPA. ISPA is concerned that these units are not adequately resourced. It must be a policing priority to ensure that personnel are fully trained and all requests are processed in a timely manner.

- **Additional public authorities**

Explanatory notes accompanying the Section 22 order tabled (and subsequently withdrawn) this summer indicated that additional authorities would only have access to certain data types

Written Evidence to the All Party Parliamentary Internet Group

and for specific types of investigations. We would welcome clarity from the Government in this area and, again, **would recommend that in reviewing which additional authorities would be able to request communications data and for what purposes, the Home Office consult fully with industry on the operational implementation of these provisions and, in particular, give assurances that additional authorities will have a properly designated SPOC.**

Anti-terrorism, Crime and Security (ATCS) Act 2002

The Communications industry has been in dialogue with the Home Office since January 2002 on the proposed voluntary Code of Practice on the retention of communications data. However, this approach has been found to be fundamentally flawed in both legal and practical terms. Our concerns are detailed below:

- **Disparity of purpose between RIPA and ATCS**

The Office of the Information Commissioner (OIC) has highlighted a conflict between the purposes of retaining data under the ATCS Act (i.e. for national security) and the fact that data can be disclosed under section 22 of RIPA for far broader purposes. The Home Office, however, maintains there is no need to amend RIPA to resolve this conflict. Service providers believe that this disparity of purpose must be resolved before the consultation advances further. [I don't think there's an obvious link between this and s.8]

- **Focus of consultation**

CSPs have repeatedly asked law enforcement agencies to show why an extension to retention periods is necessary and justified to protect national security, through the publication of a "business case" detailing what data types they feel were needed and how long they should be retained. The Case was finally published in September 2002 but failed to present a compelling case to support the Home Office's view that it is necessary to extend data retention periods which would satisfy the OIC and the broader public.

Throughout the 11-month period of consultation, discussions have been dominated by the numerous legal concerns surrounding the Code. This has left little time to discuss related technical and cost issues. These issues are significant and should be an integral part of this proportionality and necessity assessment.

ISPA would recommend that the Home Office now begin to focus on issues of technical feasibility and cost implications, which will aid the debate concerning the necessity and proportionality of data retention requests.

- **Going forward**

The ATCS Act contains provisions for the Secretary of State to invoke a reserve power to make the code of practice mandatory, should the voluntary approach not meet the objectives of the Act. While we accept the current approach presents many legal and practical difficulties, **we would recommend the Government first take time to fully assess the impact of data retention. This review should consider whether a less intrusive mechanism might achieve the Government's objectives, as well as issues of technical feasibility and cost.**

Computer Misuse Act

Finally, ISPA would like to make a recommendation concerning the Computer Misuse Act (CMA) and Denial of Service (DoS) attacks in particular.

There has been much debate as to whether the CMA, as it currently stands, criminalises service attacks aimed at electronic networks. This is an issue of fundamental importance to

Written Evidence to the All Party Parliamentary Internet Group

the communications industry and requires immediate clarification. **We would therefore recommend to the Government that the Crown Prosecution Service be encouraged to launch a test case under the CMA as soon as possible and that, if it is found that perpetrators of DoS attacks cannot be prosecuted within the scope of the CMA, that the Act is modified accordingly as a matter of urgency.**

General recommendation

An over-arching recommendation for Government and law enforcement in considering how best to combat crime perpetrated against or by means of communication systems would be to work in partnership with industry as it can provide invaluable expertise on issues of technical feasibility, practicality and cost.