

All Party Internet Group – Public Inquiry into the retention of and access to communications data for law enforcement purposes

The undersigned communication service providers (CSPs) welcome the opportunity to submit written comments to APIG's inquiry in to data retention and disclosure. Due to the restrictions on the length of submissions, we have limited our comments to the most pressing issues arising from RIPA and the ATCS Act.

Regulation of Investigatory Powers Act Part I Chapter II

- ◆ RIPA provides for a framework for the disclosure of communications data to designated public authorities. This aims to streamline current procedures and ensure that disclosures are compatible with EU and UK data protection and human rights legislation. On this basis, RIPA has the full support of CSPs as it aims to bring all public authorities within a single procedure and introduce robust safeguards to protect Internet users. It also provides a framework for CSPs to recover reasonable costs incurred from assisting investigations in this way.
- ◆ However, CSPs are disappointed that the Government has not yet brought in to force the code of practice which will give effect to these disclosure provisions. Implementation has been further delayed while the Home Office considers whether these powers should be extended to more public authorities other than those named in s.22 of the Act.
- ◆ The intended streamlining to a single procedure has not occurred. Indeed, it is not clear that public authorities with pre-existing powers to request data will have these powers repealed and be brought within the RIPA framework, for example the Department of Works, Pensions and Social Security and the Health and Safety Executive. This could allow those authorities to circumvent RIPA in terms of accountability as these powers generally do not have comparable, robust procedures.
- ◆ It is crucial that all public authorities listed in s.22 have appropriately designated single points of contact (SPoCs) to manage requests for the disclosure of communications data and that these units are adequately resourced. The current resourcing levels of SPoCs cause frequent delays in preparing and processing requests and can frustrate public investigations.

Anti-Terrorism Crime and Security Act Part 11

- ◆ Discussions between CSPs and the Home Office on the proposed voluntary code of practice for data retention began in January 2002 and remain on-going. During this time, all parties have struggled with many complex legal and practical issues arising from these provisions.
- ◆ Legal concerns arise from the fact that compliance with the code of practice is *voluntary* and could expose CSPs to the risk of claims from data subjects under EU data protection and human rights legislation. In addition, advice obtained by the Office of the Information Commissioner (OIC) concludes that CSPs could be deemed a “*public authority*” for the purposes of data retention and may, therefore, be open to legal challenge under Articles 6 and 8 of the Human Rights Act (HRA). In particular, CSPs are

not in a position to reach a view on whether the additional retention of data proposed is 'necessary' for the purpose of the various public authorities' functions

- ◆ There is also a disparity of purpose - identified by legal counsel to the OIC - between the ATCS Act and RIPA with respect to the disclosure of retained data. Data retained under the ATCS Act is retained "*for the purpose of safeguarding national security or the prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security*". Retained data may, however, be disclosed to a range of public authorities under the provisions of RIPA Part I Chapter II for purposes other than the protection of national security. The Home Office and the OIC must come to a common view on this matter to enable CSPs to understand and manage their legal obligations.
- ◆ CSPs have examined a number of options to reconcile the framework set out in the Act with existing statutory obligations under data protection and human rights legislation. It is very doubtful that a solution can be found within the *voluntary* framework - a point which was made during the Bill stages - and so a new approach is required.
- ◆ More recently, detailed discussions of the significant practical difficulties arising from data retention have begun recently between CSPs and the Home Office. These include:
 - the extent to which different data types are useful and usable to investigations;
 - the technical feasibility of prospectively retaining data on all users for long periods (as well as searching and disclosing large volumes of data in a timely way); and
 - the capital and operational costs to service providers.

Conclusions

CSPs remain committed to doing all that is reasonably practicable to fight terrorism and protect national security, and assist the prevention and detection of serious crime. However, adequate safeguards are required to protect CSPs and their customers. The Government could resolve this uncertainty by considering the following:

RIPA Part I Chapter II

- ◆ There is no compelling reason why implementation of the Chapter II should be further delayed by linking it to the review of s.22. In fact, heightened public awareness of privacy matters strengthens the case for implementing the code as soon as possible for the authorities on the face of the Act. This can only help satisfy the public that the necessary safeguards are in place and functioning well, before it is determined whether these powers should be extended to other public authorities under s.22.
- ◆ The commitment to streamline data disclosure procedures should be met by bringing those public authorities with pre-existing (and non-HRA compliant) powers within the RIPA framework.
- ◆ Disclosure procedures should be strengthened by mandating the use of SPoCs by all public authorities. It should equally be a policing priority to adequately resource and train SPoC personnel to ensure that disclosure requests are processed in a timely way and that rigorous and consistent standards are established and maintained across all public authorities.

ATCS Act Part 11

- ◆ Service providers believe that the legal concerns are now well understood by the Home Office and remain committed to continuing discussions on an appropriate way forward.
- ◆ The accelerated passage of the Act through Parliament allowed little time to measure the need and impact of data retention (in terms of proportionality, technical feasibility and cost), including whether a less intrusive solution might achieve the stated objectives of the Act. There is a strong case that this broader assessment should take place now, perhaps as part of the RIPA s.22 review announced by the Home Secretary this Summer.
- ◆ The full range of issues which flow from data retention should be identified and assessed as a whole. These include how such national security measures interrelate with CSPs' broader obligations (e.g.: to disclose data under RIPA and safeguard their customers' privacy under privacy statutes).
- ◆ Measures to retain communications data should be informed by EU legislation and developments and seek to converge national retention regimes. This is an important issue given that many CSPs operate internationally.

This submission is made on 3 December 2002 behalf of:

Cable & Wireless

BT

T-Mobile

Telewest

ntl

Nortel Networks

Worldcom

O₂ (UK)

O₂ Online

Colt

Hutchison 3G

Orange

Vodafone

Kingston Communications

Thus

Energis

Your Communications