

Introductory remarks

1. This submission is made on behalf of the JNT Association, trading as UKERNA, to the All Party Internet Group's public inquiry into the retention of and access to communications data for law enforcement purposes.
2. UKERNA operates the JANET network, connecting universities, colleges and research organisations in the UK together, and providing them with access to the public Internet. JANET is one of the largest and fastest private networks in the country, with over a million users and a backbone running at a speed of 10Gbit/s.
3. This submission contains UKERNA's concerns about the matters to be discussed in the inquiry, primarily the data retention provisions of the Anti-Terrorism, Crime and Security Act 2001 (ATCS) and the data access provisions of Part I Chapter II of the Regulation of Investigatory Powers Act 2000 (RIP), and also concerns that have been expressed to us by organisations connected to the JANET network.

Data Retention

4. We are concerned that any data retention provisions should recognise the variety of types of Communications Service Provider. Like other providers of IP backbone networks, UKERNA has no operational requirement to collect communications data. Our network operations are concerned with moving IP packets from place to place, not with the e-mail messages, web browsing or other communications that groups of those packets may represent. In particular we have no access to information about the individuals using our network: that is created and held by the customer organisations that we provide with connectivity. Any mandatory requirement that did not recognise the different types of Communications Service Provider would be difficult, if not impossible, to implement.
5. Our customer organisations are concerned that implementing a mandatory code would place them at risk of breaking one of the overlapping pieces of legislation in this area. Any code on data retention must make clear how it is to be reconciled with the apparently contradictory requirements of the Data Protection and Human Rights Acts. The relationship between the different purposes for which data may be retained under the ATCS Act and disclosed under the RIP Act also needs to be clarified before organisations risk liability under one Act by attempting to comply with the other.
6. Customer organisations are also concerned at the financial cost of complying with a mandatory data retention code. This cost will arise not only from the simple need to store data for longer, but also from managing access to that data. All our customers already have to respond to Subject Access Requests under the Data Protection Act 1998 and most will have to respond, from 2005, to public information requests under the Freedom of Information Act 2000. If retained data is subject, in whole or in part, to requests under those Acts then the cost of handling requests will be significantly increased, especially as retained data is likely to be held in off-line storage. Even if data is exempt from access requests, an organisation that asserts exemption for a large quantity of its data is likely to suffer damage to its reputation.

Data Access

7. UKERNA and its customers have a good working relationship with the police and have provided useful information to them in the past, either anonymised or under the disclosure provisions of the Data Protection Act. While we welcome the clarification of disclosure rules provided by Part I Chapter II of the RIP Act, we have concerns that the extension of this process leaves it vulnerable to abuse and loss of public confidence.
8. Under the present regime, holders of communications data deal with a few dozen police single points of contact (SPOCs). In some cases we already know these SPOCs and their identity and their right to request data can be immediately verified. If there is doubt on either count we can quickly obtain independent confirmation by personal contact with members of staff of the National High Tech Crime Unit. If an extension of data access rights results in either a significant increase in the number of officers entitled to demand data or the loss of a simple independent check then there is a considerable risk that fraudulent demands for data will be made by individuals not involved in law enforcement. We understand that significant numbers of such requests are already made under the existing Data Protection Act provisions.
9. The present police SPOCs are thoroughly trained and are familiar, through frequent and regular contact, with the operation of the Internet and Communication Service Providers. They are therefore well prepared to meet the RIP Act requirements that demands be both proportionate (section 22(5)) and reasonably practical (section 22(7)). They are also familiar with the uses to which data may or may not be put. If there is any increase in the organisations that can demand data we believe that their officers must have equivalent training and expertise. Without this there is a real risk of abuse of the process that will damage both the operations of Communications Service Providers (and possibly expose them to liability) and confidence in the law enforcement process. Effective oversight and punishment of those who abuse the system are essential to maintaining public and jury confidence.
10. Data that has been obtained under these provisions must be held securely, with appropriate technical and procedural protection. The data archive could be useful to criminals and is likely to be a target for attack. Again, public confidence depends as much on the perception of secure storage as on the fact.

Use of Data

11. Finally we note that, outside the major Internet Service Providers, few if any staff of educational organisations, or indeed private companies, that operate communications networks have been trained in collecting computer evidence to forensic standards. If data retained and accessed under these provisions are not to be seriously doubted in court this will require a great deal of individual tuition of network operators by law enforcement officers, and a considerable amount of effort for both parties.

For further information, please contact
Andrew Cormack, Chief Security Advisor,
UKERNA, Atlas Centre, Fermi Avenue, Chilton, DIDCOT, OX11 0QS
E-mail: A.Cormack@ukerna.ac.uk Phone: 01235 822200

29 November 2002