

Hugh Milward
Director
The Internet Society of England
c/o Weber Shandwick | GJW Public Affairs
Fox Court
14 Gray's Inn Road
London WC1X 8WS



The Internet Society of England
www.England.isoc.org

Response from

ISOC England

to the Parliamentary All Party Internet Group's consultation on the retention of and access to communications data for law enforcement purposes

Introduction

1. The Internet Society of England (ISOC England) thanks the All-Party Internet Group for its invitation to comment on its inquiry into data retention and access. Although not directly representing the views of Internet service providers, telecoms companies or companies responsible for data mining, collection or management, ISOC England feels qualified to comment on these proposals since they will affect the individual's attitude towards the Internet and the way in which the Internet develops and will be used in the future. ISOC England represents a cross section of the Internet community, from members working in Internet Standards development in the IETF, in commercial and non-commercial sectors of the Internet to those at the centre of Internet management and Internet public policy internationally.
2. We believe it is essential to get this legislation right if the Internet is to continue to develop at the rapid pace it has set to date. This rapid growth has been a significant contributor to the development of new technologies, business and working practices. We are keen for this pace to continue unhindered by the fear individuals have of scrutiny of their everyday lives and habits. The body of evidence does not support the need for legislation for blanket data retention at this time. Indeed there is evidence that blanket data retention could weaken security and may contribute to further damage to an already weakened commercial and non-commercial Internet sectors in the UK.

ISOC England

3. The Internet Society (ISOC) operates under the banner of 'the Internet is for everyone'. ISOC England's mission is to promote the effective operation and development of the Internet and its related technologies in the public interest through leadership in standards, issues and education. The ISOC England Board's primary focus is to deliver this mission and, in so doing, to develop an active and influential ISOC Chapter with a membership of like minded individuals and organisations who share our vision, and who want to support and/or participate in helping us deliver our mission.

Broad Principles

4. ISOC England is not in favour of broad data retention and disclosure rules. We consider the rules potentially to be a significant invasion of privacy. There will be additional costs to consumers for these rules, the effects of which appear to be unproven and untested. While we do not consider it necessarily to be the benchmark in all Internet-related issues, the US, arguably in greater need, has not seen fit to introduce these types of rules.
5. However, we do understand the need for the security services to protect the UK citizen. If there can be a case made that this type of data retention and disclosure could have a beneficial effect on national security (as opposed to general duties of the police forces and government in fighting crime and collecting taxes), we would support the limited and controlled collection and disclosure of data.
6. The ability to retain data in a targeted and auditable way by law enforcement agencies for the most serious investigations of crimes under the guidance of a security cleared qualified investigative court magistrate or judge should be considered to ensure that investigations qualify the data being retained and mined specific to that investigation.
7. Data retention over and beyond that needed to service customers and user services raises important issues for user security, privacy and contractual relationships as well as costs. Many data producers such as individuals, children on gaming networks, writers' circles and small trades businesses who operate using emerging club based city wireless networks will find that data retention provisions are simply not feasible to implement.
8. There should be an ability to distinguish between data retention on different types of data. Each type of data has different issues which need to be carefully weighed up and understood, not just on a national basis but internationally (as so much ICT service provision is now sub contracted to organisations with global ICT processing facilities). Important types of data include: traffic data, content, applications usage, code, and the retention of these data types have different implications for the Internet itself and for Internet users of all sorts.

Benefits to national security

9. The benefits of this information to protecting national security should be clearly demonstrated. So far, the Government is working on the basis that it believes that data retention rules are essential for maintaining national security. However, ISOC England would like to be convinced of the benefits of data retention. Due to the ability of criminal elements of society to avoid the UK's jurisdiction by using, for example, international ISPs, web-based email accounts and satellite telephones to cover paths, we are not convinced that the type of information required will have any real affect on national security.
10. Blanket data retention is not technically a solution to security needs. Indeed it may well harm security as it is very expensive and will draw limited resources away from more productive, closely targeted measures.

11. It fails to take into account that much Internet traffic is ephemeral in the sense it is not stored. Indeed next generation Internet projects such as Internet2 and The Grid imply that data is never permanently stored but simply circulates on very fast optical networks.
12. Streaming technologies as used in MPEG4 for video, webcams, video conferences, audio and others indicate an enormous amount of data of all types (see below) is involved. Growth in always-on and wider bandwidth usage of Internet applications demonstrates that traffic volumes are increasing rapidly and this has serious implications for the reasonableness of relying on blanket data retention.
13. Developments in alternative Internet access such as multi-homing and informal networks suggest that the assumption of an industry model of a single ISP supplier for a customer is not a model that security services should rely upon. Regulation to restrict Internet service provision would be exceptionally damaging to the long-term interests of an open free market-based UK economy.
14. Technologies such as steganography are freely available to make data retained appear innocent when it may or may not be. Therefore there is no surety that data once retained will offer any increase in the ability for security services to protect UK citizens.
15. Therefore the challenges for applying data retention as a security tool should not be underestimated, nor should the costs. Even if government security services require others to finance the retention of data, the transfer, searching and analysis requirements of this data can only increase as exponentially as the use of Internet itself.

Other uses of data

16. We believe that there should be complete clarity as to which bodies will be entitled to access any data retained by organisations. We consider it highly inappropriate for this type of data to be made available to the wide number of central government departments, local authorities and government agencies that the Home Secretary had first planned at the beginning of 2002. We do not consider that it is appropriate for bodies to give themselves authority to access any retained data. We would consider it essential to have a check and balance on this type of activity and to be scrutinised by Parliament. Scrutiny should also be extended to the issue of data leakage, which appears to be increasingly prevalent.

Human Rights Act

17. It is not clear whether the rules breach the Human Rights Act by allowing access to the information for police and others investigating cases that are not related to national security.

Technological neutrality

18. The rules are being applied specifically to online activity, which goes against the principles of technological neutrality that the Government has been keen to encourage. As such, email sender, recipients and subject matter would be recorded and retained for access at a later date, while no one would expect users of the traditional postal service to record such information. Similarly, the general public would not consider it to be appropriate for this type

of high level of scrutiny for the average high street shopping trip, whereas these blanket data retention rules are proposing this treatment for the online equivalent.

Voluntary vs mandatory

19. We do not consider that a mandatory code is appropriate. ISOC England's commitment to 'the Internet is for everyone' means that in principle, we do not approve of measures which restrict access to the Internet for individuals. We believe that the Internet remains in early stage deployment in the UK and that developments in access, service provision and end user devices will dramatically alter the Internet landscape and the economics of communications with unforeseeable opportunities for the UK economy and society. Legislation and regulation that makes assumptions about the Internet landscape of today is very likely to not reflect the landscape of tomorrow. Attempts to enforce a vision of how access provision of Internet is currently managed will fail as the economics of the market will dictate how access is in practice implemented.

Costs

20. We would consider that the costs involved in both retention and disclosure to be prohibitive to small businesses. Large businesses are often better positioned to be able to react swiftly to disclosure demands and due to the large quantity of data, to build disclosure forecasts into their business models. Each demand for disclosure will affect small businesses to a far greater degree and could result in punitive costs.

21. In all cases, the costs involved in data retention and disclosure are likely to be passed on to the consumer, creating further disparities between the larger operators, who have a larger customer base over which to spread costs, and smaller operators who will be forced to charge customers considerably more.

Exposure to third countries

22. We are concerned that the costs of data disclosure to foreign countries in compliance with their own regulations would have to be borne by UK companies. For third countries with particularly active regimes, a high volume of requests for data disclosure would put a considerable financial burden on UK industry.

Jurisdiction

23. The nature of the Internet means that physical location of a recipient or sender is often irrelevant. Different rules in different countries may put additional burdens on UK companies who are required to disclose information. We do not believe that UK companies should be required to retain data in order to comply with the data retention laws of another European country. If there are to be rules on data retention, ISOC England recommends that this should be under UK or European law.