Mr Simon Watkin
Access to communications data consultation
Home Office, Room 732
50 Queen Anne's Gate
London, SW1H 9AT

03 June 2003

Dear Mr Watkin,

Access to Communications Data: Respecting privacy and protecting the public from crime

GreenNet Limited (GNL) welcomes the opportunity to comment on issues relating to the 'Access to Communications Data'.

Although GNL appreciates the Government's concerns regarding national security and the need to protect the public from crime, we feel that the current proposals will have a significantly negative impact on the public's trust and confidence in the UK Internet environment.

GNL is unique in its response to the current consultations because it straddles both the commercial ISP and human rights, community development, 'NGO' and charity sectors. GNL, a non-profit ISP dedicated to supporting and promoting groups and individuals working for peace, human rights and the environment through the use of ICTs, is owned by a registered Charity, the GreenNet Educational Trust. GreenNet Limited, aims to realise the rights of all individuals in the UK to enjoy full access to information and communication services.

Our response places emphasis on the concerns of individual and community groups as ***users*** of communication technology services, rather than only the needs of communication service ***providers'***. In making this submission, GNL alludes not only to those who are privileged to make use of communication services at present, but also takes into consideration the potential of a free and open communication network to benefit the realisation of social, political, economic and human rights for **all** in the UK.

GNL has endorsed the ISPA responses to the current consultation and fully supports ISPA's concerns about liability and cost, but wishes to make the following additional comments and suggestions.

Trust

In a recent conference for women's groups in the UK to discuss the role of new technologies in facilitating their efforts in achieving gender justice, individuals expressed great concern at the current proposals, in fact, many noted that they would think seriously about continuing to use the internet in the many ways they do now.

Victims of violence and abuse have been able to use the relative privacy and anonymity of the Internet to express themselves and their situation in a way that would have been previously impossible. Research of Gender and ICT advocates has highlighted the need for women to have secure, private and safe spaces, as a pre-condition for full and free expression, particularly when concerning

sensitive, and sometimes life-threatening information.[1]

Just as privacy, confidentiality, integrity and secure infrastructure are essential in the operation of a 'safe- house' or women's refuge, so they are also are in the environs of the Internet as far as many women are concerned[2].

As noted by the Home Secretary in the Foreword to the Consultation Document: " [the] Government needs to secure public confidence that the boundary between privacy and protecting the public is set correctly'.

We feel that the boundaries are set incorrectly, overstating 'the interests of national security' and neglecting the rights of individuals and organisations who make use of electronic communication networks. Rights, including privacy and data protection, have come under unprecedented stress in the UK and throughout the world in the course of policy development and legislation in this area`[3], and we feel these proposals contribute further to that stress.

The current proposals will greatly diminish the confidence of these user communities, as well as countless others, who have discovered the Internet as one of the only means of accessing information, communicating and realising their fundamental human rights.

So, whilst asking whether the approach being taken is appropriate and proportionate in relation to the threat to national security, one must also address the potential impact the current proposals could have in relation to trust, privacy and confidence, for thousands of existing users in the UK and millions who have yet to enjoy the benefits of a free and open internet environment.

Judicial Oversight

Another major issue of concern is the ease with which personal communications data can presently be accessed by authorities. GNL reasserts the need to build in strong safeguards to protect users from any personal invasion of privacy.

We remain convinced that only by assuring full judicial oversight in the granting of public authority's access to communications data, can the Government be assured of building the confidence and trust it seeks.

In addition, an 'Access to Data Communications' full disclosure table, which would keep tabs on requests granted, requests served, and those which assist public authorities in solving crime, would also contribute to building that confidence and trust by demonstrating transparency and accountability. An independent third party should be responsible for maintaining the database.

In the absence of such judicial oversight, users have a right to be informed when any third party requests access to their personal data, as is the practice of many ISPs who conform with Data Protection Principles.

Training

[1] http://www.apcwomen.org/gem/Gender_ICT/index.htm#privacy
[2] http://www.greenneteducationaltrust.org.uk//programme.htm
[3] http://www.privacyinternational.org/intl_orgs/eu/delgado-letter-503.html

Trends in the UK point to an increasing tendency amongst ISPs, particularly small and medium sized, to take the 'least cost – least hassle' route when dealing with requests for data, or questions regards content hosting.

As a report by the Law Commission recently noted[4], many ISPs are in effect acting as censors when responding to legal or other threats of libel and defamation by adopting a 'take-down' policy. This is often done in the interests of time saving, stress avoidance or lack of awareness of existing rights, but in effect, has the impact of removing content from the public domain which may be in the public interest.

The same situation may develop with ISPs in relation to requests for Access to Data Communications. In the interests of expediency and with insufficient training, ISPs will hand over sensitive, personal data to unauthorised entities.

Training for ISPs in understanding and complying with Data Protection Law, how to recognise legitimate and lawful access requests and how to authenticate a request, should be provided and resourced.

Consultation

We appreciate that the Home Office has provided a 3-month time frame for consultation, as is standard practice. However, we urge the Government to acknowledge that this is not a 'standard' situation.

As noted above, existing rights such as privacy and data protection are under unprecedented stress, the Industry remains unconvinced that the current proposals will achieve the government stated aims, the general public has not been sufficiently informed of the issues and outside of a small number of ISPs, participation in consultation has been limited to a very small number of representatives from only one of the many stake-holders who will be affected.

We aim to continue to raise awareness around these issues with the hope of educating at least some of the public, to enable them to make informed and responsible choices.

As the Home Secretary states: 'There is a judgement to be made here; one that we are determined should be informed by wide public debate of the issues.'

We would then ask that the Home Secretary extend the consultation period and develop an accompanying educational or awareness raising programme, which will be open and accessible to all those who will be affected by these proposals.

Please don't hesitate to contact me if you require any further information.

Best regards,

Karen Banks
Director, GreenNet Limited

[4] http://www.lawcom.gov.uk/files/defamation2.pdf