Faegre & Benson LLP
7 Pilgrim Street
London
EC4V 6LB

17th August 2009

Feagre & Benson LLP have been requested by The Cloud Networks Limited to provide legal advice, in the form an open letter, on recent EU directives that came into force in April 2009. The UK government brought into force a EU Directive covering the delivery of public Internet services permitting it to require individuals, businesses and other organisations to retain specific user/customer information to ensure compliance with the EU Directive covering Data Retention Regulations.

The Cloud Networks Limited has requested that we explain their legal responsibilities, in the form of an open letter, to allow other businesses and organisations to fully understand their obligations if considering the delivery of public access Internet services, including the full implications of breach and the legal remedies available to the UK authorities, which ultimately can extend to uncapped fines, imprisonment and payment of damages.

Faegre & Benson LLP are an international legal practice offering specialist skills in telecommunications regulation and operations. In addition, we offer a full complement of other legal services to clients ranging from emerging enterprises to multinational companies. Our practice has more than 500 lawyers handling complex transactions and litigation matters throughout Europe, the Middle East, the United States and Asia.

If you require further information or advice regarding new legislation, its implications, your obligations, please contact John Enstone, legal counsel and telecommunications lawyer at **jenstone@faegre.com** or 020 7450 4557.

Background

The Data Retention (EC Directive) Regulations 2009 came into force on the 6th of April 2009. The regulations apply to public communications providers and the data generated or processed in the UK by virtue of supplying the communications service or network concerned. The legislation is an extension of existing requirements to Internet service and network providers.

A public communications provider is defined as:

- anyone who provides a public electronic communications network (defined as being provided wholly or mainly for the purpose of making electronics services available to the public),
- anyone who provides a public electronic communications service (defined as being provided to be available for use by the public), or
- a person who makes available facilities associated with a public electronic communications network or a public electronic communications service.

WiFi hotspots in public and enterprise environments providing access to the internet to members of the public, free or paid, are public communications services. The provider of the location and the operator of the network are public communications providers under the legislation.

The legal authorities are within their rights to seek access to this data, as the legislation is designed to avoid anonymous access and to ensure full compliance with the telecommunications regulatory framework.

FAEGRE & BENSON LLP

Legal Obligations

A notified public communications provider must retain the following data about Internet access, Internet email and Internet telephony for 12 months from the date of the communication in question and be prepared to provide this information on-demand to authorised law enforcement and other authorities:

- communication source – the user ID allocated; user ID and telephone number allocated to the communication entering the public network; and the name and address of the subscriber to whom an IP address or telephone number was allocated at the time of the communication,

- communication destination – the user ID or telephone number of the intended recipient of the call (internet telephony); and the name and address of the subscriber and the user ID of the intended recipient of the communication (email or internet telephony),

- communication origination – (in the case of internet access) the date and time of the log-in to and log-off from the internet access service, based on a specified time zone; the IP address allocated by the internet access service provider to the communication; and the user ID of the subscriber of the internet access service; (in the case of email or internet telephony) the date and time of the log-in to and log-off from the email or internet telephony service, based on a specified time zone,

- communication type – the internet service used,

- communication equipment – identification of the location and edge equipment used by the originator of the communication.

Public communication providers are not required to keep a copy of the content of user communications, and indeed keeping copies of content without permission from the user concerned can create other liabilities.

The public communication provider must report the status of their compliance with the legislation annually to the Secretary of State, including: the number of disclosures of the retained data in response to a request; the time between data retention and the request for disclosure; and the number of occasions when a request for lawfully disclosable data retained in accordance with the Regulations could not be met.

The Data Protection Act 1988 ("DPA") creates a further set of obligations on anyone who provides a public communication service to hold and process personal data on the users of their networks in compliance with a defined set of Data Protection Principles, including: to process data fairly and lawfully, obtain the consent of users in certain circumstances, store the data securely, destroy the data when no longer required, and meet higher standards for sensitive personal data (race, religion, political opinions, etc.).

Other applicable and related legislation and information include:

- Regulation of Investigatory Powers Act 2000 (and supporting Orders), which regulate how the data held by public communications providers may be accessed.

- Anti-Terrorism, Crime and Security Act 2001, which addresses the powers available to law enforcement agencies investigating serious crime relating to national security.

- The Home Office Consultation Paper "Protecting the Public in a Changing Communications Environment (April 2009)" which proposes that public communications providers be required to organise and match third party data to their own data and to collect third party data crossing their networks.

- The Home Office Consultation Paper "Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice (April 2009)" which proposes a review of the powers of public authorities.

- European Convention on Human Rights and Fundamental Freedoms,

- Human Rights Act 1998.

Liability & Penalties for Breaches

The Information Commissioner and Secretary of State are responsible for monitoring the application of the provisions of the legislation.

The regulations are enforceable by civil proceedings by the Secretary of State ("SOS"), including an injunction or an order for specific performance of a statutory duty, together with damages. Failure to comply with a notice from the SOS can result in a fine (uncapped) or imprisonment (s.45 of The Court of Session Act 1988). A body corporate's directors, managers, secretary and similar officers are liable under the DPA for its acts if it can be shown that they consented, connived or were negligent.

The Government intends to create an implementation group to give guidance on interpretation of the regulations in practice. Existing guidance indicates that the Government may introduce stronger sanctions if compliance falls short of expectations.

NOTE: The foregoing is intended to alert readers to certain important aspects of new legislation only and should not be considered or relied upon as legal advice. Specific professional advice should be sought before any action is taken.