February 2007

The effects of EU Directive on Free Wi-Fi

Summary of Directive 2006/24/EC (15 March 2006) on the retention of data generated or processed with the provision of publicly available electronic communication services or of public communications networks

The effects of EU Directive on Free Wi-Fi

Summary of Directive 2006/24/EC (15 March 2006) on the retention of data generated or processed with the provision of publicly available electronic communication services or of public communications networks

Background to the Directive

The Directive was passed in the wake of the 7 July 2005 bombings in London. The aim of the Directive was to create uniform standards for the retention of communications data across the EU. The purpose of this was to make it easier for law enforcement agencies to combat terrorism and organised crime, by ensuring that electronic communications data is traceable and retained securely for a minimum period. The Directive covers fixed telephone services, mobile telephone services, Internet access as well as Internet telephone services.

The requirements for retention of data in relation to all providers of Internet access, Internet email and Internet telephony services

The Directive requires that data necessary to trace the source of a communication is stored. This means that the individual user ID, telephone number, and name and address of the subscriber using the service at the time of a communication must be stored. In addition the same data must be stored so that the destination of a communication can be traced. Data must also be stored so that the date, time and duration of the communication can be traced, including the date and time of the log-in and log-off of the user.

The data must be stored for a minimum of 6 months, and destroyed after 2 years. The data must be stored securely, which means that service providers must ensure that it cannot be tampered with or altered, and that only specially authorised personnel can access the data. It must be stored in such a way that it can be supplied without undue delay to law enforcement authorities. There will be a public authority in the UK allocated the task of ensuring compliance with the requirements of the Directive.

When will it come into force in the UK?

The Directive will be enacted into UK law before it becomes effective. This must happen between 15 September 2007 and 15 March 2009 at the latest. Given the UK's stance and concerns about combating terrorism, as well as their recent enthusiasm for enacting anti terrorism legislation it seems likely that they will implement the directive reasonably quickly.

Will this new law apply to Wi-Fi Service Providers?

Yes, the new law will apply to any company providing Internet access to its customers, whether the user has to pay for access to the Internet or not. This will catch all Wi-Fi service providers from networks like BT Openzone, aggregators like BOZII, down to independent hotspot operators like coffee shops or hotels.

Implications for Service Providers

There are four factors which service providers will need to take into consideration when complying with the new law:

1. Storage requirements
2. Retention management and disposal of data
3. Designing a system that allows the authorities to access data required without undue delay
4. Cost

Despite ISPs collecting data on usage patterns, for billing and marketing purposes, the new law will mean that ISPs will now need to store additional data such as IP addresses, records of e-mails and Internet calls, all of which will require large amounts of storage capacity.

> **Gartner** predict that an additional 50,000 terabytes would have to be collected and stored within the EU. "The size of the storage systems needed to support such activities may need to be large and able to scale without performance degradation throughout its life," said a spokesperson at Gartner.

It is uncertain how long ISPs will be required to store the data, and the management of disposing of data before the 2 year deadline. The EU directive requires ISPs to store data for a minimum time of 6 months, but it is likely that when the law comes into effect in the UK, retention of data will be required for the full 2 year maximum period.

> "I think that we would be on the extreme end of the time limits for these regulations," said Graham Titterington,

principal analyst at **Ovum**. "I'd expect the UK to impose the maximum time limits."[1]

Who will have to pay for implementation of this new law?

The company providing the Internet access to the end user will have to bear the cost of setting up, maintaining and managing the retention of data, whether the Wi-Fi service is charged for or not.

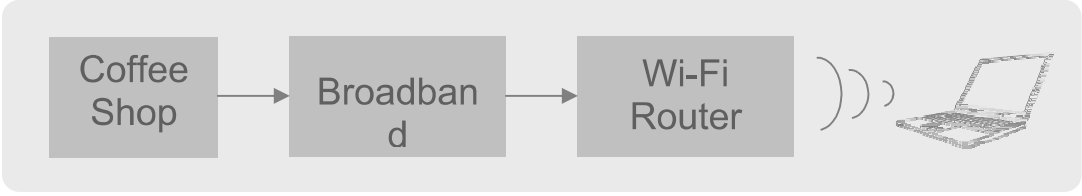
The directive does not oblige member states to reimburse telecom companies for additional costs incurred in servicing law enforcement requests, a factor highlighted by market analysts **Frost & Sullivan** in a recent report on the impact of the directive on the telecoms sector[2].

> **ISPA** cites estimates from one large UK-based ISP that it would cost £26m to set up data retention kit on its systems and £9m a year in running costs to service law enforcement requests.

Italian ISP **Tiscali** also believes this is a serious issue if the law is to work. "There is a concern that the directive makes no provision for reimbursement to ISPs for extended data retention," said Emeric Miszti, Security and AUP Officer at Tiscali. "Data retention is not simply about disk drives. The development, management, and security costs must be taken into account."[3].

How will this affect companies who offer Free Wi-Fi?

Quite often companies who run a free Wi-Fi service are aiming to entice more customers to their establishment, such as hotels and coffee shops with a cheap value added service. Often the management of the establishment will use an existing broadband line and simply attach a Wi-Fi access point to offer a free and open service.



[1] http://www.pcpro.co.uk/security/news/102171/fears-grow-over-eu-data-retention-law.html
[2] http://www.out-law.com/page-7635
[3] http://news.zdnet.co.uk/itmanagement/0,1000000308,39246970,00.htm

Because the objective of the EU directive is combating terrorism, it will apply to these locations which offer free Wi-Fi services, despite their core business not being an Internet Service Provider and the lack of profit they receive from their service.

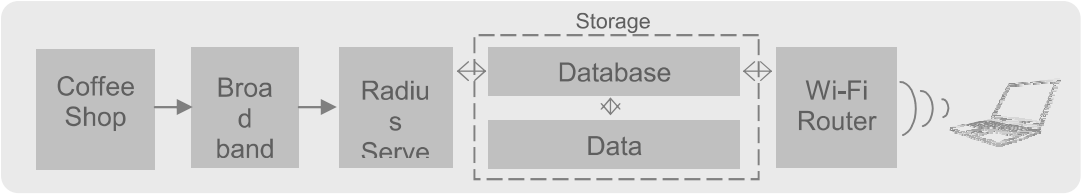
> Importantly service providers not previously obligated to retain data will now be governed by the EU Directive stipulations, **Frost & Sullivan** notes[4].

Under the new law, businesses who want to run a free Wi-Fi service will need to do the following:

Store data about the user
Store the IP address associated with that user during their session
Store the start and end time of their session and the duration of the session
Store web traffic on internet calls, times and dates of e-mail checking and web mail, etc

To comply with the law the business will need the following equipment:

Radius server for authenticating users
Storage server for holding data
Database to store user details and internet data



The cost of setting up such a service will increase astronomically, with hardware and labour set-up costs running well in to the thousands of pounds, and monthly hosting, storage and data management fees exceeding hundreds of pounds per month.

It is this high level of cost and management that will deter independent establishments wishing to entice customers to their coffee shop or hotel with free Wi-Fi from providing such a service in the

[4] http://www.out-law.com/page-7635