

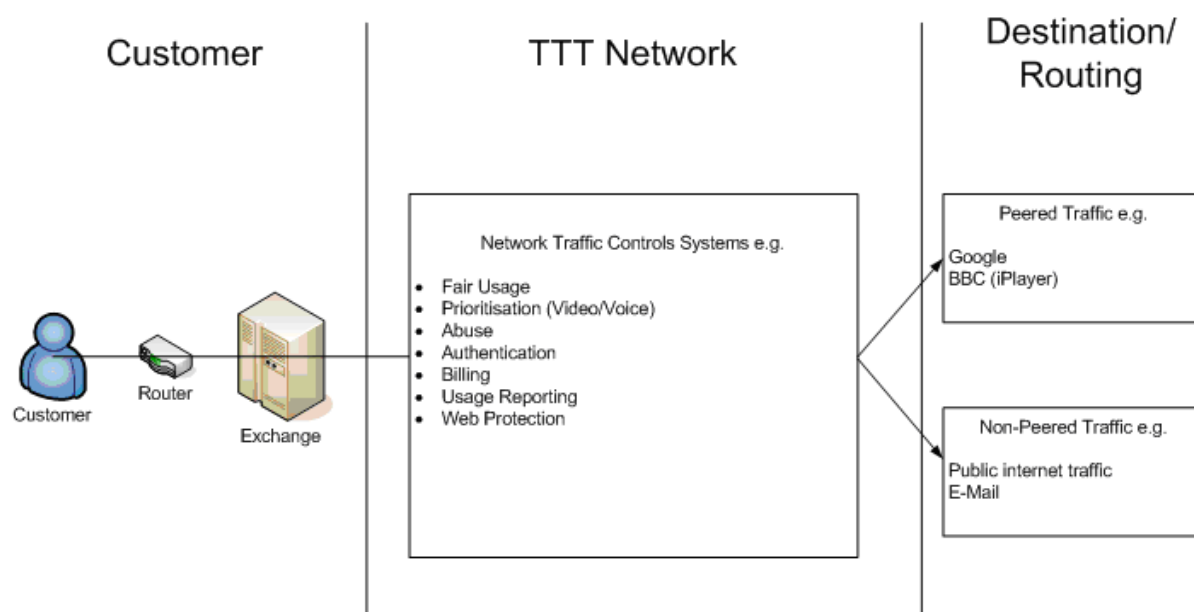
## TalkTalk Group Anti-Malware System Summary

This note is provided in response to a letter from the Information Commissioner dated 30 July 2010 as well as those enquiries made during a meeting with a representative of the ICO on 16 August 2010.

### TalkTalk Network

As a network operator, TalkTalk receives and processes billions of requests each day from its customers to connect to websites across the internet. These requests are routed across the TalkTalk network and beyond to connect customers to these websites.

Below is a diagram of how traffic is routed through the TalkTalk network.

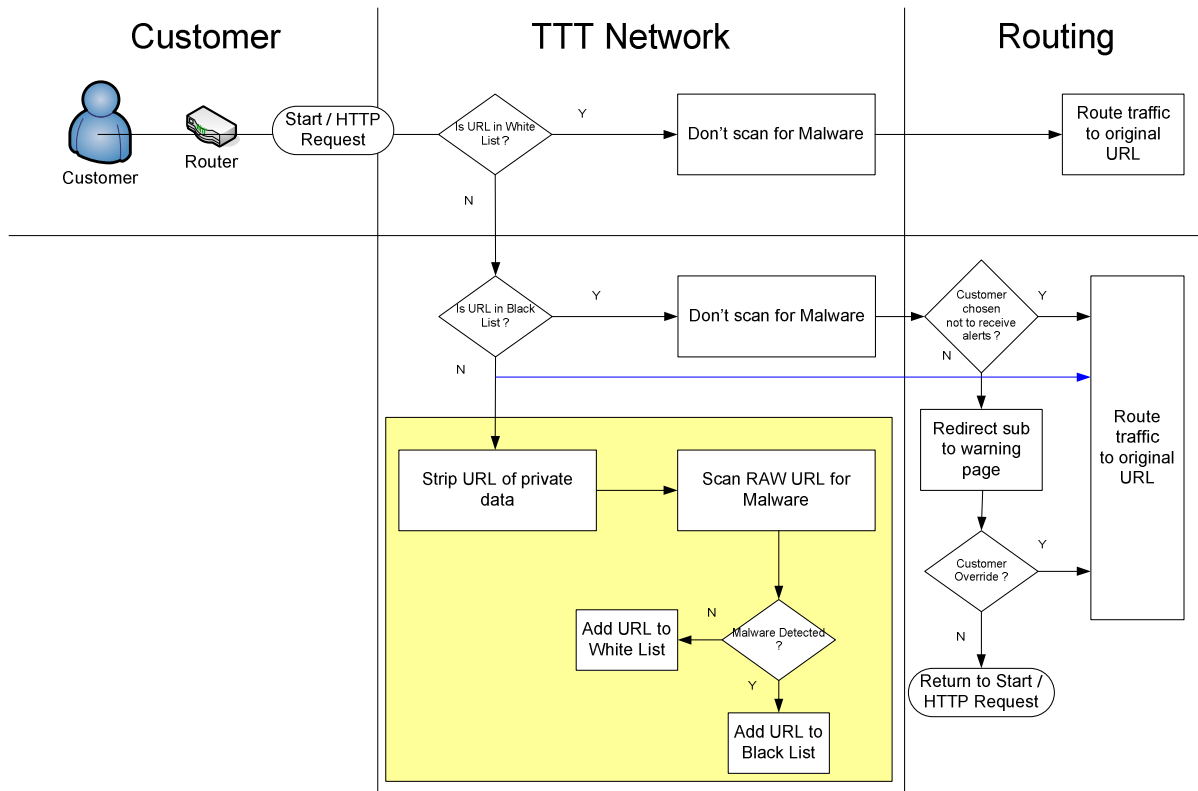


### The Anti-Malware System

TalkTalk's anti-malware system is located in the TalkTalk network. Being located in the TalkTalk network, the anti-malware system is subject to the same high level of security applicable to the TalkTalk network and TalkTalk's customer data. The anti-malware system does not record or scan any secure "https" website URLs.

The anti-malware system is currently being run as a trial and, as such, no personal data is being processed. In due course we intend to introduce a warning system in relation to potentially harmful URLs.

Below is a diagram setting out how the anti-malware system will operate when implemented as a product offering to customers.



The anti-malware process starts when a customer points his or her browser to a URL. If that specific URL has not been routed through the network that day the specific URL is extracted by the anti-malware system from the general traffic routing data associated with that request. The anti-malware system does not record who sends the request or any other personal data with the URL.

The anti-malware system then scans the URL and implements analysis and detection. Following the analysis and detection each website URL is placed in a white list (the scan is clean - retained for up to 24 hours and then automatically deleted) or a black list (the scan shows viruses, malware or other irregularities - retained for up to 7 days and then automatically deleted).

Given the volume of website URLs, the network processes billions of routing requests a day, these lists are recorded in transient memory and not in accessible physical storage.

When the anti-malware warning service goes live these lists will be used to alert customers to websites suspected to have malware or viruses, depending on whether they have chosen not to receive such alerts. Customers who have chosen not to receive alerts will continue to browse as they do today without alerts when they visit potentially harmful websites.

#### Data Protection Act 1998 ("DPA")

The anti-malware system records website URLs alone (and not together with any other information). The website URLs constitute "data" under the DPA. While the data relates to a living individual (as it is an individual who initiates the request to access the website URL), the individual cannot be identified from the data itself nor from the data together with any other information in our possession.

The website URL may by its nature contain information about racial or ethnic origin, political beliefs, religious beliefs or other areas referred to in section 2 DPA. However, as the website URL data does not constitute "personal data" under the DPA, it will not by definition constitute "sensitive personal data".

Pursuant to section 17 of the DPA, both Opal Telecom Limited (the network provider) and TalkTalk Telecom Limited (the primary entity contracting with customers) are registered under the DPA.

### Privacy and Electronic Communications (EC Directive) Regulations 2003 (“PECR”)

Under PECR, “traffic data” is defined to include “data relating to the routing, duration or time of a communication”. The website URL is traffic data.

Our use of the traffic data is compliant with regulation 7 of PECR. The traffic data, when no longer required for the purpose of the transmission of the communication (i.e. requesting the website URL), is modified such that it ceases to be personal data (under regulation 7(1)(b) or (c)). In fact, the website URL does not require modification as it never becomes personal data. The network records the destination website URL with no reference to the customer who made the request.

The anti-malware service does not store information, or gain access to information stored, in the terminal equipment of a customer. PECR regulation 6 does not accordingly apply.