TalkTalk Network Security and RIPA

Representatives from TalkTalk and Open Rights Group met at the offices of TalkTalk for an "on the record" discussion about TalkTalk's proposed Network Security product "BrightFeed".

Open Rights Group questioned whether the operation of the virus alerts system within the proposed Network Security product was compliant with the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). TalkTalk was confident that the virus alerts system did not contravene RIPA and offered to set out its reasons for this. TalkTalk's legal analysis of the position is set out below in a format designed to be understood by people having differing levels of technical knowledge. It is a non-exhaustive summary.

Network Security Virus Alerts

When a TalkTalk customer decides to access a website URL using TalkTalk's network, the network will route the customer to that URL. It is important to stress that it is TalkTalk's network that routes the customer to the chosen URL. There is no manual intervention by TalkTalk employees, for example by seeing which URL has been requested and then routing the customer accordingly. TalkTalk's network through its many circuits, devices, systems and electrical components, is a closed network ("**Closed Network**"). It is the Closed Network that is made aware of the chosen URL and it is the Closed Network that routes the customer to the website URL.

The Closed Network does not report on individual customer's browsing details. Once a customer has been routed to a URL, the Closed Network remains "closed" and TalkTalk does not produce any report of which URL was visited by that customer. As such, TalkTalk does not knowingly keep the browsing information of which particular website a particular customer has visited.

Once a customer has visited a URL, the virus alerts system within the Closed Network uses the URL only and takes all reasonable steps to anonymise any personal data in the URL. Then, if it is the first time that day that a customer has visited the URL, the virus alerts system will later also visit that URL and scan that website for viruses and other malware. (No secure "https" URLs are scanned.) If viruses or other malware are found at that URL, customers who are receiving the Bright Feed virus alerts service will receive a pop up warning if they request that URL. The customer can then choose whether to continue to the URL or not.

Does the Closed System Intercept a Communication?

RIPA seeks to protect the confidentiality of communications on public telecommunication systems by making it an offence to intentionally, and without lawful authority, intercept a communication in the course of transmission. Section 2(2) of RIPA provides that:

> *"a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he —*
>
> *(a) so modifies or interferes with the system, or its operation,*
>
> *(b) so monitors transmissions made by means of the system, or*

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."

TalkTalk is not monitoring transmissions made by means of the Closed Network. The Closed Network does not monitor the transmissions it makes but, following a URL request from a customer, actually effects the transmission across the Closed Network. It is through this process that the Closed Network becomes aware of the URL, not through the process of monitoring a transmission which would fall under Section 2(2)(b) above. (The actions of the virus alerts system in the Closed Network do not fall under Sections 2(2)(a) or (c) above.)

In TalkTalk's opinion, the way in which the Closed Network operates, and the manner in which the Closed Network becomes aware of URLs which customers visit, does not constitute an intercept of a communication in the course of transmission for the purposes of RIPA. The Closed Network does not monitor a transmission for the simple reason that the Closed Network actually makes the transmission and is already aware of the transmission. The Closed Network being aware of the URL, then allows the virus alerts system within the Closed Network to scan the URL for viruses and other malware.

Lawful Usage under RIPA

Even if TalkTalk's opinion that the operation of the Closed Network and the virus alert system does not constitute an intercept of a communication in the course of transmission is incorrect, TalkTalk remains confident that RIPA permits the operation of the virus alert system in the following ways:

A. Traffic Data

RIPA contains an exception for "traffic data". Section 2(5) of RIPA states that the interception of a communication in the course of its transmission does not include references to:

"any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any … telecommunication system by means of which it is being or may be transmitted"

Section 2(9) of RIPA defines "traffic data", in relation to any communication, as:

"(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;
(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;
(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication; and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication;

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored."

In TalkTalk's opinion a specific URL entered into a browser to request access to a specific website falls under the definition of "traffic data" under RIPA. A URL is a form of data identifying where a communication is to be transmitted, i.e. to the website identified by the URL following which contact can be made available to the user. As such, it is lawful for TalkTalk under RIPA to use this traffic data for its virus alerts system.

B. Operation of TalkTalk's Service

The rapid growth of the internet and the number of people using it provides e-criminals with an even greater range of targets for viruses and malware, including individuals, organisations and the networks through which they access the internet. To combat this activity, and to protect our customers and network, TalkTalk already scans incoming emails received on TalkTalk domains for viruses and other malware. The virus alerts system is simply an extension of TalkTalk's existing actions to protect customers and our network from viruses and malware.

The interception of a communication is lawful under Section 3(3)(b) of RIPA if:

"it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services."

It is generally accepted that the following types of interception are justified under section 3(3)(b), namely (i) scanning/filtering to prevent the distribution of bulk unsolicited email (spam), and (ii) scanning/filtering to prevent the distribution of viruses and other malicious code.

TalkTalk's virus alert system falls within these purposes being connected with the provision or operation of TalkTalk's service. Without such scanning/filtering, spam and other viruses and malware would render customers computers useless, or turn them into sources of spam and malware inflicted on others resulting in email, and ultimately networks, becoming unreliable, unusable and unstable. The internet would not continue to function without ongoing efforts to remove viruses and malware.

TalkTalk has further obligations in this regard under the Privacy and Elections Communications (EC Directive) Regulations 2003 (**"PECR"**) to safeguard the security of its service. Regulation 5(1) of PECR states:

"… a provider of a public electronic communications service ("the service provider") shall take appropriate technical and organisational measures to safeguard the security of that service."

Implementing the virus alerts system is a further measure TalkTalk is taking not only to help protect consumers, but also to safeguard the security of TalkTalk's network from the effects of viruses and malware. The furtherance of these obligations is also permitted under section 3(3)(b).

TalkTalk Group Limited
28 January 2011