Network Neutrality

Definition: Network neutrality has been used to describe a number of contentious issues from a commercial, legal, security and operational viewpoint. Generally speaking, it has been taken to mean that any choice of communications service or information technology component does not reduce other choices available to the user for different services or components, and that each choice is treated neutrally by other elements in the end-to-end service continuum. This includes all devices, services, management tools, content and applications, and the sender or receiver IP address. Despite the step change nature of technical progress, the principle of neutrality remains an objective, and the impact on existing investments requires mitigation via maximising backwards compatibility.

Background/Context: Industry debate on network neutrality has been unduly dominated by representations from the intellectual property movement and the media content industry, and by misguided attempts to eliminate or block illegal or undesirable content. It has also suffered from premature classification of content and applications as justification for blocking service usage. Inadequate attention has been directed towards business users, and their needs for differentiated quality of service guarantees. The mixed-use environment of the internet must accommodate the real practical considerations associated with applications and content delivery, which need, for example, very low latency.

The internet is being used increasingly by machines as well as people, and in an international borderless context. The extended supply chain in most commercial industries and in the public sector means that end-to-end connectivity traverses different suppliers of components, all of which are not under the control of a single service supplier or user. The key objective here is seamless, timeless interoperability. This includes functionality, operability, total quality, information content and display capability, and includes indirect connection of a piece of technology via one or more intermediate devices.

These aims must not, however, prevent traffic prioritisation to enable differentiated quality of service and delivery of guaranteed service levels for specific applications and content. The need for a defined quality of service for the internet beyond 'best efforts' is essential for business users.
A correct regulatory balance is therefore necessary to achieve this without sacrificing open access and a competitive market. Exceptions for network security and integrity, for example to block spam, may be justifiable, but exclusion of a specific application from data volume limits (caps) where an operator's partner provides the application is positive discrimination, and is unacceptable.

BCS position on key issues:

- **Content and application definition and classification**

BCS believes that a prerequisite to acceptable transparent traffic management is the presence of open and standard agreed definitions and classification of content and applications. Any regulation defining if and how certain applications may be prioritised can only be based on such agreement. Current disagreements on this issue, for example with regard to blocking Skype as 'Voice over IP', when the provider claims that it is an application, not 'Voice over IP', is just one example.

- **Transparent traffic management**

Prioritisation of certain traffic due to the classification of its content or its application, for example streamed video, financial transactions, energy control device management, traffic systems or for

health monitoring are acceptable and justified, but BCS believes this must always be transparent, including in failover situations. This is necessary to ensure prioritisation is not applied for any other reason, such as to favour a particular supplier of the service, who may be the traffic manager.

- **Equivalence of access input**

BCS believes that the choice of supplier for a network access component, for example wholesale broadband input, must be network neutral in terms of equivalence for traffic management throughout the rest of the end-to-end connection. This is essential to ensure fair competition for supply where a dominant supplier is providing unbundled access, for example, to a competing network supplier. IP network aspects of network neutrality clarify vertical separation between transport and services. This reinforces the required flexibility, where a user has a clear competitive choice for service and transport providers independently. In the internet, the carrier generally bears transit costs and bills the customer for the cost of termination. However, IP Quality of Service transport classes introduce a technical potential for implementation of discrimination contravening network neutrality principles.

- **Interoperability and switching**

The multi-site, multinational connectivity requirements of enterprises demand a greater level of network neutrality, as well as common standards across national boundaries. Any regulation needs to protect end-to-end connectivity and interoperability from denial of application use, or blockage of content, due to the actions of one service provider within the connectivity chain. BCS believes that regulation is needed to safeguard critical business processes, especially for SMEs who cannot tolerate differentiation or discrimination like an individual consumer, who can use a competitive retail market to change supplier. Enterprise customers cannot do so in such circumstances. It must be possible for each organisation within the extended supply chain to switch supplier of just one, or more, service components, whilst preserving interoperability with the rest of the end-to-end communication.

- **Illegal content, intellectual property rights and piracy**

Preserving intellectual property rights is the responsibility of the IPR owner and not providers of the delivery services between content and user. BCS does not believe network service providers can police illegal downloading of content, or unlicensed use of applications, nor should they be held responsible for stopping such breaches. Attempts to prevent continued illegal use by demanding disconnection of users is neither appropriate nor feasible. Internet Service Providers are unaware of the identity of their entire user base, and could disconnect a potentially unrelated business service by mistake. Deep packet inspection to assess the nature of content in a communication should not be demanded.

- **Vertical integration and bundling**

BCS believes there must be clear prevention of discrimination through vertical integration. This has the indirect benefit of recognising the importance of demand aggregation, and single or dual supplier strategy, as mechanisms for business users to optimise contract arrangements, minimise cost and simplify operational administration through leveraging economies of scale. The use of service ’bundles’ to obscure discrimination is a further challenge for national regulatory authorities to identify, given that in some cases this may be indirect positive discrimination, where the bundle includes bought in, or separately supplied services or devices. General fair trade regulation, preventing linked sales and below cost service subsidisation, may be adequate to prevent such practice.

Nick White, Chair INTUG (author)
Rick Chandler, BCS CMA SG (spokesperson)
Roger Marshall, BCS Immediate Past President (spokesperson)