Your response

Akamai's response to Ofcom's Consultation: Net Neutrality Review

January 13, 2023

Akamai appreciates the opportunity to participate in the dialogue Ofcom has convened to review the U.K.'s net neutrality rules and assess whether those rules continue to encourage innovation, investment, and growth by key players in the internet value chain. From its founding, Akamai has been committed to ensuring that its customers interact with an efficient, reliable, and secure internet and respectfully submits its comments to Ofcom's questions regarding traffic management below. These responses reflect Akamai's concern that Ofcom's proposal to permit internet service providers to manage congestion by prioritising different classes of content will undermine the incentives that have made U.K. networks some of the most resilient in the world. In so doing, it may inadvertently make the market for internet content less competitive, slow down the pace of innovation, and create new threats to user privacy.

I. Akamai Background

Akamai develops solutions to the many issues that businesses confront on the dynamic landscape of the internet. Based in Cambridge, Massachusetts (U.S.), Akamai has forty-two offices across five continents, including two in the United Kingdom (London and Edinburgh). Akamai employs over 9,200 people.

Entrepreneurship and innovation have driven Akamai since its genesis at the Massachusetts Institute of Technology ('MIT'). In 1995, Sir Timothy Berners-Lee — inventor of the World Wide Web — recognised that internet congestion would become a problem and challenged his MIT colleagues to devise a solution. Dr Tom Leighton, who headed MIT's Algorithms Group (and is now Akamai's CEO), recruited graduate student Danny Lewin to help solve the problem. Leighton and Lewin collaborated with their colleagues to develop innovative algorithms that would allow for the replication of content over a wide network of distributed servers, and the routing of consumer requests for content to optimal servers. In 1997, the group entered the renowned MIT Entrepreneurship Competition and was selected as one of six finalists. With the goal of making the internet faster and more reliable, the founding team added members and planned the business that would become Akamai in 1998.

The story of Akamai and its growth over the years mirrors that of the development of the internet as it has become more and more central to the everyday lives of billions of people around the globe. With each new phase in the life of the internet, Akamai has shifted to address new challenges and problems facing the internet community including greater sophistication of online communications, global security concerns, and the shift to cloud infrastructure for traditional networking, compute, and storage functions.

As a pioneer in the content delivery industry, Akamai defined the space and developed extensive distributed architecture and intelligent mapping algorithms, unique among companies in the industry, designed to reduce network congestion and improve performance. Unlike other content delivery companies that serve content at (or outside) highly congested network peering points, Akamai implements its technologies deep in the networks of last-mile broadband providers and caches content locally. Akamai's customers — web sites, web application providers, and enterprises — provide content and applications that Akamai distributes across these networks. When a consumer requests content or accesses an

application, Akamai directs the request to the optimal server for the user balancing geographic proximity, performance, and traffic congestion. To do so, Akamai also uses specialised technologies — e.g., advanced domain name service mapping, communication protocols, load balancing, and data analysis — to respond to consumer requests for information most efficiently. As a result, Akamai's services effectively offload traffic from the middle mile, improving performance for both big and small content providers.

Akamai's content delivery network ('CDN') comprises over 365,000 servers in thousands of locations inside over 1,400 global networks located in over 135 countries. On a typical day, its CDN offloads more than 178 Gbps from the middle mile. Akamai's congestion-management and capacity-enhancement practices benefit not only Akamai's customers, but also other content providers and carriers, who gain in general from networks with reduced congestion and increased capacity.

Globally, Akamai's customers include: 16 of the 20 most popular video streaming services, 18 of the 20 largest video games companies, 17 of the 20 biggest telecommunications companies, 8 of the top 10 banking, brokerage and fintech firms and 15 of the 20 largest pharmaceuticals companies. Akamai has deployed the most pervasive, highly distributed content delivery network (CDN) in the world, averaging over 6 trillion deliveries per day.

As Berners-Lee predicted, the internet has witnessed ever-increasing volume and sophistication of online communications, resulting in significant challenges to the internet's ability to function in the face of the staggering traffic load and Akamai has been there to face these challenges. As the world has grown to rely on the internet, a trend that was dramatically intensified with the world's heightened reliance on the internet for work, education, health services, and entertainment during the COVID-19 pandemic, security has become a material concern for users and enterprises. Akamai has pivoted over the years to address these concerns as well by developing unique technologies that allow its customers to interact with the global community of internet users in an efficient, reliable, and secure manner.

Akamai's distributed architecture also enhances network security. It keeps harmful attacks farther from content providers' servers and enables Akamai to inspect and mitigate attacks at the 'edge' of the internet. Akamai also provides protection across all pathways to data centres. Whether these attacks are volumetric (so-called 'DDoS attacks') in nature and designed to shut down access to a website or application, or are attempts to deliver malware, ransomware, or 'bots' to breach security protection or steal data and services, Akamai has developed solutions to prevent and mitigate the harm to customers, data centres, and internet users. By blocking attack traffic originating from overseas before it can reach the U.K., for example, Akamai prevents enormous volumes of attack traffic from clogging U.K. networks, benefitting internet users across the U.K. regardless of whether the content they access is on the Akamai network. By protecting some of the world's largest and most-attacked web properties, Akamai also develops valuable insights into the nature and scope of threats. Akamai combines these insights with its robust suite of security services to identify and block malicious traffic and activity across the internet.

The rise of the internet and the reliance of consumers on the internet in their lives have driven a third significant addition to the role of Akamai in making the internet faster, more reliable, and more secure — cloud services. Many enterprises, to provide services to consumers in a more efficient and cost-effective manner, have turned to third party cloud service providers for compute, storage, and networking services to supplement operations. The shift to the cloud, however, has brought its own performance, cost, and security challenges which Akamai, again, has risen to address. With its recent acquisition of Linode, a popular cloud services provider, Akamai has taken steps to integrate cloud storage and compute functionality into its highly distributed infrastructure.

The nature of services delivered via the internet today has become increasingly complex. Different use cases require different solutions in order to optimise the user experience. Some functions such as large databases benefit from centralised scalable infrastructure in the cloud, while other more real-time workflows such as image scaling and streaming can better be optimised at the edge closer to the consumer. Akamai addresses both of these use case types in one integrated platform, allowing its customers to focus on their services and trust Akamai with the global performance and security aspects of their cloud infrastructure.

Since its inception, Akamai has helped carriers and content providers deliver the fast, reliable, and secure internet experience that consumers need. Now, more than ever, Akamai's services play a vital role in ensuring that the internet is able to support the myriad users who depend upon it for work, school, health, and entertainment. Simply put, the internet would not function well without Akamai's services.

II. Overview of Akamai's Comments to Ofcom's Questions Regarding Traffic Management

The U.K. is currently a leader in network deployment, in part because existing market incentives have led to healthy industry norms. As Ofcom notes, competition among ISPs creates 'appropriate incentives [for ISPs] to make investments' such as 'capacity upgrades to ensure they can carry all their expected traffic at the busy hour . . . .'[1] ISPs and other entities in the internet value chain are also incentivised to collaborate on 'traffic and network planning . . . , particularly where any anticipated traffic events might result in congestion and have a material impact on the quality of experience of their respective customers.'[2] Akamai, for its part, deploys its CDNs deep within ISP networks, which effectively expands capacity by shifting portions of ISP traffic onto the CDN, to mitigate high traffic.

This current model has been stress tested by the unprecedented increase in internet traffic during the COVID-19 pandemic — and, as Ofcom observes, 'there has been a limited need for ISPs to manage traffic to address congestion or otherwise ensure robustness of their networks.'[3] Against this backdrop, Akamai (i) believes that there should be a strong presumption that the existing model is effective and (ii) cautions against any steps that may alter existing incentives that drive network planning by ISPs.

Akamai believes that many proposals discussed in the Consultation are not necessary to address any real or potential congestion issue — instead, they are likely to undermine existing incentives that support aggressive long-term capacity planning by ISPs. In doing so, Ofcom's attempt to mitigate theoretical future harms will likely create more problems than solutions for network deployment in the U.K. Below, Akamai provides an overview of its comments regarding Ofcom's proposed guidance on (a) retail offers with different quality levels, (b) traffic management, and (c) specialised services. While Akamai applauds and supports Ofcom's goal to mitigate future congestion issues in the U.K.'s network deployment, we believe the proposed traffic management guidance is unnecessary and likely counterproductive.

(a) Retail offers with different quality levels

In principle, Akamai agrees with Ofcom that retail offers with different quality of service levels (e.g., gold, silver, and bronze tiered services with respect to speed, latency, jitter, or

[1] Ofcom, *Net Neutrality Review* § 6.19.
[2] *Id.* § 6.20.
[3] *Id.* § 6.2.

packet loss) are permissible as long as three conditions are met. First, the choice must be up to the end user. Second, as noted in Annex 5, the quality of service must be 'independent of the content, applications and online services accessed.'[4] Tiering based on offers presented to content owners (e.g., all users gain unlimited access to Content Provider A but limited access subject to throttling or quota for Content Provider B) will stifle innovation and concentrate market power within a small group of well-resourced incumbent content providers. Third, ISPs must be held to strict transparency requirements to ensure that users are able to make informed decisions and compare offerings from different providers.

(b) Traffic management

(i) Guidance permitting ISPs to restrict certain categories of content

Guidance permitting ISPs to respond to high-traffic events by restricting certain categories of content will inevitably encourage ISPs to take the path of least resistance. Where today ISPs plan for high-traffic events through cross-industry collaboration and capacity upgrades, Ofcom's proposed guidance may encourage ISPs to respond to these events in the future by simply restricting categories of content — a more convenient and less costly measure. The U.K.'s network infrastructure may suffer as a consequence: fewer investments in capacity upgrades and a decrease in collaboration across the internet value chain can result in a network in which serious congestion is a more typical operating condition rather than the extreme rarity it is today.

Worse still, Ofcom should be cognisant of the risk that its rules can incentivise ISPs to be overly broad in their definitions of 'congestion' or even engineer it in certain parts of its network to the extent Ofcom offers ISPs more flexibility when their networks are congested. While ISPs should not be forced to expand capacity if links are not reaching a reasonable level of 'busy-hour' utilisation, they also should not be allowed to invite congestion by refusing to upgrade capacity. Certainly Ofcom should not reward them for doing so by granting them greater network-management flexibility when their networks become congested. In the past, ISPs in other markets have used this tactic to create leverage and force content owners and CDNs to purchase additional port capacity at unreasonable prices. By granting even more discretion to ISPs, this guidance may encourage them to take further advantage of their 'gatekeeper position . . . between their customers and the CAPs that want to deliver content and services to these customers' — the very scenario net neutrality rules seek to prevent.[5]

(ii) Guidance permitting ISPs to prioritise different categories of traffic

Guidance that would permit ISPs to prioritise different categories of traffic is also particularly concerning. ISPs would be in the position to make unilateral judgements about the value of different traffic classes (i.e., which traffic is time- or quality-sensitive), when these decisions should be left to users and their individual decisions about what content or data to consume. As the Consultation notes, ISPs currently do not have the capability to differentiate among different traffic classes,[6] much less to do it reliably. Permitting ISPs to prioritise different categories of traffic will threaten user privacy and materially impede innovation, investment, and growth in the internet that net neutrality rules were designed to promote.

Permitting ISPs to prioritise different categories of traffic may incentivise them to explore mechanisms for identifying different traffic classes to the detriment of U.K. internet users. For instance, if ISPs develop techniques such as deep packet inspection, user privacy

---

[4] *Id.* § A5.42.

[5] *Id.* § 6.5.

[6] *Id.* §§ 6.65, 6.79.

could be compromised since providers will — intentionally or not — gain new and unwelcome insights into their users' patterns of behaviour.

Additionally, this guidance may have harmful repercussions for digital competition more broadly. First, if ISPs are permitted to prioritise, or de-prioritise, traffic based on its content category, incumbent content providers, with greater resources and more robust industry connections, will inevitably be more effective in ensuring that their traffic is categorised in the most advantageous way. As a result, ISP's traffic management policies will create yet another competitive advantage for incumbent content providers.

Second, even if ISPs are allowed to implement a merely voluntary traffic classification program — such as a program where providers can voluntarily identify their content as real-time interactive video — large incumbent content providers will be better able to take advantage of these arrangements. New, independent providers will be left to navigate potentially complex classification programs from multiple ISPs on their own. As a result, even this form of voluntary classification program may further entrench the positions of large incumbent providers.

Third, a classification program will also ossify existing content categories at the expense of future technologies, thereby stifling innovation. For instance, although it may seem obvious today that latency-sensitive video conferencing traffic should be prioritised, we do not know what services might be created in the future that may be equally or more latency-sensitive. Thus, a program of traffic classification may make it harder for future technologies to flourish, since it will take time to properly prioritise them with respect to other traffic categories. This kind of scenario underscores the importance of leaving it up to the *users* what content they think is important. ISP content categories may be slow to change, but users express their own preferences in real-time by deciding what data to consume.

(iii) Alternative solutions to future congestion issues

In truly extraordinary events where congestion threatens to keep ISPs from delivering to users all the data that they have requested, some form of traffic management is unavoidable. But this should be neutral, without attempting to prioritise specific services or content categories. Akamai believes a better solution would be to encourage and reward distributed interconnection and/or deeper on-net caching to ensure that ISPs are providing fair access to their networks in major population centres.

As a recent report by Netflix/Analysys Mason[7] illustrates, ISP last mile costs are largely invariant with traffic volumes and most of the costs that scale with increased traffic are in the middle mile. Distributed interconnection and/or deeper on-net deployments have proven to be an effective technique to reduce the burden on ISP middle mile costs, and thus should be encouraged.

(c) Specialised services

If Ofcom allows different treatment of specialised services, it should clarify that these specialised services may constitute only a *de minimis* portion of an ISP's total network traffic. This should be more than adequate to allow appropriate treatment of traffic that truly needs it, while addressing the risk that this category of traffic — where ISPs enjoy greater flexibility — does not grow beyond what Ofcom intended.

---

[7] David Abecassis & Andrew Daly, *Netflix's Open Connect Program and Codec Optimisation Helped ISPs Save Over USD1 Billion Globally in 2021*, Analysys Mason (July 14, 2022), https://www.analysysmason.com/consulting-redirect/reports/netflix-open-connect/.

Traffic management

Question	Your response
Question 5: Do you agree with our assessment of retail offers with different quality levels and our proposed approach?	Confidential? – N Akamai agrees with Ofcom that retail offers with different quality of service levels (e.g., gold, silver, and bronze tiered services with respect to speed, latency, jitter, or packet loss) could be permissible as long as three conditions are met. First, the choice must be up to the end user. Second, as noted in Annex 5, the quality of service must be 'independent of the content, applications and online services accessed.'[8] If tiering is based on offers presented to content owners (e.g., all users gain unlimited access to Content Provider A but limited access subject to throttling or quota for Content Provider B), it could stifle innovation in the market and concentrate power to larger content providers that have more resources. Third, robust transparency measures should be implemented to ensure that users are able to make informed decisions about which plans to subscribe to, and to compare offerings between competing ISPs.
Question 6: Do you agree with the approach in our guidance in Annex 5 in relation to differentiated retail offers, including transparency requirements, improved regulatory monitoring and reporting of retail offers with different quality levels as well as the general quality of the internet access services?	*See response to Question 5*
Question 7: What are your views on a more permissive approach towards retail offers where different quality levels are content and service specific?	Akamai strongly opposes an approach that would permit different quality levels based on content and service. Such an approach would stifle innovation and concentrate power to larger content providers that have the resources to obtain preferential treatment and access to customers. A large content provider that can purchase preferential access for its content would be at a major competitive advantage against a new or small content provider with an innovative product that does not have the resources to purchase the highest speed. This proposed approach would constrain internet growth and give disproportionate pricing power to the largest content providers.

[8] Ofcom, *Net Neutrality Review* § A5.42.

Question 8: Do you agree with our assessment of how traffic management can be used to address congestion and our proposed approach?	Akamai disagrees with Ofcom's proposed approach of permitting ISPs to respond to high-traffic events by restricting certain categories of content. As discussed in our cover letter, the U.K. is currently a world leader in network deployment. Existing incentives within the U.K. market have led to healthy industry norms — competition among ISPs, for instance, incentivises them to invest regularly in 'capacity upgrades to ensure they can carry all their expected traffic at the busy hour ....'[9] Additionally, ISPs and other entities in the internet value chain are incentivised to collaborate on 'traffic and network planning ..., particularly where any anticipated traffic events might result in congestion and have a material impact on the quality of experience of their respective customers.'[10] This existing model has successfully managed the unprecedented increase in internet traffic during the COVID-19 pandemic. As such, Akamai (i) believes that there should be a strong presumption that the current model is effective and (ii) cautions against any steps that may alter the existing incentives that drive network planning by ISPs. Permitting ISPs to restrict certain categories of content in response to high-traffic events will likely undermine existing incentives that support aggressive long-term capacity planning by ISPs. ISPs will seek to address potential congestion in the most expeditious, lowest cost way: content restriction, rather than investment in capacity upgrades and collaboration with other players in the internet value chain. And the U.K.'s network infrastructure may suffer as a consequence: fewer investments in capacity upgrades and a decrease in collaboration across the internet value chain can result in a network in which serious congestion is a more typical operating condition rather than the extreme rarity it is today. Worse still, Ofcom should be cognisant of the risk that its rules can incentivise ISPs to be overly broad in their definitions of 'congestion' or even engineer it in certain parts of its network to the extent it offers ISPs more flexibility when their networks are congested. While ISPs should not be forced to expand capacity if links are not reaching a reasonable level of 'busy-hour' utilisation, they also should not be rewarded with greater flexibility because they failed to upgrade capacity. ISPs have used this tactic previously to create leverage and force content owners and CDNs to purchase additional port capacity at unreasonable prices. By granting even more discretion to ISPs, Ofcom's proposal may encourage them to take further advantage of their 'gatekeeper position . . . between their customers and the CAPs that want to deliver content and services to these customers' — the very scenario net neutrality rules seek to

[9] *Id.* § 6.19.
[10] *Id.* § 6.20.

	prevent.[11] Ofcom's attempt to mitigate theoretical future harms here will likely do more harm than good.
Question 9: Do you agree with the approach in our guidance in Annex 5 in relation to the use of traffic management to address congestion, including transparency requirements, improved regulatory monitoring and reporting of general network performance metrics, the use of traffic management and the impact on service quality?	As discussed in response to other questions, Akamai would not support guidance that would allow ISPs to manage congestion through content-based prioritisation. To the extent that Ofcom does authorise any such techniques, however, they should be accompanied by robust transparency requirements. This should include public notifications about when an ISP's network is congested and the categories of content that it deprioritised in order to manage this congestion. This will ensure that the public will be able to assess the frequency of congestion on an ISP's network and help users understand why their preferred content may have been delivered more slowly during a given period, enabling them to make informed market decisions.
Question 10: What are your views on a more focused approach to traffic management to address congestion?	Akamai disagrees with Ofcom's proposal to permit ISPs to prioritise different categories of traffic. ISPs would be in the position to make unilateral judgements about the value of different traffic classes (i.e., which traffic is time- or quality-sensitive), when these decisions should be left to users' individual choices about what content or data to consume. As the Consultation notes, ISPs currently do not have the capability to distinguish among traffic classes,[12] much less to do it reliably. Permitting ISPs to prioritise different categories of traffic will harm user privacy and materially impede innovation, investment, and growth in the internet that net neutrality rules were designed to promote. Permitting ISPs to prioritise different categories of traffic may incentivise them to explore mechanisms for identifying different traffic classes to the detriment of U.K. internet users. For instance, if ISPs develop techniques such as deep packet inspection, user privacy could be compromised since providers will — intentionally or not — gain new and unwelcome insights into their users' patterns of behaviour. Additionally, this guidance may have several repercussions for digital competition more broadly. First, incumbent content providers that have the resources to ensure that their traffic is categorised in the most advantageous way will inevitably be advantaged over new competitors. Second, even if content providers are permitted to merely opt-in to an ISP's voluntary traffic classification program, large incumbent content providers will be better able to take advantage of these arrangements. New, independent providers will be left to navigate potentially complex

[11] *Id.* § 6.5.
[12] *Id.* §§ 6.65, 6.79.

	classification programs from multiple ISPs on their own. As a result, a classification program may further entrench the positions of large incumbent providers. Third, a classification program will also ossify existing content categories at the expense of future categories, thereby stifling innovation. For instance, although it may seem obvious today that latency-sensitive video conferencing traffic should be prioritised, we do not know what services might be created in the future. Thus, a program of traffic classification may make it harder for future technologies to flourish, since it will take time to properly prioritise them with respect to other traffic categories. This kind of scenario underscores the importance of leaving it up to the *users* what content they think is important. ISP content categories may be slow to change, but users express their own preferences in real-time by deciding what data to consume. In truly extraordinary events where congestion threatens to keep ISPs from delivering to users all the data that they have requested, some form of traffic management is unavoidable. But this should be neutral, without attempting to prioritise specific services or content categories. Content-neutral network management techniques allow ISPs to manage congestion while respecting users' choices. A better solution would be to encourage and reward distributed interconnection and/or deeper on-net caching to ensure that ISPs are providing fair access to their networks in major population centres. As a recent report by Netflix/Analysys Mason[13] illustrates, ISP last mile costs are largely invariant with traffic volumes and most of the costs that scale with increased traffic are in the middle mile. Distributed interconnection and/or deeper on-net deployments have proven to be an effective technique to reduce the burden on ISP middle mile costs. Additionally, industry players should also work together to identify incentives to encourage end-users to time-shift traffic and content owners to opt for background delivery services that are pre-emptible.
Please provide any further evidence you have to support your responses.	

[13] David Abecassis & Andrew Daly, *Netflix's Open Connect Program and Codec Optimisation Helped ISPs Save Over USD1 Billion Globally in 2021*, Analysys Mason (July 14, 2022), https://www.analysysmason.com/consulting-redirect/reports/netflix-open-connect/.

Specialised services

Question	Your response
Question 11: Do you agree with our assessment of specialised services and our proposed approach?	Confidential? – N If Ofcom allows different treatment of specialised services, it should clarify that these specialised services may constitute only a *de minimis* portion of an ISP's total network traffic. This should be more than adequate to allow appropriate treatment of traffic that truly needs it, while addressing the risk that this category of traffic — where ISPs enjoy greater flexibility — does not grow beyond what Ofcom intended. It should also require ISPs to disclose which categories of specialised traffic it prioritises — both to users and to regulators — with specific justifications for this prioritisation. It should also require ISPs to periodically report what portion of its network traffic these services constitute.
Question 12: Do you agree with the approach in our guidance in Annex 5 in relation to specialised services, including transparency requirements, improved regulatory monitoring and reporting of the need for optimisation of a service, the general performance of internet access services and the impact of specialised services on the quality internet access?	See response to Question 11.
Please provide any further evidence you have to support your responses.	