
ENEA
Openwave
8 TRENDS THAT WILL SHAPE MOBILE DATA IN 2021
SPRING 2021
Telefónica
STRATEGY ANALYTICS
ABIresearch
TRUSTED INTELLIGENCE SINCE 1990
RootMetrics
By IHS Markit
TUTELA
analysys mason
AT&T

EXECUTIVE SUMMARY

Welcome to the 8 Trends That Will Shape Mobile Data in 2021. This book is an extension of the webinar held recently with an all-star panel including mobile operators, telecom vendors, and leading analysts.

To say that the past 12 months have been disruptive would be a colossal understatement! Disruption however isn't necessarily a bad thing. In telecommunications, it can be exactly what is needed to tip the scales from business-as-usual to next-gen innovation. As the world changes in the aftermath of Covid-19, network providers will continue to feel its lasting impact, but this provides opportunities as well as challenges.

Our panel identified 8 trends to impact almost every operator globally this year and we discuss them under four headings:

Continuing legacy of Covid-19

1 As a consequence of worldwide lockdowns a new mobile traffic phenomenon has emerged: the "7 day weekend". Demand for data has grown, all week long in suburban areas, while falling in traditional business districts. Facing a new reality, operators must re-plan network resources to deliver consistent Quality of Experience.

2 As lockdowns proliferated, the increase in devices coming online and the subsequent surge of information requires more effective data management. Learn from approaches that are being adopted in 5G core infrastructure (NSA and SA) for effective data management.

Cloud gaming on 5G

3 Cloud gaming will be a key use case in 2021/2022 as mobile gaming traffic grows 5X in 2021. Our panel highlighted how they expect the top use cases for 5G to be cloud gaming and group video calling (consumer), and private 5G (enterprise).

4 In 2021, the mobile gaming ecosystem will expand beyond the behemoths of Google, Microsoft, and Amazon to incorporate smaller independent gaming companies. Read how operators can place themselves at the heart of the gaming ecosystem.

Operator benchmarking / mobile user experience

5 2020 has changed how mobile operators are benchmarked. Operators now have to *consistently* manage new use case-based criteria in their quest to become #1 Carrier. Get expert tips from the world's leading specialists in operator benchmarking: Tutela and Rootmetrics.

6 And in 2020 customer expectation soared even more than expected. Operators will be blamed for poor user experience as consumers are becoming much more discerning about mobile connectivity and Wi-Fi during enforced home-working and home-schooling.

QUIC, new encryption… and a centralized internet?

7 QUIC has become the undisputed leader in transport protocols. This is impeding operators in classifying traffic and forcing the use of sophisticated heuristic and machine learning based approaches in order to manage network performance and subscriber QoE.

8 Meanwhile, hyperscalers could blind operators with new encryption protocols in late 2021 even before standards emerge. Ultimately, encryption could bring about a centralized internet where a few unregulated players hold all the keys. *How can operators respond?*

In addition to our core content this book includes the 4th Edition of our annual Mobile Video Index (MVI). This includes the latest charts and video data-trends that Enea has seen across our dashboard of over 40 mobile operators worldwide.

We trust you will find this year's extraordinary edition of the MVI along with our summary of data trends valuable as you seek to maximize the opportunities and overcome the challenges of 2021!

Many thanks to our contributors:

Tom Cannon
LEAD PRINCIPAL TECHNICAL ARCHITECT,
AT&T

Dr Diego Lopez
GLOBAL CTIO OFFICE,
TELEFONICA & ETSI NFV GROUP CHAIR

Kevin Hasley
CEO,
ROOTMETRICS

Chris Mills
HEAD OF INDUSTRY ANALYSIS,
TUTELA

Phil Kendall
EXEC RESEARCH DIRECTOR,
STRATEGY ANALYTICS

Dimitris Mavrakis
DIRECTOR,
ABI RESEARCH

Gorkem Yigit
SENIOR ANALYST,
ANALYSYS MASON

Indranil Chatterjee
CHIEF CUSTOMER OFFICER,
ENEA

Roland Steiner
SVP TELECOMS,
ENEA

Kishor Panpaliya
VP AMERICAS & APAC,
ENEA

Fergus Wills
DIRECTOR,
ENEA

Santiago Bouzas
DIRECTOR,
ENEA

1

THE CONTINUING LEGACY OF COVID ON MOBILE OPERATORS

Changing patterns of data traffic, new user behaviors and data management challenges present mobile operators with unprecedented disruption... and unparalleled opportunity

Contributions from

Telefónica STRATEGY ANALYTICS

Back to contents

The past is past - what of the future?

Much has been discussed and many reports written on the impacts of the worldwide pandemic on the telecoms industry.

This discussion, however, focuses on the future legacy of COVID on mobile operators through 2021, 2022 and beyond. It is not all negative. The disrupting effects of a pandemic on user behavior, 5G timescales, operator budgets, and cloudification in several cases are positive, or will be seen in hindsight to be positive even though they may appear painful right now.

A second positive is that the “distraction” afforded by COVID has generated a break in the race to deploy 5G. This pause in the race can be used to good effect if operators can take the time to fine tune current plans, and make more informed decisions on where their 5G priorities should now be.

With these in mind, this chapter provides “snapshots” on the lasting legacy of COVID. It does so from four perspectives: consumers, governments, device manufacturers and enterprises - before ending with a look at the state of 5G rollouts.

Consumers have radically changed what they do - and what they expect

The changes that have occurred in user behavior over the past year have been dramatic, and may be permanent. Home-working and schooling have generated the spikes in data we have grown used to seeing (and indeed reported elsewhere in this eBook). But it’s not just peaks in online voice and video, the very shape of data profiles have changed. Specifically, many operators now report a “7-day weekend” phenomenon where data has grown, 7 days a week in suburban areas, while falling in traditional business districts. And most people accept that Working From Home (WFH) represents a permanent shift in society, in fact the UK Government estimates that 2 million people who have been displaced from their offices during the pandemic will never return to the office.

The implications on our industry are far reaching and range from where operators deploy radio infrastructure to how employers ensure that workers enjoy secure fast connections.

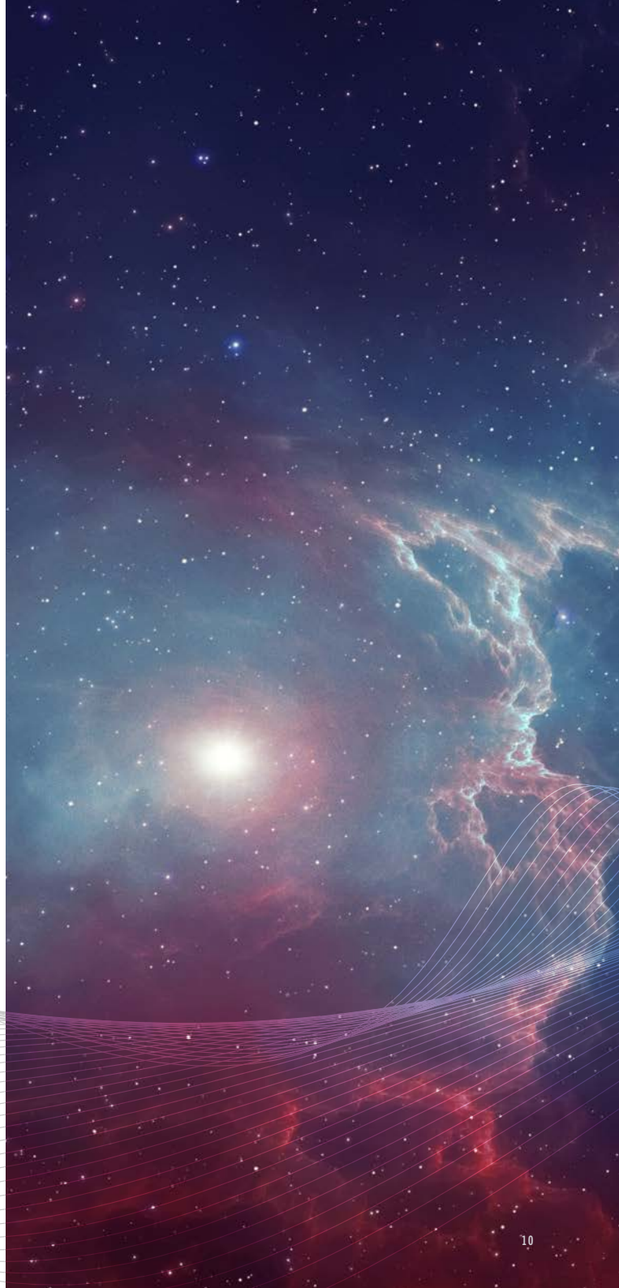
Employers worldwide should now consider how they self-facilitate WFH technically, culturally, and organizationally - and this goes far beyond issuing employees with a VPN. At the same time, for operators, moving traffic hotspots from the centers of our cities into suburban areas will continue to have a significant impact on traffic profiling.

And this rise in home usage has fueled a dramatic increase in knowledge when it comes to QoE. From the very young being schooled at home to the very elderly resorting to mobile video to stay in touch, to professionals getting familiar with workforce and collaboration tools from their homes, we see a much more educated userbase than ever before. These use cases completely expose the quality of the network experience.

In particular video has become the common yardstick with which to measure how good your connection is. Suddenly, video QoE (discussed in Chapter 3) matters, whether that is pixelation or buffering on Netflix, a work zoom meeting or a family video call. Consumers switching off their video to make their voices more clearly heard or switching from wireless to wired is now common practice even among non-technical audiences. These workarounds may be tolerated for now but users will quickly determine the providers who offer ‘laggy’ connections with buffering, and those who support a high video QoE. Video traffic management and acceleration solutions have never been as important as they are now.

> “Revenues are down but data consumption is up. A good analogy is the impact of lockdowns on the high street fueling unprecedented growth in online shopping - the opportunities are there!”

ENEA Openwave



Device manufacturers are catching up as network rollouts are slowing down

One interesting side-effect of the pandemic is that handset manufacturers have the opportunity to design and release 5G handsets “ahead of” network deployments. So the old excuse of “not enough handsets” is unlikely to work when it comes to 5G rollouts. In particular there has been a huge expansion in the number and range of affordable 5G phones at the bottom-end of the market - including a US$149 5G phone launched in China, and sub US$100 5G Chinese handsets expected in 2021. At the top-end, the iPhone 12 launch last year is opening up 5G as a mature proposition in the minds of consumers... “if Apple has a product then it must be a mature technology”.

Strategy Analytics estimate that there could be 750 million 5G devices sold by the end of 2021 even if they are not used on 5G networks for some time.

Governments are helping to restart the telecoms economy

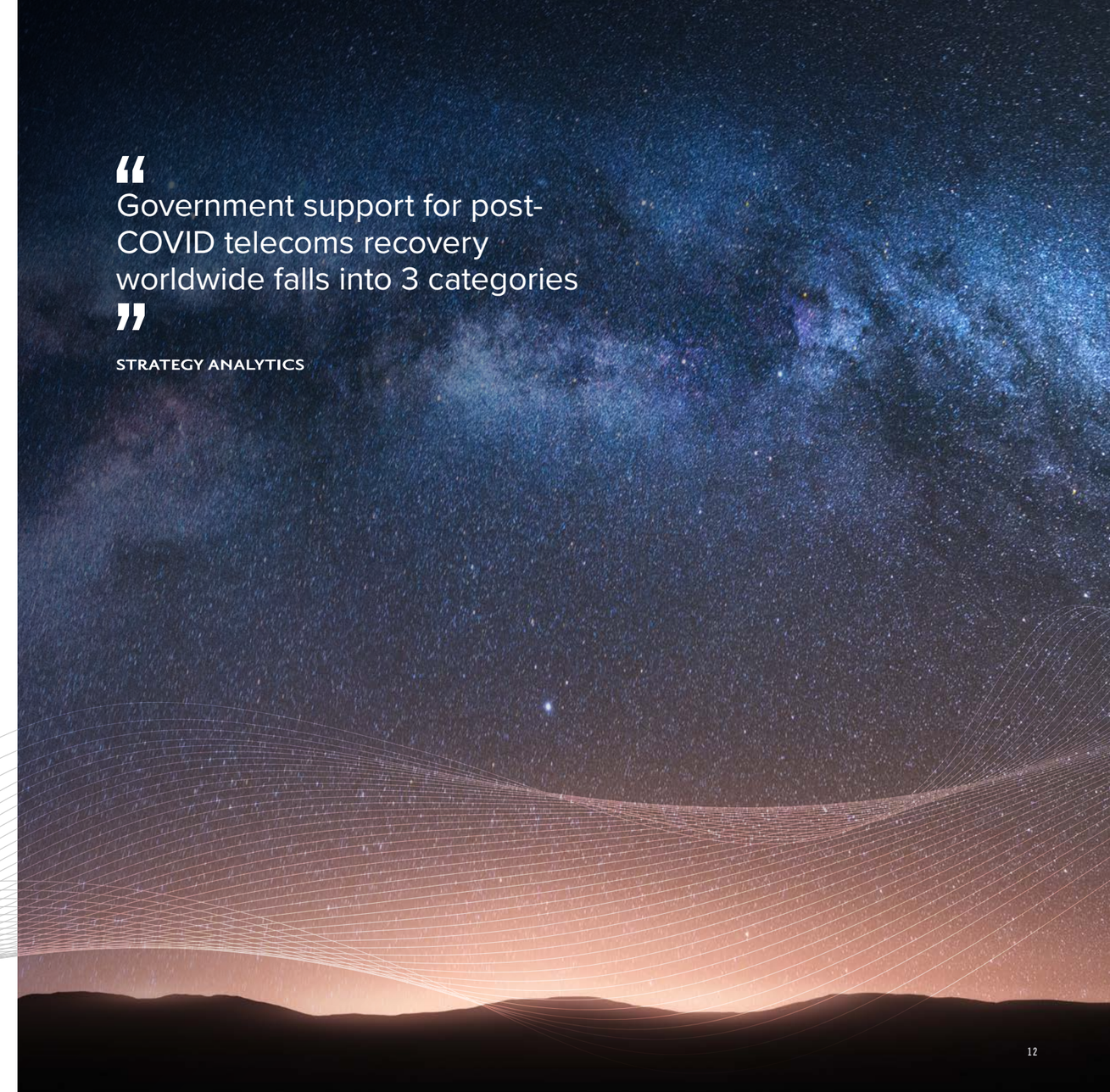
Globally governments appear keen to support the telecoms market, and we see three different categories of support.

Primarily in China, state-owned operators are under pressure and encouragement to drive an infrastructure-led recovery. New investment after all should stimulate employment and growth.

Secondly many more governments are offering “post COVID stimulus packages” which come in different guises but include eg The NextGenerationEU plan in Europe, or the Digital New Deal in South Korea. These programs aim to promote “build back better” propositions rather than throwing money at failing organizations. They aim to be future looking and include incentives for green initiatives.

Thirdly there are some initiatives targeted very specifically at enabling WFH practices, bridging the so-called “digital divide” and aimed at both fixed and wireless enabling a Gigabit society that will largely be WFH.

> “A US$149 5G handset has been released in China - an insanely low price point!”
>
> STRATEGY ANALYTICS



> “Government support for post-COVID telecoms recovery worldwide falls into 3 categories”
>
> STRATEGY ANALYTICS

Enterprises will adopt 5G for collaborative working

There is an increasing trend for enterprise to be connected to the mobile network including factories, warehouses, harbors, etc. In addition, these enterprises often have a need to collaborate - just in time manufacturing for example requires detailed and frequent interactions that go beyond simply sending an email. Generally, such organizations have their own network indoors but they want the advantages of becoming part of a “wider private network”, extending also to the global communication network, but retaining a degree of control and security in their communications. 5G offers this connectivity along with inherent security and privacy.

This federation of non-public networks, or “private 5G” is a key use case for operators, including enterprises that will require ultra-reliable, ultra low-latency and IoT connectivity, etc. It is a key use case not so much in handset volume but certainly in terms of operator focus, not least because these networks are inherently easier to monetize since they do not suffer from the sometimes absurdly low price points, we find in consumer markets.

And what about the trends of deploying 5G (SA and NSA) and data management?

Although there have certainly been delays in 5G deployments the truth is more nuanced.

The potential market for 5G deployments remains buoyant from an operator perspective. There have been commercial launches throughout the pandemic. However, a good number of these “5G deployments” are actually souped up 4G ie LTE but with 5G radio. This provides a capacity upgrade, a kind of intensification of 4G. Most operators prefer to call this simply “5G” for obvious reasons.

True standalone 5G SA is also on the rise but some way behind and partly driven by the need for ultra-high performance to support industrial use cases such as Private 5G, or consumer use cases like AR/VR and cloud gaming (all discussed in this eBook). Currently, 5G SA deployments tend to be limited to small islands and proofs of concept but this is an accelerating trend.

> “Federation of non-public networks, or Private 5G, remains the key enterprise use case for 5G”
>
> Telefónica

How will Data Management cope with all of this?

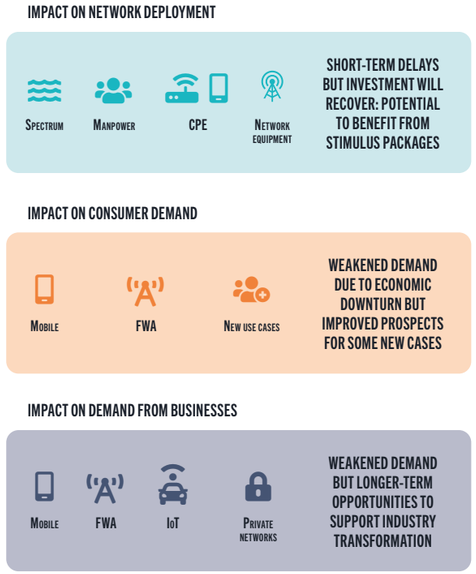
A McKinsey & Company report in 2020 found that enterprises digitized operations 20 to 25 times faster during COVID-19. As such, innovative use cases, new connected devices and the accelerated surge of digitalization requires more effective Subscriber Data Management (SDM) to strengthen the 5G core. Indeed, 5G subscribers could number in the billions, so, managing subscriber, profile, application and live session data should be a focal point for any CXO's strategic thinking in 2021. The alternative is a tsunami of unmanageable data and ground lost to Amazon, Google and Microsoft as OTTs continue to aggregate and monetize operator data.

The storage of much of this secure data is moving to the edge in cloud native data stores, and this is independent on whether it's SA/NSA. 3GPP 5G architecture is open and service based, and as such, it should be embraced by operators to maximize agility and avoid vendor lock-in. Services share data and can be combined based on open registration capability. Certainly, operators are now issuing SDM RFPs in this area at a faster rate.

The opportunities

The pandemic and lockdowns may have driven stock valuations down but data consumption is up and mobile communications is now recognized worldwide as a critical, essential, even emergency service. Fully exploiting a new post-pandemic world means overcoming barriers to innovation. Some of these barriers are technical - for example the reluctance of some to embrace cloudification - although those who experience true "cloud native" never want to go back to how things were since operations became so much easier. Other barriers are cultural and extend to regulators and technology providers - these are typically harder to overcome.

Although in times of uncertainty the instinctive reaction is always to "manage costs", forward thinking operators must overcome these barriers to discover the huge opportunity that always lies in the wake of disruption.



Supply-side and demand-side elements of 5G that are affected by the COVID-19 pandemic

Source: Analysys Mason

Watch the 15 Minute Microcast: The Continuing Legacy of COVID-19

Telefónica

Dr Diego Lopez
GLOBAL CTIO OFFICE,
TELEFONICA & ETSI NFV GROUP CHAIR

Dr Lopez is in charge of the Technology Exploration activities within the GCTIO Unit for Telefonica and also chairs the ETSI ISGs on Network Function Virtualization and Permissioned Distributed Ledgers.

STRATEGY ANALYTICS

Phil Kendall
EXEC RESEARCH DIRECTOR,
STRATEGY ANALYTICS

Phil provides support to leading telecoms operators, worldwide. He is a regular speaker and authors major reports on subjects including 5G go-to market, 5G use cases and business model development and Wi-Fi market evolution.

2

CLOUD GAMING ON 5G

Gaming is now a US$150 billion industry, larger than music or even movies. And, as with music and movies, the migration of gaming to mobile is inevitable.

Contributions from

AT&T

analysys mason

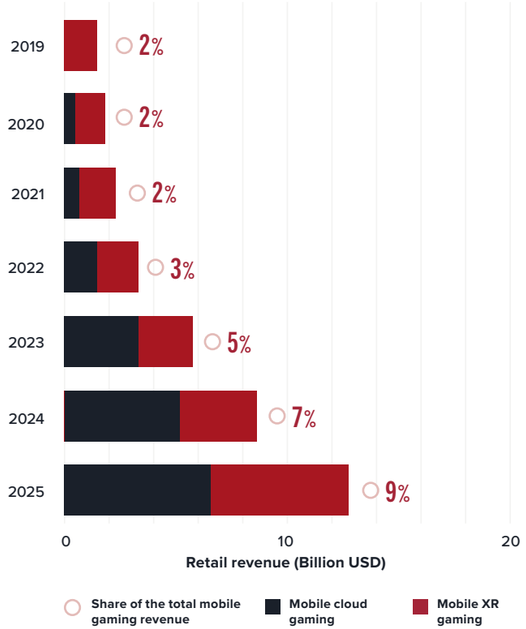
Back to contents

The market

Imagine... you're engrossed in a game of Minecraft on your console at home. You leave the house to go to work and "flip" the game seamlessly onto your 5G phone and continue playing during your commute. On arrival at the office you flip it once again onto your laptop and carry on gaming (while pretending to work, naturally!).

This "flipper use case" is key if cloud gaming on 5G is to take off. But it requires all kinds of technology, including near zero lag on a 5G connection, automatic video transcoding for different devices, seamless handovers between WiFi and mobile, and, almost certainly, edge computing. In this chapter we summarize some of the technologies involved and take a look at the evolving ecosystem. First, however, we provide a market snapshot.

We see the cloud take-up of gaming on 5G as a late 2021 or 2022 trend. Analysys Mason estimate that cloud gaming revenues will reach US$15 billion as early as 2025. But that means, as a mobile operator looking to get a piece of this pie, you need to get your strategy in place - now.



Digital gaming service revenue unlocked by 5G between 2020 and 2025

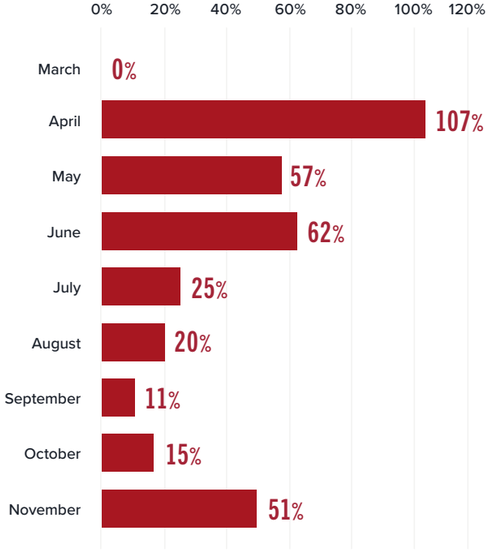
Digital gaming is the fastest growing segment of entertainment - 5G will widen its potential.

Source: Analysys Mason

Additionally, although gaming right now largely remains in people's homes, mobile networks have seen a knock-on effect as a result of the "COVID spikes", this is partly caused by mobile gamers which, according to AT&T and Analysys Mason, see no sign of significant dropping off post-pandemic. The accompanying chart illustrates the situation at just one of Enea Openwave's North American customers.

> "Cloud gaming is the most important consumer use case for 5G because it is directly associated with 5G's latency and throughput benefits"

analysys mason



Growth of mobile gaming traffic for sample operator North America 2020

Chart shows % CHANGE in contribution to mobile traffic of mobile gaming, with month 1 (pre-lockdown) taken as zero

Source: Enea Openwave worldwide deployments

The technology

Gamers hate lag! For hardcore gamers on a multiplayer game, network latency has to be down to 10ms or less, anything worse and you place the gamer at a competitive disadvantage - they will not forgive you! Such low latency may be achievable on 5G but there are many variables that affect it, including encoding/decoding and RAN congestion and, of course, moving to the cloud can create latency.

Additionally, with gaming in the cloud, there is a new factor: “input lag”. This is the time from pressing a button on a controller or a mouse, to it registering with the computer system or console which is now in the cloud. Both causes of lag (network lag and input lag) present operators with a challenge. Both need to be solved to prevent hinderance to the gaming experience.

One solution - much discussed over the past 12-24 months - is edge technology. Cloud gaming with its high sensitivity to latency and jitter makes it an ideal use case for the edge. By locating servers near end users and coupling them with 5G connectivity, the gaming experience can be improved significantly.

But there are other benefits that 5G is bringing to cloud gaming. For example, the core architecture of 5G enables the network to self-configure and expose API’s that allow third party gaming services to see current network metrics around latency and performance. This helps to modify the network so that it can provide a better experience for the gamer in real-time. Effectively, parameters such as location and network congestion can be communicated to trusted partners in the cloud gaming environment or the public cloud to adapt and create an optimum gaming environment. Operators such as AT&T are moving towards this type of dynamic network that adapts to optimize and enhance the user’s gaming experience.

> “AT&T are moving towards a dynamic self-configuring network that adapts to optimize and enhance the user’s gaming experience”

A final area of technology worth noting - and one where mobile operators already have a distinct advantage - is Mobile Identity. Mobile operators already have the systems in place to verify the identity of users instantly. Added to this, studies undertaken by Enea Openwave found that subscribers trust mobile operators to hold their identity data - surprisingly, at the same level of trust they have with their bank.

If the previously mentioned “flipper use case” is ever to become a reality, gamers must be able to move from platform to platform, device to device, without having to remember credentials or repeatedly sign in. Projects such as the carriers’ initiative Zenkey, supported by AT&T, Verizon and T-Mobile, are providing this single sign-on capability for mobile services including gaming.

A bonus of verified-identity is that it can also limit cheating. Cheating is in fact a significant “growth industry” with lucrative, albeit illicit, revenues. Cheating has the potential to undermine big-name gaming networks by rendering a game meaningless. With mobile operator verified-identity there is much more incentive for people to play fairly since their identity is known, ie they cannot so easily create a new identity with the same levels of achievements, and, conversely, they can be penalized by gaming organizers.

> “Sharing network metrics with our content partners will help us bring a better end-to-end experience that delights our gamers”
>
> AT&T

The ecosystem

The gaming ecosystem today comes down to a small number of big players. Principally, Nintendo (Wii and Switch), Sony (PlayStation), the OTTs including Microsoft (Xbox), and relative newcomer Google (Stadia). Then there are cloud players such as Amazon and of course the game publishers. But like many fledgling industries, as gaming moves to encompass mobile, it is starting to open up to smaller players who bring greater innovation at increased pace.

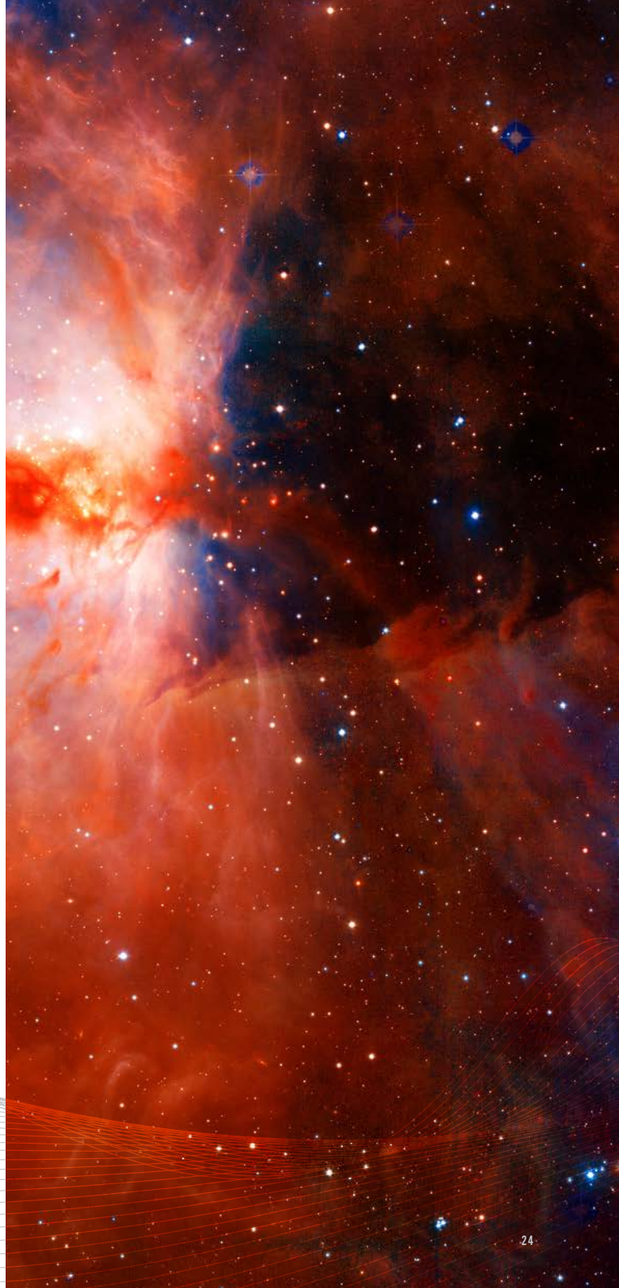
One way operators are enabling smaller players is to open up their edge networks and their infrastructures to allow them to deploy game servers within the operator infrastructure. This new development could be a crucial move to enable heightened performance. The parallel path for operators which we are also seeing is to create industry alliances with other operators and gaming providers to offer a unified developer framework so that developers don't need to create different versions of a game for each operator.

Mobile gaming ecosystem - The 3 C's

Ultimately - as with movies and music - the bulk of the money is in the content and we see evidence of this. For example Microsoft's Xbox strategy is now less about selling consoles and much more about selling its Netflix-like subscription service for games, Xbox Game Pass, for multi-platform gameplay. Similarly, Sony, although a game publisher themselves, are increasing their vertical integration through acquisitions. Content owners are also increasing their direct relationship with customers through offerings such as EA Play, and Ubisoft Connect.

And gamers ultimately are loyal to the game - they will follow a game rather than say a console manufacturer or mobile operator. So once games are "cloudified" users are free to abandon specific gaming devices. In that case the specific console manufacturer (or mobile operator) could be no more relevant than the fact that Samsung or Panasonic manufactured your TV... you don't care, you just want to play Call of Duty.

Many mobile operators already wise to this have started to align themselves closely with gaming providers. Just one example of this is SK Telecom Vodafone and T-Mobile partnering with Microsoft on Project xCloud, Microsoft's cloud gaming service. Such partnerships involve testing of APIs and delivery of QoE. Partnering is also taking place between cloud providers and operators for edge computing as mentioned previously.



The journey ahead

Cloud gaming is a gold rush about to happen, but, given that the greatest monetizable value remains in the game, what role can the mobile operator play to avoid becoming “a pipe”, necessary yet also somehow irrelevant?

In fact, mobile operators have an opportunity to position themselves as providers of “specialist mining equipment” in this gold rush.

- The unique value that forward thinking operators could bring lies firstly in the fact that their APIs allow for the network to adapt. For those operators who can do it, the creation of an adaptive or self-configuring mobile network that adapts depending on factors such as location or network congestion brings a competitive edge.
- Secondly, the concept of Mobile Identity is truly a unique, we could say game-changing, advantage that operators possess.
- And thirdly of course the connectivity. Connectivity - including intelligent deployment of edge technology alongside 5G - will make or break mobile cloud gaming because of the diverse and extreme performance requirements.

It is by combining these unique advantages with commercial alliances that operators can succeed commercially and simultaneously delight their users.

Watch the 15 Minute Microcast: Cloud Gaming on 5G now

AT&T

Tom Cannon
LEAD PRINCIPAL TECHNICAL ARCHITECT AT&T

Tom is Lead Principal Technical Architect at AT&T, with significant experience in high pressure, mission critical, environments. He has a focus on mobile technologies, internet applications, API’s, virtualization, gaming and cloud computing.

analysys mason

Gorkem Yigit
SENIOR ANALYST, ANALYSYS MASON

Gorkem is the lead analyst for Analysys Mason’s Service Delivery Platforms program and a key contributor to the Software-Controlled Networking and Network Orchestration programs, focusing on producing market share, forecast and research collateral.

3

USER EXPERIENCE AND OPERATOR BENCHMARKING

Enea brings together the world's leading operator benchmarking companies to discuss Quality of Experience (QoE) and benchmarking, especially for mobile video

Contributions from

RootMetrics® By IHS Markit

TUTELA

Back to contents

The mobile user experience

QoE is a topic which can be scientific and objective but is also intangible and rather subjective.

One of the key experiences subscribers will use to gauge quality is mobile video calling - especially during the last 12 months' "Zoom boom" as video calls skyrocketed. Video calls became a daily ritual for millions and many were forced to use it for the first time. Indeed, phrases such as "You're on mute!" and "Can you see me? I can't see you." have now entered our common vocabulary. But when it comes to viewing video on mobile, QoE is in fact a combination of several factors:

1. **Quality of Delivery** - including buffering or waiting for the video to begin and stuttering once the video begins to play.
2. **Quality of Picture** - low definition, high definition, etc.

For most consumers, the most important factor here is Quality of Delivery - QoD. There is evidence of this from consumer surveys undertaken by Enea Openwave: on mobile people prefer a video that starts quickly and plays smoothly rather than a HD experience.

However, of course Quality of Picture (QoP) DOES matter depending on the content being viewed. Watching a football (soccer) game becomes a pointless experience if you cannot track a fast-moving ball, even if it is buffer free. This is the case for all sporting or high-motion events - and of course these are also occasions at which mobile usage can soar. So the definition, whether that be low, standard or high, can matter as much as the extent of buffering.

Then - just to add complication - there is one further factor that contributes towards QoE:

3. User Perception

This is the non-scientific factor of user experience - but arguably it is the most important one of all, since, if users *believe* they get a great experience, the reality is almost irrelevant. This is partly why operator ranking and benchmarking is so important - it provides marketing as well as bench-marking. Being ranked "number 1 fastest network" gives huge marketing advantage in the retail storefront of any operator, while being number 3 or 4 has the opposite effect.

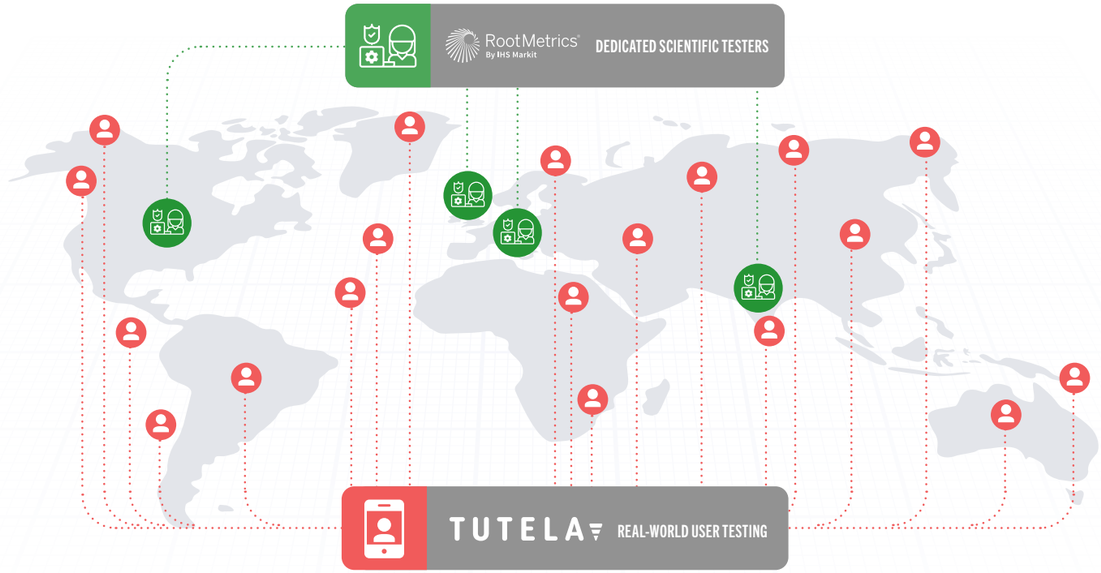
How operator benchmarking is performed - a summary

World leading independent benchmarking organizations Tutela and RootMetrics regularly test and rank mobile operators against each other within a country. There is no standardization in the area of operator ranking / benchmarking. Each ranking organization has their own approach.

For example, Chris Mills at Tutela summarizes their methodology: "our focus is on end-to-end real-world experience. We use crowd sourcing and partner with thousands of consumer applications to collect data from real-world users using a variety of devices, and we test against the most frequently used content delivery networks". Tutela's crowd-sourced approach has a real world feel to it.

But RootMetrics employs a very different approach. Kevin Hasley of RootMetrics: "we operate with our own people and our own scientific team with off-the-shelf handsets that every consumer uses. We add our proprietary software and collect the data. We randomize the locations throughout the market to make sure we don't introduce any bias in our data results and we include tests for latency, jitter and packet loss". So, the RootMetrics approach focuses on a small but well-controlled set of lab-based tests, run by experts, with a scientific base.

Clearly the two approaches both have merit - but clearly, they are also *vastly different.*



Operator benchmarking: contrasting approaches, identical goal

Has benchmarking been affected by changing trends?

Both organizations have observed to greater and lesser extents a number of trends that ultimately can affect the way operators are ranked. These include:

- The adoption of group video-calling - from an occasional use case to one which millions are now dependent on every day for home and school working. A second use case around mobile video is the rise of “watch parties” where people gather remotely to watch a Netflix, Disney+ or Amazon Prime etc new release at the same time. Both present very demanding use cases to operators.
- The rollout of 5G. Many networks in 2020 either had their first launches, or ramped up their 5G deployments, and of course there are more 5G devices available. The consequence is that some operators have taken major steps forward in terms of network quality.
- An increasing move towards mobile gaming (see Chapter 2).
- Increased use of mobile data as a backup or even replacement for conventional fixed broadband.
- Increasing intolerance from users to accept poor data quality and an increasing willingness to churn.

Although these trends do not fundamentally alter the way benchmarking is carried out, they have helped to drive a change within benchmarking. There is now a move towards testing which is firstly more use-case based and secondly, focused on consistency and repeatability of experience. Consistency of experience has soared in importance. For example, a valid question posed in benchmarking now could be how often does the network enable a group HD video call? Or does the network enable *repeated successful* attempts to perform cloud gaming at “low latency”?

These are difficult questions to pose scientifically and also for networks to handle consistently. In effect, benchmarking has gone beyond the measurement of simple parameters to ask: does this network support a use case and does it support it repeatedly?

One further “trend” in the past 12 months, not initiated by users or operators, was legislation or “strong recommendations” from bodies to restrict the resolution of commercial streamed video content to SD, rather than HD. This was introduced to reduce congestion on both wireless and wired networks.

This was a change in the default settings within devices to play SD rather than HD video, but in most cases it still allowed users to switch to HD if they chose. Although this was a temporary measure put in place for exceptional mobile traffic due to COVID-19, this is a tool that operators could use for example in developing countries, or if a hugely popular event such as the Olympics took place with millions of tourists arriving armed with mobile devices to temporarily mitigate the total data-load.

“In the last year, we’ve definitely added more measures of reliability and consistency into our metrics”

TUTELA

Video quality metrics

What specific parameters do benchmarking companies look at when measuring quality of video (QoD or QoP)?

Both organizations stream videos from content delivery networks like Netflix, YouTube and Facebook and collect data points regarding the performance of that video streaming experience including - how long did the video take to buffer and did playback stall at any point, etc?

Most tests utilize an adaptive bit-rate scenario ie where the network connection determines the quality (resolution) and the bit-rate of the video that a user receives. The video player adjusts the quality, varying this from say 180p to 360p to 720p depending on the quality of connection. Effectively, the QoP is being managed.

QoD parameters measured include bit rate, latency, packet loss, and “consistency of playback”. The latter measurement is based on a formula with 2 inputs:

a. The number of times a video stops to buffer with more tolerance given to long form videos over short form

b. For short videos, the length of time that the video takes to begin playback

Benchmarking organizations do not examine usability parameters such as video watch times, on the grounds that this would be an invasion of privacy.

> “Successive surveys we have performed demonstrate that users will switch carrier services, or video services, when they don’t get the experience they expect”

RootMetrics
By IHS Markit

Concluding words

Ultimately, to achieve top marks from benchmarking organizations operators need to be able to ensure consistency of experience for use cases that are becoming ever more complex. That is no easy matter when it comes down to the ability of radio networks to perform predictably. And of course, although we have focused only on data, being “#1 network” is also about voice and texting - ie all the aspects of the network matter.

On video QoE we can be a little more specific. Although QoD, QoP, and user perception appear to be disconnected goals, in fact, there are some simple conclusions that can be drawn.

- QoP (mainly resolution) is important, especially in fast-moving / sports videos, but once it becomes acceptable on a mobile device (a visible fast-moving football), it becomes a “soft KPI” and there is no added value to further improving it.
- QoD on the other hand always matters, but even then, once QoD is perceived to have reached an acceptable level, it also drops in importance.

These are simple yet important points because, for example, High Definition (HD) requires 3 - 4 times more bandwidth than SD, and of course there are handsets now commonly offering 8K video. Setting KPIs around such a subjective area is not easy, but it can be done - QoP and QoD can be traded off when improving overall QoE. Added to that, we see that reducing resolution of video did not generate any significant backlash from users during the COVID-19 traffic peaks, and this may be useful to operators who want to effectively manage peaks on the network, for example during important sporting events.

Watch the 15 Minute Microcast: User Experience and Operator Benchmarking now

RootMetrics
By IHS Markit

Kevin Hasley
CEO,
ROOTMETRICS

With more than three decades of experience in the mobile and telecommunications industry, Kevin leads RootMetrics Performance Benchmarking within IHS Markit. Its real-world measurement and benchmarking insights help customers gain a competitive advantage.

TUTELA

Chris Mills
HEAD OF INDUSTRY ANALYSIS,
TUTELA

Chris Mills is the Head of Industry Analysis at Tutela, a crowdsourced mobile data company. At Tutela, Chris leads the analysis of emerging and established wireless networks around the globe, using crowdsourced network quality data to answer the most pressing questions for leading telecoms industry players.

4

QUIC, NEW ENCRYPTION … AND A CENTRALIZED INTERNET?

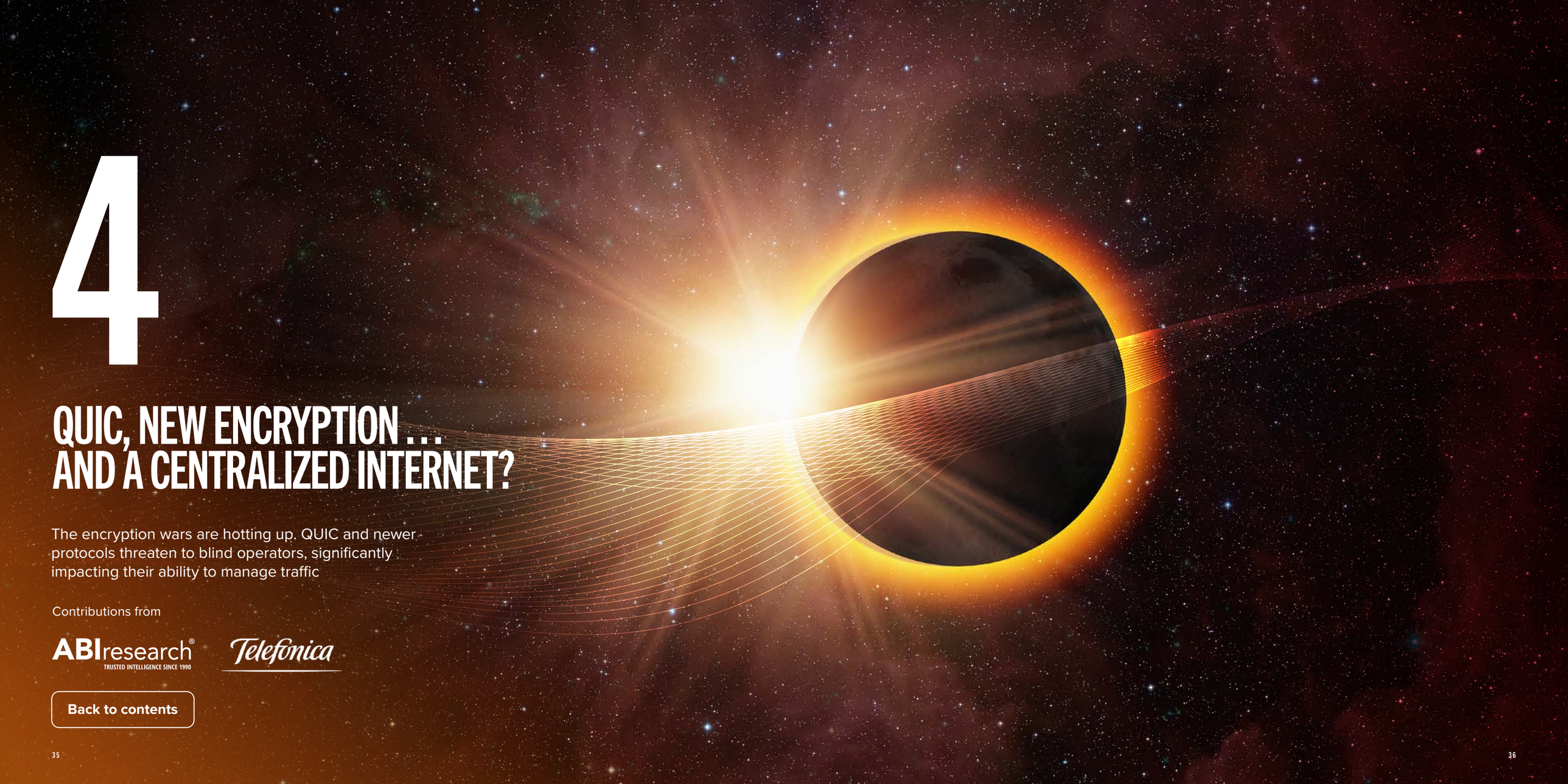
The encryption wars are hotting up. QUIC and newer protocols threaten to blind operators, significantly impacting their ability to manage traffic

Contributions from

ABIresearch® TRUSTED INTELLIGENCE SINCE 1990

Telefónica

Back to contents



“Encryption 2.0”

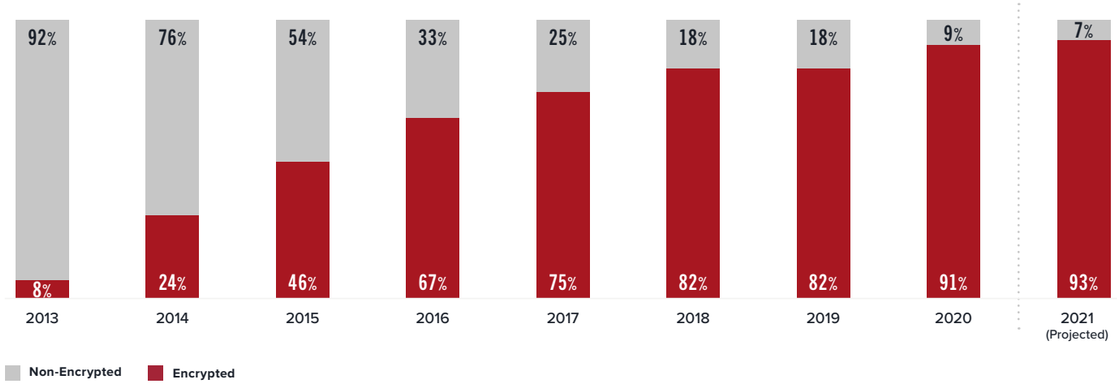
Most people are familiar with the rapid advance of encryption in mobile networks over recent years.

Within a short space of time, HTTPS became the norm and the internet “went dark” driven partly by security concerns and partly by the agendas of OTT content providers. Today over 90% of traffic on mobile networks is encrypted (see accompanying chart - Appendix 1 contains further data analysis on encryption).

However, mobile operators responded and were able to adopt HTTPS traffic management technologies that allowed them to continue to add value to end users. Although the content of data packets became invisible, the destination , via a field called “Server Name Indication” or SNI, was still accessible. The availability of the destination meant that services based on packet inspection and classification, such as content filtering, parental controls and video optimization, could still be offered.

There is now a far greater depth of encryption emerging via the Internet Engineering Task Force (IETF) and driven by industry players including hyperscalers and Operating System (OS) & browser vendors, along with Domain Name Server (DNS) solution providers. They offer users an even higher degree of privacy, but once again they threaten to impede the operator’s ability to manage traffic and perform essential value-added services such as parental controls. This time both the content and the destination of data packets will become inaccessible to mobile operators. For an introduction to these specifications, see the inset.

> “Let’s not kid ourselves. Hyperscalers don’t wait for standards to appear”
>
> ABIresearch
> TRUSTED INTELLIGENCE SINCE 1990



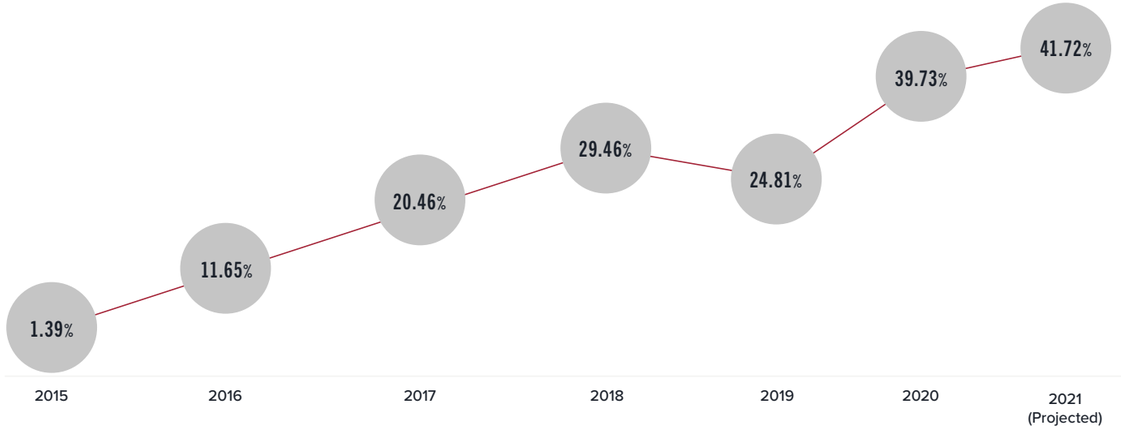
Mobile data traffic by encryption

The spectacular rise of QUIC (see also the Appendix)

Google introduced QUIC back in 2013 as an experimental protocol to improve the performance and efficiency of transport layer protocols. Since then, the default adoption of UDP and QUIC by Google and the IETF standardization process around QUIC and HTTP/3 has also persuaded other content providers, such as Facebook, to consider replacing HTTPS over TCP by HTTP over QUIC, using UDP at the transport layer.

As of January 2021 QUIC, (in both Google and IETF-implementations), boosts UDP as the default transport protocol for close to 40% of mobile internet traffic, to the detriment of TCP. Managing QUIC delivery performance and subscriber QoE has become critical for Mobile Operators, who need to look now at extending their TCP optimization and acceleration systems to manage UDP traffic.

Although QUIC enhancements do help improve performance, they also create new challenges for mobile operators to properly identify traffic and preserve QoE. The most recent developments include a major transition of Google services and applications to their latest QUIC version (Q050), which has many similarities with IETF QUIC. In addition, since October 2020, Facebook replaced TCP (and all previous initiatives such as FB Zero) with their own implementation of IETF’s QUIC, known as *mvfst*. Both Q050 and *mvfst* introduce obfuscation mechanisms that prevent existing network elements from deriving information about the content that is being accessed, requiring now more sophisticated heuristics and machine learning based controls for operators to supervise network performance and subscriber QoE.



Growth of QUIC

The reasons for the rise are explained in the following section.

Timing and political considerations

Although the IETF specifications are still emerging, large hyperscalers are not waiting for standards to appear, and deployment of these new encryption techniques has already begun. Encrypted Client Hello (ECH) and Encrypted SNI (eSNI) only becomes possible with TLS 1.3, so wide adoption is not anticipated until mid-2022, but organizations such as CloudFlare (CDN), and Firefox browsers already offer the option of eSNI. DoH, although used by ECH/eSNI, has no dependency on TLS and adoption will occur sooner. In fact, Google introduced DoH into Chrome in 2020. Currently it is an optional setting, and most users will not have heard of it, let alone enable it, but that will certainly change over time. And it's not just Google. Apple's iOS 14 and macOS 11, Windows 10, and Ubuntu 18.04 already support some form of DoH, as do Microsoft Edge and Firefox browsers. In short, it's already started.

Although it may seem that the internet behemoths will drive support for DoH, DoT and ECH/eSNI, there are political and even ideological issues when it comes to its implementation across geographies which are slowing this trend down.

Some countries (eg China and Russia) at the time of writing have banned DoH/eSNI, while others in North America and Europe are trying to work with the industry to better understand the impact. Eg the UK has reached out to vendors to not enable DoH by default, and some cable companies and telecommunications industry groups in the US such as Comcast are lobbying against such deep encryption.

Could this lead to a "centralized internet"?

As well as national governments, law enforcement agencies and judicial systems worldwide are taking an interest in developments. In most countries the enforcement of laws to protect children from inappropriate content or for crime prevention and detection increasingly depends on identifying domain names. This makes it relatively straightforward to decide what content is permissible.

Deep encryption not only makes this difficult but tends to generate a centralization of authority within the internet. A few players determine what can be seen, who can see it, what value added services can be provided, and who can provide them.

Such a model goes against the spirit of the internet which was always intended to be a decentralized way of sharing information. Indeed, veterans such as Tim Berners-Lee now argue that we need to return to a decentralized model where individuals determine the

IN SUMMARY:

The new encryption protocols and who's driving them

Over 90% of mobile network traffic is now encrypted. This ensures that the communication between two end points is secure and no bad actor can see or modify it. However, there is a loophole which allows some level of inspection. In the Client Hello message of a TLS handshake, one can look at an extension called Server Name Indication (SNI) and identify the domain name which is in plaintext. Though the connection and data transfer afterwards remains encrypted, information on domain name can be used to enable use cases around cybersecurity, deep packet inspection, content filtering and parental control, video optimization etc. However, the same loophole can also be exploited by bad actors in the system for malware and phishing attacks etc.

> "If this sounds alarmist, remember that HTTPS encryption on mobile networks went from zero to over two thirds of traffic in less than 3 years"
>
> ENEA Openwave

level of privacy they desire, have access to their own data and understand where their data is being used.

It is not even clear whether users actually want additional encryption. On the one hand users have the right to expect their communications to remain private and untampered. But on the other hand, hyperscalers increasingly dictate the entire content delivery chain. For example, take Google/Android: it is now almost impossible to use an Android phone without Google services. Google host the applications, create the developer communities and are even deploying their own networks.

As another example, Facebook has a mandatory update to WhatsApp to enable the application to share user data with Facebook to enhance advertising and personalization. The authority that a few players get to exercise is increasing and if we add deep encryption to the mix, in some people's eyes it could become total control.

This level of control is driven by their business model. Of course, the business models of Google, Amazon, Facebook etc are advertising based. They are perfectly legal but benefit greatly from "control" of user data flows. Ultimately, they are answerable to their shareholders and the pressure on them to deliver increased profits quarter after quarter is enormous. When advertisers under pressure to perform are also managing the end user's privacy - that has to be a conflict of interest.

The argument for regulating big-tech hyperscalers remains strong - why should they not be regulated since operators are heavily regulated? On the other hand of course big-tech has deep pockets and huge influence. It is hoped that long before entering the courts, there would be cross industry dialogue.

Despite these concerns and possible delays, our estimate is that DoH will become mainstream around the middle of 2021, while SNI encryption, possibly in the form of ECH, will take another year or so for mass adoption. If this sounds alarmist, remember that HTTPS encryption on mobile data networks went from almost zero to over two thirds of traffic in less than 3 years. Once these trends begin – and are backed by the hyperscalers- they quickly become a runaway train.

> "Such a model seems to be completely against the original spirit of the internet"
>
> Telefónica

Don't be blind-sided

Operators need to prepare for a new phase when data traffic once again becomes dark potentially rendering services useless including current traffic filtering, parental control, and video acceleration. Relying on geo-political events to reduce or limit the impact of second-generation encryption protocols is a high-risk strategy. So, what are the options?

Step 1

DoH will impact all traffic filtering solutions that rely on DNS inspection / classification - and there are many such solutions currently in use. All of these will be rendered ineffective since these solutions will simply not be able to view the details within a DNS flow. Solutions that perform "in-line" inspection however will not be impacted by DoH. So step-1 is: ensure you employ inline inspection traffic management. But that, alone, is insufficient.

Step 2

Extensive rollout of SNI encryption will impact ALL exiting traffic classification and filtering solutions and render them obsolete. No traffic management services offered today will work. Although this situation is unlikely to arise before mid-2022 it makes sense to ensure now that your vendor's roadmap includes a convincing solution for tracking these events.

As a mobile operator, your traffic classification-based services - including optimization, content filtering, and protecting minors - and ultimately your reputation, depend on getting this right.

Watch the 15 Minute Microcast on New Encryption Protocols

Telefónica

Dr Diego Lopez
GLOBAL CTIO OFFICE,
TELEFONICA & ETSI NFV GROUP CHAIR

Dr Lopez is in charge of the Technology Exploration activities within the GCTIO Unit for Telefonica and also chairs the ETSI ISGs on Network Function Virtualization.

ABIresearch
TRUSTED INTELLIGENCE SINCE 1990

Dimitris Mavrakis
DIRECTOR, ABI RESEARCH

Dimitris manages ABI Research's telco network coverage, including telco cloud platforms, digital transformation, and mobile network infrastructure.

IN SUMMARY:

Encrypted SNI (eSNI) and Encrypted Client Hello (ECH)

To address this loophole, IETF is working on TLS 1.3 extensions that include the encryption of the SNI (eSNI) and more recently, an update to the eSNI draft to consider encrypting the entire Client Hello (ECH). This will ensure that the target domain information is not visible in the TLS handshake.

Although this is a good step towards protecting the privacy of users, it presents challenges for regulatory authorities, mobile network operators and network security solution vendors in terms of preventing access to harmful and adult content for minors, preventing cyber-attacks etc. Some of these can be overcome by intercepting plaintext DNS requests that include intended domain names. This means SNI encryption does not ensure full privacy unless DNS queries are also encrypted.

DNS over HTTPS (DoH) and DNS over TLS (DoT)

In addition to the above, IETF has published a document that defines the DoH protocol for sending DNS queries and responses over HTTP and TLS (HTTPS). To be widely adopted, DoH will require support from the OS/app/browser ecosystem as well as DNS servers. This is already happening: Apple's iOS 14 and macOS 11, Windows 10, and Ubuntu 18.04 already support DoH; Microsoft Edge, Chrome and Firefox browsers have also introduced support for enabling DoH; and Cloudflare and Google are many of the public DNS resolvers supporting DoH.

5

WHERE TO NEXT?

Most mobile operators faced great adversity over the past year and yet remained resilient and steadfast

Back to contents

That was mainly down to dynamic workforce, innovation, and agility when it came to delivering connectivity. Thanks to telecom operators' pivotal role in delivering connectivity, a World Bank International Finance Corporation report found that telecom operators globally performed better on the S&P 500 when compared to other industries impacted by the pandemic.

However, a separate report from Deloitte sounds a warning bell that some operators may face revenue issues in the long term - and this year's Mobile Video Index identified a number of storm clouds on the horizon that operators must heed. One particularly ominous cloud – excuse the pun - are the cloud-native hyperscalers. Hyperscalers have shown their mastery of monetizing data - a key ingredient on every successful operator network. And as this book has highlighted, hyperscalers have made major inroads and are fortifying their presence in telecoms.

- After lockdowns were introduced, the volume of video traffic from the likes of Netflix and YouTube has surged. Along with this flood of traffic has come blinding encryption
- In encryption, the hyperscalers are not only forcing extensive deployment of QUIC but also introducing new encryption protocols eveh before standards for the latter are agreed. These could shroud networks in darkness, blighting user experience.
- As the likes of Microsoft Teams, Zoom and Google Meet become commonplace for consumers, any buffering or poor user experience is blamed on the operator
- And in cloud gaming, some of the largest technology firms have control over the gaming ecosystem - and can decide who can enter or leave - this multibillion-dollar industry

It is easy to just focus on the essential day-to-day activities of delivering connectivity and fail to focus on the long-term impacts or threats. There is quite rightly an unrelenting drive to set up and launch 5G networks, but nonetheless there are key hotspots that need additional focus - as this book has highlighted.

Disruption is the new normal

As the hyperscalers have amply demonstrated, disruption is the new normal. Now is not the time for operators to sit on their laurels and tune out of critical issues that will impact the industry well after the pandemic. Now is the time for action.

6

APPENDIX

THE MOBILE VIDEO INDEX 2021

Based on live data from over 40 mobile operators, worldwide

Back to contents

Impacts of the pandemic on mobile data

Much has been written on the harrowing effects of COVID-19 on individuals, businesses, and economies. As experts in traffic management, and with a widely deployed base across many countries, we performed our own analysis of mobile data consumption trends in 2020 and with a particular focus on mobile video. Here are some snippets from our analysis.

Streaming Video: significant rise in consumption during lockdowns

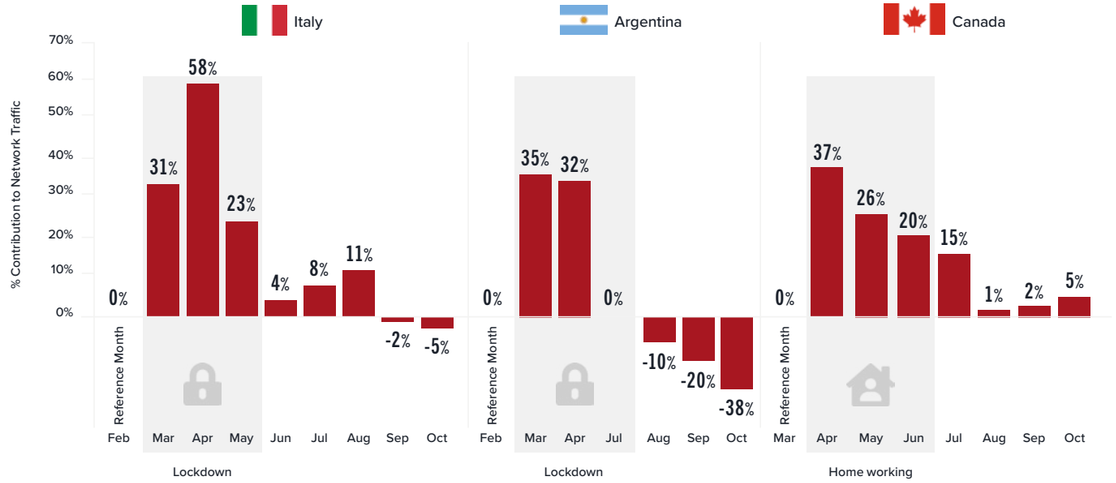
We identified a common pattern. With the month before the first national lockdown in that country considered as the benchmark ("zero" in the chart below), subsequent months witnessed a sharp rise in Netflix traffic during the lockdown. For example, in Italy and Argentina, the first lockdown was imposed in early March and lasted until mid-May. In Canada, a national lockdown was not imposed but people restricted their movement by working from home. The resulting Netflix consumption trend in mobile data can be seen below.

Consequential rises in the Middle East and North America

In Egypt stringent measures were implemented from early March until May. If we consider the YouTube traffic contribution in February as the benchmark ("zero"), there was a consistent increase from March to July.

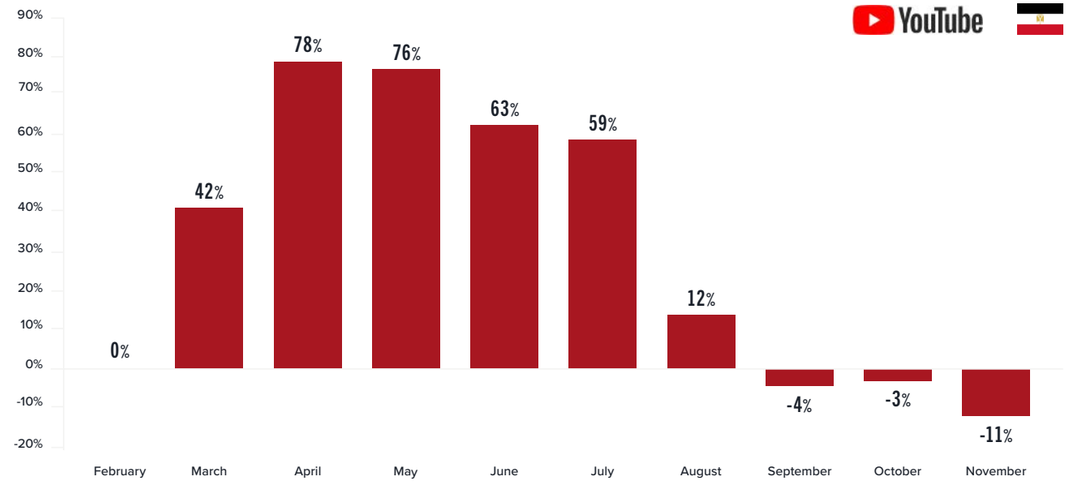
Relative Change in NETFLIX traffic during lockdowns 2020

Chart shows the % contribution to mobile data traffic of NETFLIX - with month 1 (pre-lockdown) taken as zero

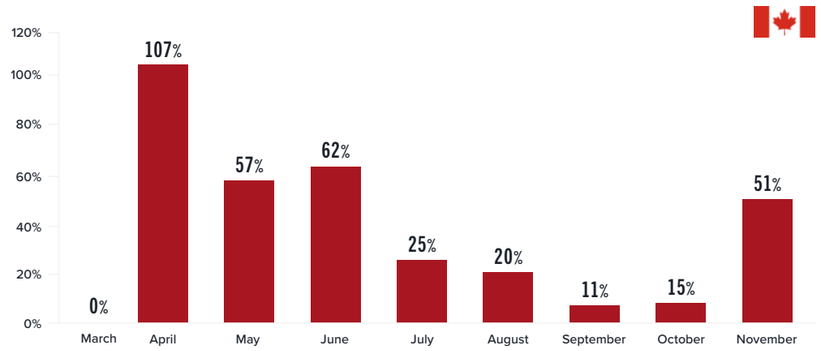


Source: Enea Openwave worldwide deployments

YouTube: Relative change in traffic contribution to mobile networks in Egypt (2020)

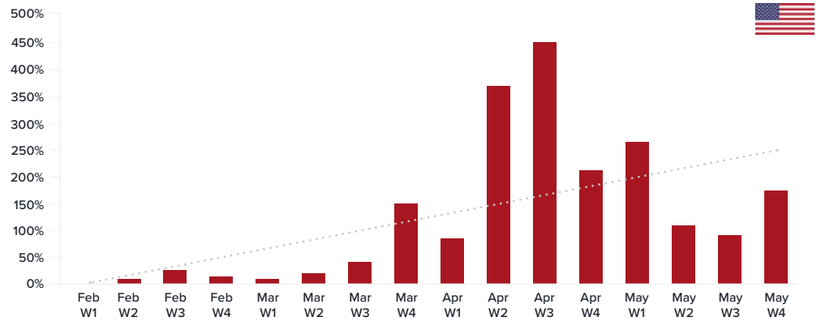


Similarly, although there was no nationwide lockdown in Canada, mobile gaming traffic witnessed a surge during April to June compared to its contribution in March.



Mobile gaming: Relative change in traffic contribution to mobile networks in Canada (2020)

And in the US, we again see a similar pattern:

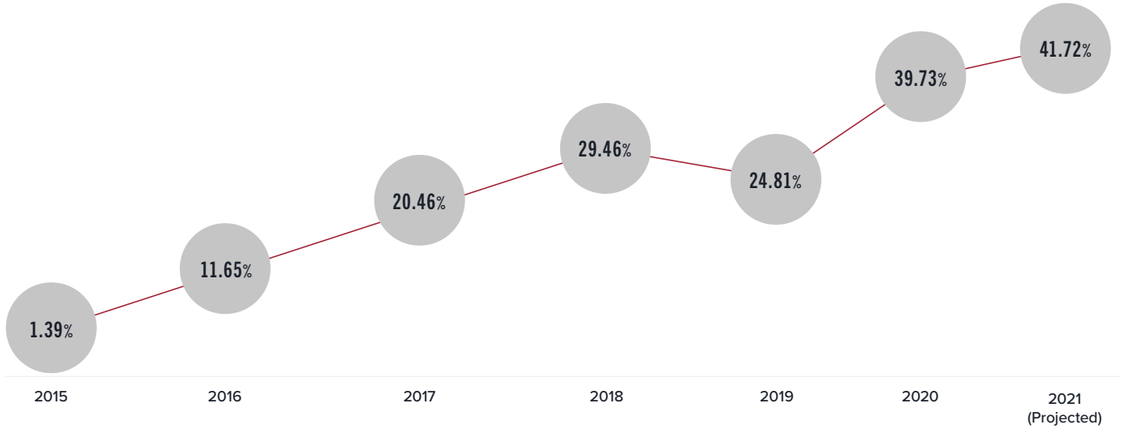


Growth of gaming traffic for one mobile operator in the US

These charts provide a glimpse of just how demanding it has been for Mobile Network Operators (MNOs) to address sudden and sustained surges in network traffic without hampering subscriber QoE. Those MNOs, which were swift enough, retained their user base and are well placed to take advantage of new traffic patterns exemplified by the “7 day weekend”.

The spectacular rise of QUIC: a prophecy fulfilled

In February 2018, we published a blog on how QUIC attained a meteoric rise to fame, and we predicted its continued growth in subsequent years. As we predicted, as of January 2021 QUIC is responsible for almost 40% of mobile network traffic globally. The following chart portrays its spectacular rise from 2015 to 2020.



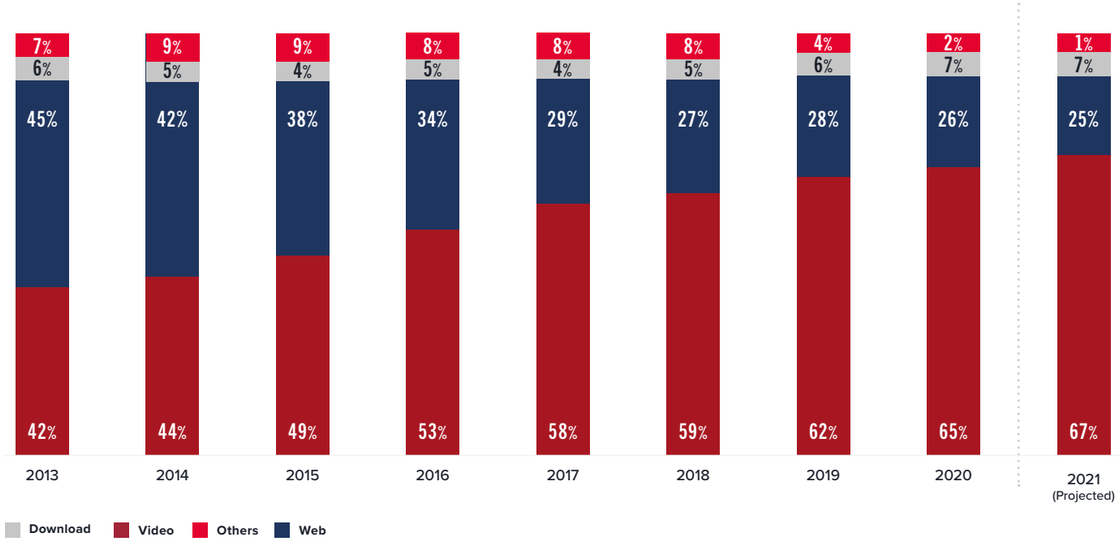
Growth of QUIC

Mobile video growth continues unabated

From December 2020, video content was responsible for over 65% of traffic in mobile networks globally. Most mobile video content was generated from on-demand OTT content platforms - primarily YouTube, Netflix, and Facebook.

Until recently, TCP was the de facto protocol for video delivery. However, Google's "experiment" proved that QUIC, its UDP based protocol, provided better performance especially when delivering YouTube video. Following Google's success, Facebook announced in 2020 that they would be using their in-house implementation of QUIC protocol called mvfst (pronounced "move fast") which also uses UDP as transport.

Today, more than 75% of Facebook traffic uses QUIC. YouTube settled on QUIC for their video delivery in 2016 and almost 95% of their content today is delivered over QUIC. Will the other dominant hyperscaler/OTT content providers in the market make a similar move?

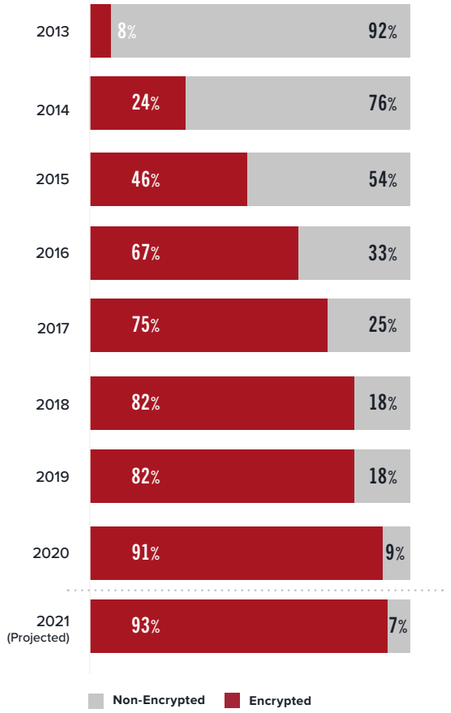


Mobile data traffic by content type

Encryption - operators going blind... again

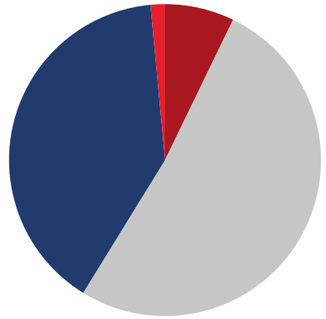
See also Chapter 4 for the in-depth discussion on encryption

Since December 2020, more than 90% of mobile network traffic has been delivered encrypted.



Mobile data traffic by encryption

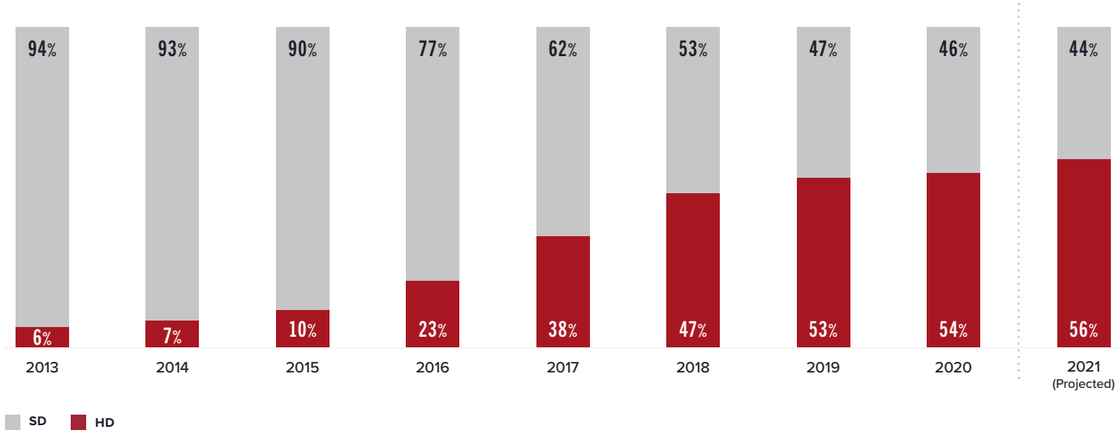
The main driver for this continued growth was the combined dominance of HTTPS and QUIC; these being the most preferred communication protocols due to the security and user privacy that they provide over HTTP.



Data type	2020	2021 Projections
HTTP	7.19%	6.47%
HTTPS	51.60%	50.35%
QUIC	39.73%	41.72%
OTHERS	1.48%	1.48%

Mobile data traffic by protocol (2020)

The contribution of high-definition video content increased compared to the previous year. However, the rate of growth here seems to have plateaued. This could be attributed to increased stress on networks, limiting HD content to users, even under favorable network conditions.

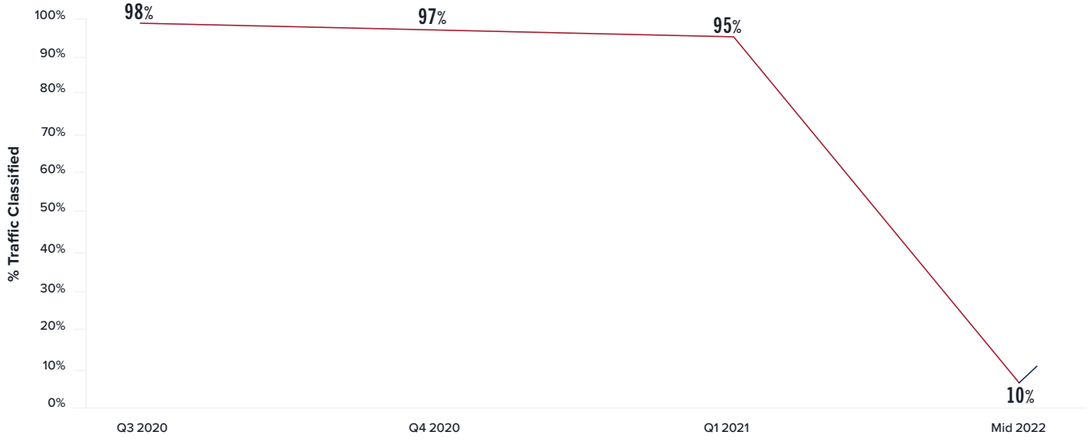


Mobile data traffic by resolution

While it is beneficial for end users to have more than 90% of their communication encrypted, it poses challenges around traffic management, and network security for mobile network operators (see Chapter 4). Of course, with the right set of tools, such challenges can be preemptively and convincingly addressed.

Encryption 2.0

There is a potential shift in the internet industry in using encrypted DNS queries and encrypted SNI to secure end-to-end communication for the users. While this delivers complete privacy for the subscribers, it also poses significant challenges for operators when it comes to preventing malware or cyber-attacks or implementing government mandated policies around harmful content prevention. Owing to this shift, by mid-2022 we anticipate a significant decline in the percentage of traffic that can be classified using today's conventional traffic management solutions.



Encryption 2.0: Inflection point

These data points represent anonymized and aggregated data taken from Enea Openwave Traffic Management deployments worldwide. For more information please contact us using the details at the end of this book.

ABOUT ENEA

Enea is one of the world's leading suppliers of innovative software for telecommunications. It provides award-winning cloud-native, 5G-ready products for data management, video traffic optimization, edge virtualization, and traffic intelligence.

Enea is the first vendor to launch a 5G Data Management portfolio and its traffic management solutions have been deployed by 8 out of 10 global operator groups. More than 3 billion people rely on Enea technologies in their daily lives.

FIND OUT MORE

ENEA Openwave

For further information on the above or advice on any of the topics covered in this book, please contact us. Email: info@owmobility.com

enea.com/traffic-management