ENEA

# CONTENT FILTERING & PARENTAL CONTROLS FOR MOBILE OPERATORS

WORLDWIDE SURVEY

“Over half of under 5s spend at least an hour a day online, unmonitored.”

**Check out the Infographic that accompanies this report**

# EXECUTIVE SUMMARY

**The global pandemic was a watershed event. Over 185 countries closed schools and forced entire student populations to go online, overnight. Most youngsters of course are familiar with the online world, but a UNICEF report highlighted that the lockdowns compelled younger children to go online to a degree previously not seen, and many of them were unprepared to face the internet's many hazards including explicit content, self-harm and violence.**

This report has been created primarily for mobile operators, to cement their reputation as family friendly businesses that safeguard children through content filtering and traffic classification solutions in the core network usually combined with on device parental control solutions. The report is based on a survey undertaken across 4,000 households in the USA, UK, France, Italy, Spain, and Germany (see Appendix 1). The survey was deliberately undertaken in the wake of worldwide lockdowns since this fact has altered behaviors in ways we need to understand. Some of the survey findings are unremarkable, for example almost half of 11-16 year olds spend 3 to 6 hours every day online and unmonitored. Other results however will cause surprise. Here are three such findings:

1. Over half of under 5s spend at least an hour a day online, unmonitored.
2. Parents trust their mobile operator far more than other organisations including Facebook, Google, and even the government, when it comes to safeguarding their children online.
3. Parents are also willing to pay significant additional fees for effective parental controls to be included in their data-plan.

There are numerous other findings presented in this report, along with a discussion of the alternative methods of offering parental controls and the threat posed by imminent encryption protocols. It provides essential reading for any mobile operator considering their strategy – and indeed their reputation – when it comes to child safety.

## This Report is organised as follows

**Challenge to operators & survey overview** – summarises the problem, the market and the highlights of our survey

**Enea Next Generation Traffic Filter** – a brief overview of our solution

**APPENDIX 1** – the full survey results are given here

**APPENDIX 2** – provides a tutorial to the new encryption standards and protocols we expect in the next 12 months.

# CHALLENGE TO OPERATORS & SURVEY OVERVIEW

## Young children are online more than we think

Post-pandemic more families now rely on home digital solutions to ensure continuity of learning for their children, and often on smartphones and mobile devices using both WiFi and the mobile network. This has resulted in a huge rise in children's online activities outside the school VPN or service provider safe lists.

environment and has increased the chances of them stumbling upon inappropriate or harmful content.

For example, according to the survey conducted by Enea and Censuswide, and reported in full in Appendix 1, **44%** of 11-15s spend 3-6 hours a day on the internet unmonitored.

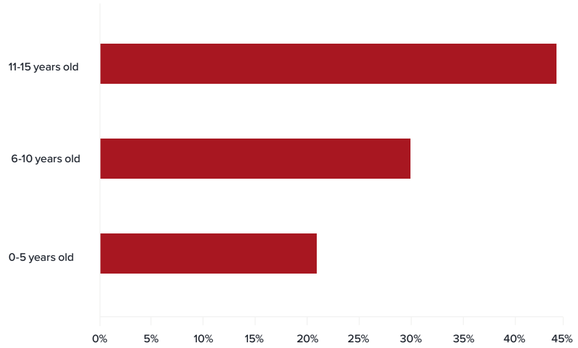
These figures remain broadly consistent across all 6 countries surveyed. Of even greater concern is the fact that **over half of under-fives spend at least one hour a day online unmonitored** (Appendix 1). This includes time spent on WiFi and / or mobile networks.

> "Over half of under-fives spend at least one hour a day online unmonitored"

These results support the findings of a report by UNICEF which highlights the issues of the pandemic causing an alarming rise in screen time for children, and suggests guidance for governments/ICT companies/educators/parents. The demand for parental control solutions whereby parents can safeguard children's online activity and enforce "safe-space" restrictions is surging.

Through effective use of content filtering / traffic classification combined with on-device parental control solutions, online activity can be restricted to certain hours of the day / days of the week and can be complemented with a combination of access control restrictions around VoIP, social media and gaming content. In most cases these solutions will work in conjunction with other on-router or on-handset solutions to create a comprehensive safeguarding experience.

A specific issue for mobile operators is rolling out effective solutions that deal with post lockdown use cases in the face of new mobile encryption protocols. These issues, as well as the worldwide survey reported in Appendix 1, are the topics of this report.




**Age of children who are online unmonitored for 3 to 6 hours a day**

*(Survey: Parents with children aged 11- 16 in the UK, US, France, Germany, Italy and Spain)*

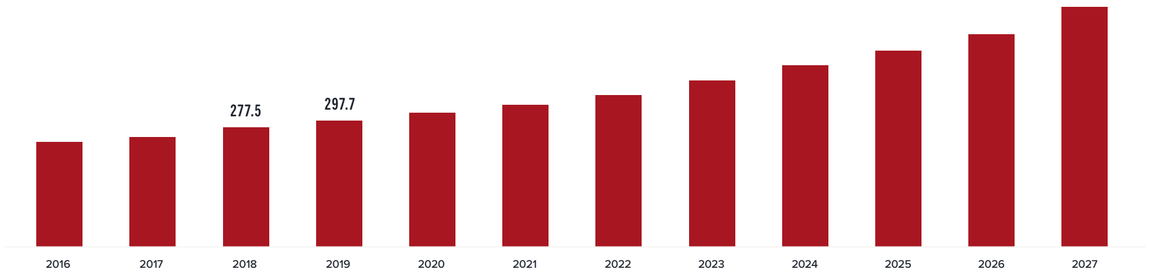
## A growing market

The global parental control software market size was US$ 797.3 million in 2019 and is projected to reach US$ 1.76 billion in 2027 at a CAGR of 10.5%, as per research conducted by Fortune Business Insights. The US market alone was worth US$300 million in 2020 (see accompanying figure).

The market can be segmented into residential and educational institutions, with deployment choices being either on premise or on cloud. Governments in some countries are also driving the adoption of parental control solutions by educational institutions so they can safeguard students online and block access to inappropriate content.

In addition to the offerings provided by operating systems such as Android and iOS, OTT content providers have devised their own ways to enforce parental control policies. For example, in February 2020 Tiktok launched a parental control feature named “family safety mode” across the UK in line with European children data policy regulations. This feature enables parents to manage screen time, disable direct messaging and turn on restricted mode.

Google also offers an app called “Family Link” for parental control use cases and lets parents set certain digital ground rules for their family. YouTube also announced that parents can let teens have supervised experiences on the platform. This is provided via an account option that acts as a bridge between YouTube Children and regular YouTube that allows older children greater access to content but still allows parents to control what they can see.




**North America Parental Control Software Market Size, 2016-2027 (USD Million)**

*(Survey: www.fortunebusinessinsights.com)*

## Who do parents trust to protect their children?

Trust is a major factor making parents have second thoughts about installing parental control apps on smartphones. In addition to (mostly incorrect) assumptions around privacy issues, parents often feel that most teens would find a workaround to on-device access controls and potentially become even more secretive about their internet activity.

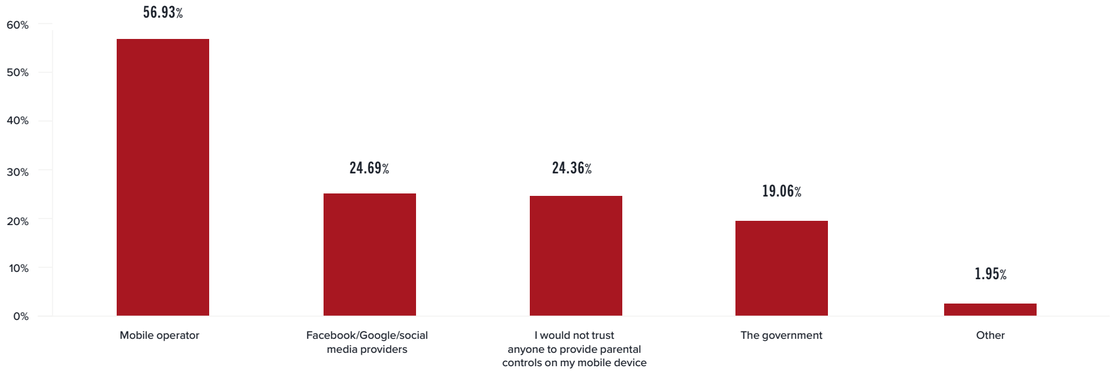
However, there is a positive side to this. Almost **57%** of parents in our worldwide survey expressed trust in Mobile Network Operators (MNOs) to provide parental control solutions that protect their children. This is in stark contrast to the fact that less than a quarter of parents will trust Facebook, Google or any social media providers.

> “57% of parents trust their mobile operator – less than a quarter trust Facebook or Google”

In fact, almost **70%** of parents are willing to pay extra for a plan that includes parental control. Specifically, almost **58%** of parents are willing to pay between US$ 5 & 14 for an effective parental control plan. At least a portion of this is available for MNOs with appropriate solutions to monetize. (Please refer to Appendix 1 for details).

Of course there are options, multiple ways of implementing parental control use cases. The main options being (a) client-based solutions, (b) network-based solutions, or (c) gateway-based solutions. Client-based solutions require individual updates and add maintenance costs and reduce the manageability of the solution.

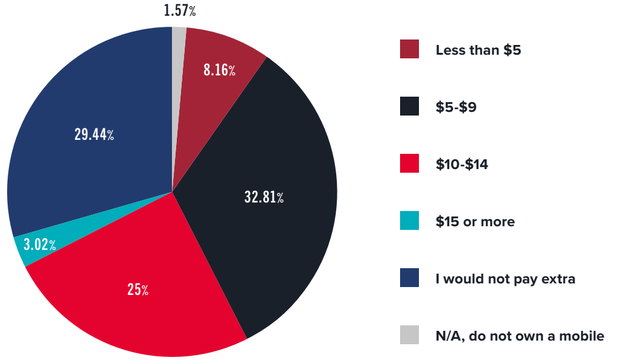
In most cases, network-based or gateway-based solutions are preferred over client-only solutions as they offer better manageability through centralized updates and provide the greatest level of granularity for web content filtering. Gateway based solutions can also be deployed in the core network to invoke selective policies around blocking or allowing a pre-defined set of categories and URLs for the end users, including malware and phishing sites. Such solutions can also enforce SafeSearch web-filtering whereby a user will be redirected to SafeSearch versions of search engines such as Google or Bing which would block explicit images, videos and websites from search results. Potentially, this can open up new revenue streams for MNOs in the form of custom data packages with parental control services.




**Who do parents trust the most to protect their children?**

This makes a strong case for the MNOs and CSPs to have solutions deployed within the core network to ensure better security and privacy.

However a serious concern for MNOs offering parental controls is the issue of encrypted content.




**How much extra are parents willing to pay opperators for effective parental controls (US$)?**

"Almost 70% of parents are willing to pay extra for a dataplan that includes parental control"

## Challenges due to the arrival of new encryption protocols

Due to the encrypted nature of the traffic, it is a gruelling task for an entity residing in the communication path to decrypt every secure (HTTPS/QUIC) transaction and determine the nature of the content (eg adult, gambling, violence etc) as the destination URL is not visible. This task requires intelligent traffic classification and filtering solutions which can overcome such challenges by building intelligence around traffic pattern analysis.

These challenges will multiply upon popular adoption of DNS over HTTPS (DoH) or DNS over TLS (DoT) and encrypted SNI (eSNI) by application/OS/browser vendors and destination servers (see Appendix 2 for a brief explanation of new encryption protocols). If not addressed effectively, these may limit the functionality of the existing solutions or, worse, render them useless.

## Monetization opportunity ... or reputation threat?

Taking all of these factors together, MNOs have the opportunity, the challenge and also the expectation of parents to help. Forward looking MNOs can enhance their reputation and potentially monetize the opportunity to enforce parental control use cases for their subscribers.

> “Forward looking MNOs can enhance their reputation and potentially monetize the opportunity to enforce parental control use cases for their subscribers.”



# ENEA NEXT GENERATION TRAFFIC FILTER

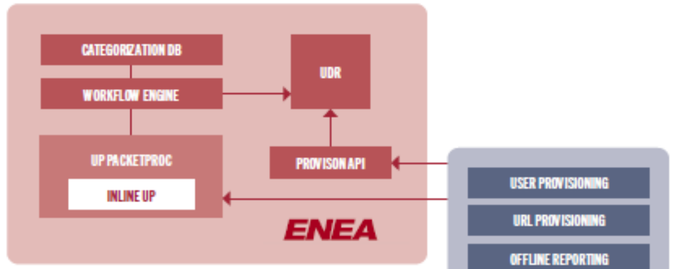
## Overcoming the challenges of new use cases and new encryption protocols

Enea's Traffic Filter solution offers MNOs a sophisticated content filtering solution deployed in the core including:

- Intelligent categorization of domains, protocol, app and activity for millions of domains on the web, either in data or DNS path.
- Instantaneous classification of content, from adult to games, or gambling to search engines, and for both encrypted and unencrypted traffic using metadata extraction algorithms which employ a combination of techniques such as statistical prediction, behavioral analysis and heuristics.

Traffic Filter enables mobile operators to implement key use cases including Parental Controls, Regulatory Compliance, and Filtering for Enterprises.

The solution embeds an intelligent categorization function that enables multi-level categorization decisions to be made based on domain, URL, user policy, or time of day, by analyzing the traffic routed from the enforcement point (usually, a PGW). The classifications may be sourced internally within the domain of the network operator or by use of external categorization databases. The following diagram illustrates component level architecture of the filtering solution:




Enea Next Generation Traffic Filter

## User provisioning

Traffic Filter provides an optional interface with either Enea or an existing Unified Data Repository (UDR), which is a converged repository of subscriber information. User(s) can be provisioned into UDR via an API and selective access control policies can be enforced.

The solution enables mobile operators and ISPs to design URL and content filtering use cases for enterprises and retail subscribers. For example,

(i) **Parental control** use case where access to adult and malicious content is restricted for minors to keep them safe online and empowers parents and educational institutions to regulate web browsing.

(ii) **Regulatory compliance** can be ensured based on the policies defined by the regulatory authority eg **CIPA**, an act passed by US Congress that mandates K-12 schools and libraries to use internet filters and implement other measures to protect children from harmful online content as a condition of the receipt of certain federal funding, especially E-rate funds.

(iii) **Enterprise level** use cases such as restricting access to social media, gaming and video streaming websites to improve productivity and reduce distractions.

## Reporting

The solution provides the user with an out-of-the-box reporting dashboard giving them an overview of traffic by protocol, category and enforcement policy. It can also expose the operational reporting database via APIs to a third-party subscriber management portal so customized reports could be constructed.

## Handling of new encrypted protocols

The solution has been designed to be effective even in the case of wide adoption of DoH and ECH in encryption protocols, see Appendix 2. Please get in touch to know more about how we overcome these challenges.

> "The solution provides the user with an out-of-the-box reporting dashboard"

# SUMMARY

**Home-working and home-schooling have heightened the importance of content filtering and parental controls.**

Our recent worldwide survey confirms this and also that this is a shared responsibility between parents and MNOs – who parents trust. In the case of failure, the risk of reputational damage to operators is considerable.

However, there are next generation solutions available, built to handle the rigours of a post-pandemic world and the best of these also enable MNOs to successfully navigate new encryption protocols.

*For further information on any aspect of the contents of this eBrief please contact: Telecom@enea.com*

> “The best of next generation solutions also enable MNOs to successfully navigate new encryption protocols.”

# APPENDIX 1:

# WORLDWIDE SURVEY OF ONLINE BEHAVIOR & PARENTAL CONTROLS

**Enea commissioned Censuswide to conduct a survey across multiple countries in Europe and the US. The objective was to understand the behavior and needs of consumers for parental control solutions.**

Over 4,000 households, with children under the age of 16, participated in the survey and it was conducted across the US, UK, France, Germany, Italy and Spain. Consumers were presented with questions in the following areas:

1. Unmonitored online activity of children of various age groups per day.
2. Trust in mobile operators/social media apps/the government to provide parental control solutions.
3. Perceived benefit of parental control solutions provided by mobile operators.
4. Willingness to pay extra to mobile operators for a parental control plan.
5. Willingness to switch mobile operator for a parental control plan.

The results obtained are summarized in this section.

Back to contents

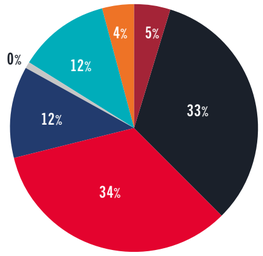


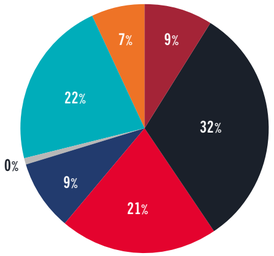
## Unmonitored online activity of children

Question: During lockdown, how many hours a day do you estimate your child stays online unmonitored on their mobile device, if any?

Averaged across age groups and countries, approximately one third of children are online unmonitored for 1-2 hours and a further one third for 3-6 hours.

Looking at the older and younger children, 34% of 11-15s were perhaps unsurprisingly found to be spending 3 to 6 hours a day online, unmonitored. Rather more surprising is the finding that, among the youngest children, under 5's, over half (actually over 60%) are online, unmonitored for at least 1 hour a day.



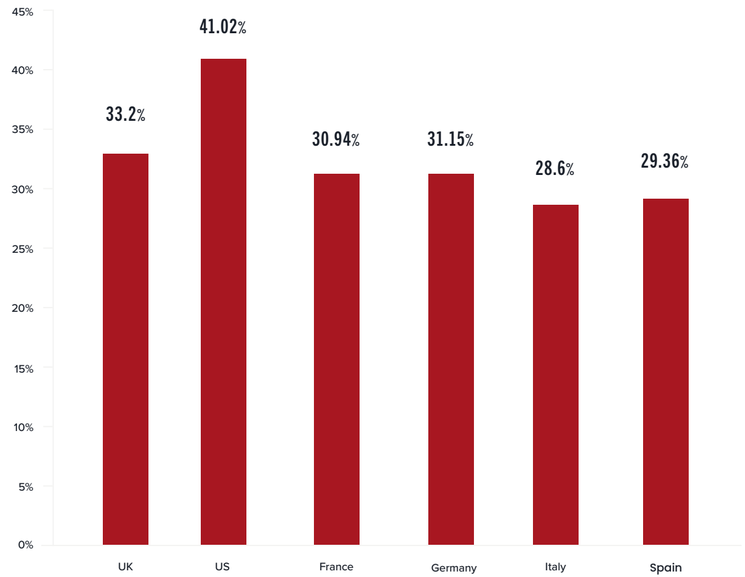

Less than an hour
Over 12 hours a day
1-2 hours
None
3-6 hours
N/A
7-12 hours

**How many hours a day children spend online unmonitored**

Less than an hour
Over 12 hours a day
1-2 hours
None
3-6 hours
N/A
7-12 hours

**The amount of time under 5s spend online, unmonitored**

Across the countries surveyed there was not much difference, eg the chart below shows the percentages of children online for 3-6 hours a day, averaged across ages.



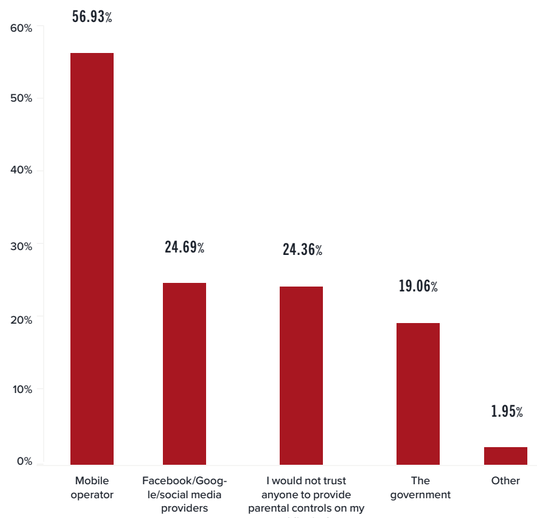

**Proportion of children across all ages who are online unmonitored for 3-6 hours a day**

## Issues of trust

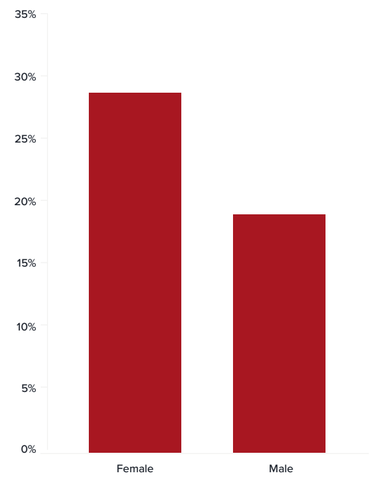
Question: Who would you trust to provide parental control on your mobile devices, if anyone? (Tick all that apply)

When asked about the parties they trust to provide parental control solutions, more than 50% of parents chose mobile operators over social media apps or the government. This reflects other surveys carried out by Enea on issues of trust in the mobile industry and is good news for MNOS considering venturing into the parental control space.

Interestingly, mothers are much less trusting than fathers of anyone to protect their children online!




**Who do parents trust to protect their children?**

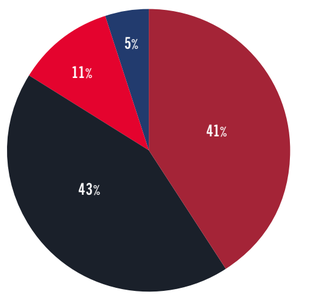



**Parents who would not trust anyone to provide parental control on their devices**

## Perceived benefit

Question: How useful would you find parental controls delivered by your mobile operator?

When asked if parental control solutions delivered by MNOs would be useful, more than 80% of the parents found that proposition useful (ie very useful + fairly useful).

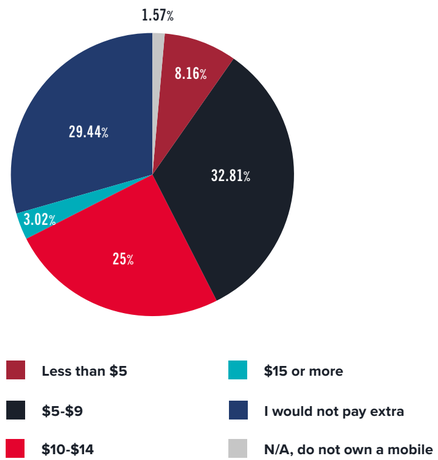



**How useful do parents find parental controls delivered by their mobile operator?**

## Willingness to pay

Question: How much **extra** would you pay your mobile operator for a plan that included parental controls, if at all?

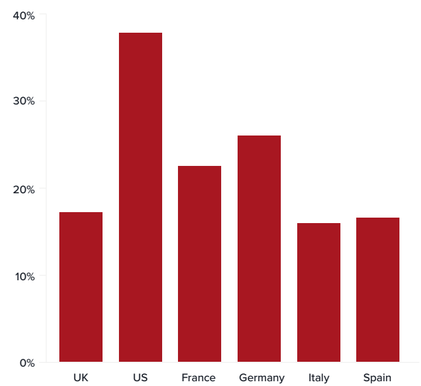
When asked about their willingness to pay extra for a parental control plan, we received the following responses from parents. Of course, in cases where connectivity provision is shared between the MNO and another broadband provider then this monetization will also be shared. Nevertheless the responses below clearly demonstrate "there is money on the table". This is perhaps unsurprising since safeguarding their children online is an immensely high priority for the vast majority of parents.




**How much extra are parents willing to pay for effective parental controls? (US$)**



In the lower price brackets there was not much divergence across countries. However, in the higher brackets, the US led the way, ie US parents are more likely to pay higher fees to MNOs in return for safeguarding their children online.



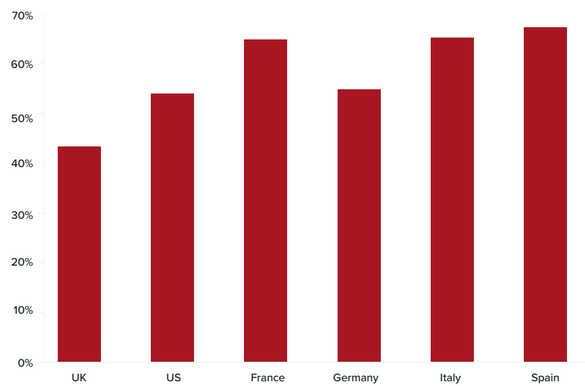

**Parents willing to pay their mobile operator $10-$14 extra for a plan with parental controls**

## Willingness to switch mobile operator for a parental control plan

Question: Would you leave your mobile operator if they did not have a parental control plan to join one that did for a similar monthly fee?

When asked if they would be willing to switch their mobile operator if the competitor offered a parental control plan for a similar monthly fee, almost 56% of the parents said they would.

*Please feel free to reach out to us at Telecom@enea.com if you need more information on the survey results.*




**Parents willing to leave their mobile operator for one offering parental controls at the same price**

# APPENDIX 2:

# EXTENDED ENCRYPTION IN INTERNET PROTOCOLS

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

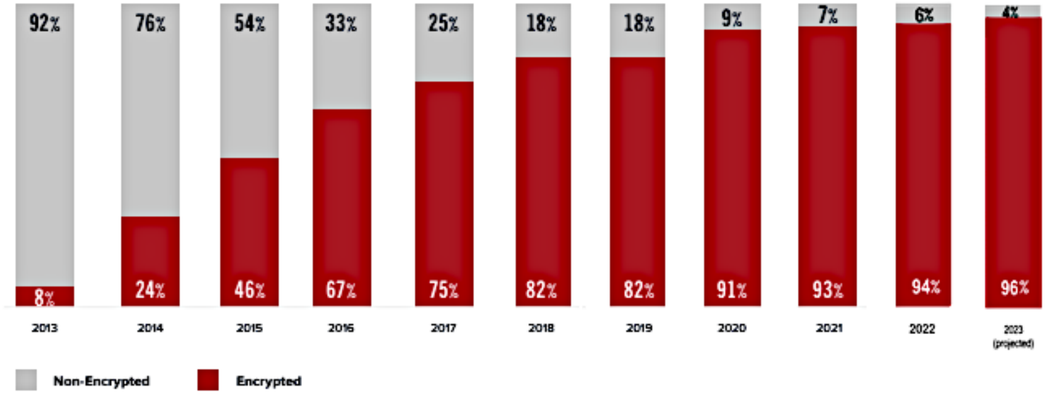
Within a short space of time, HTTPS became the norm and the internet "went dark", driven partly by security concerns and partly by the agendas of OTT content providers. Today over 90% of traffic on mobile networks is encrypted (see accompanying chart).

Back to contents



This level of encryption ensures that the communication between two end points is secure and no threat actor can see or modify it. However, there is a loophole which allows some level of inspection and for operators to manage traffic and add value. 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 plain text. Though the connection and data transfer afterwards remain 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 threat actors in the system for malware and phishing attacks etc.

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.




**Mobile data traffic by encryption (source, Enea worldwide deployments)**

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

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 plain-text 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.



# ENCRYPTION – WHAT TO DO NEXT

**DOH will impact all traffic filtering solutions that rely on DNS inspection / classification – and there are many such solutions currently in use in Tier-1 and Tier-2 networks from big-name vendors.**

All of these will be rendered ineffective since these solutions will simply not be able to view the details within a DNS flow, and thus cannot classify that traffic. Solutions that perform "in-line" inspection however will not be impacted by DOH.

Extensive rollout of eSNI will impact ALL existing 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 an effective solution to track these events and to manage, not just DOH, but critically, eSNI.

# FIND OUT MORE

**Enea Traffic Filter**

Traffic Filter enables MNOs and ISPs to deploy domain and content filtering use cases for enterprises and retail subscribers with management of upcoming encryption protocols built into the roadmap.

ENEA

For further information on the above or advice on any of the topics covered in this book, please contact us.

Email **telecom@enea.com**

**enea.com**