

# CONTENT FILTERING: PERSPECTIVES & CHALLENGES FOR MOBILE BROADBAND OPERATORS

**Azfar Adib**  
**Lead Engineer, Grameenphone Ltd.**  
**Dhaka, Bangladesh**  
**[azfar@grameenphone.com](mailto:azfar@grameenphone.com)**

**SANOG 28 1<sup>ST</sup>-9<sup>TH</sup> AUGUST 2016 MUMBAI**

# AGENDA

- WHAT IS CONTENT FILTERING
- CONTENT FILTERING REQUIREMENT: FROM AUTHORITIES
- CONTENT FILTERING REQUIREMENT: FROM CUSTOMERS
- CONTENT FILTERING REQUIREMENT: FROM OWN ARENA
- CONTENT FILTERING REQUIREMENT: FROM A COMBINED PERSPECTIVE
- CONTENT FILTERING: DOMAINS OF EXECUTION
- CONTENT FILTERING: IN USER DOMAIN
- CONTENT FILTERING: IN OTT DOMAIN
- CONTENT FILTERING: IN NETWORK DOMAIN
- CONTENT FILTERING THROUGH DPI
- CONTENT FILTERING THROUGH ICAP SERVER
- CONTENT FILTERING THROUGH DNS
- CONTENT FILTERING THROUGH FIREWALL
- CONTENT FILTERING: COMPARISON OF DIFFERENT MECHANISMS
- CONTENT FILTERING IN COMBINED MANNER : AN EXAMPLE

# WHAT IS CONTENT FILTERING

Using appropriate mechanism to screen and exclude from access or availability of selected online contents



## Access has been Denied!

Access to the page:

<http://www.badboys.com>

... has been denied for the following reason:

**Banned site: badboys.com**

You are seeing this error because what you attempted to access appears to contain, or is labeled as containing, material that has been deemed inappropriate.

If you have any queries contact your ICT Co-ordinator or Network Manager.

Powered by [DnsGuardian](#)

YOUR ORG NAME

*For mobile broadband operators, the requirement for content filtering can arise from different arena in various perspectives, like:*

- *From authorities (regulators-governmental bodies)*
- *From customers ( mass consumers – business segments)*
- *From own (local operational requirement-global guideline)*
- *Combination of all above*

# CONTENT FILTERING REQUIREMENT: FROM AUTHORITIES

## How Facetime Saved the Turkish President from His Country's Attempted Coup


By Anna Nini





July 17, 2016



## Turkey Confirms Blocking WikiLeaks Following Ruling Party Email Publication

WORLD 10:29 20.07.2016 (updated 11:44 20.07.2016) [Get short URL](#)

Topic:  Military Coup Attempt in Turkey (244)

 0  1066  3  5

Turkey's Presidency of Telecommunication and Communication (TIB) confirmed to RIA Novosti on Wednesday the blocking of the WikiLeaks investigative website following its publication of nearly 300,000 ruling party emails.

ANKARA (Sputnik) –Earlier on Wednesday the whistleblowing organization said via Twitter the the Turkish authorities have ordered a nationwide blocking of the Wikileaks website.

*"Administrative measures have been taken with regard to the WikiLeaks website," an official with the TIB, part of Turkey's Information and Communication Technologies Authority (BTK), said.*



© FLICKR/ STEVE RHODES

[WikiLeaks Publishes Internal Emails of Turkish Ruling Political Party AKP](#)

# CONTENT FILTERING REQUIREMENT: FROM AUTHORITIES

## MINISTER ASKS INDIAN ISPS TO PERMANENTLY BLOCK HUNDREDS OF 'PIRATE' SITES

BY ANDY ON OCTOBER 29, 2015

C 30

*India's Information Technology Minister has asked local Internet service providers to block at least 240 sites said to be offering 'pirate' content. During a meeting yesterday with representatives from the film and ISP industries, police and other officials, K.T. Rama Rao promised to form a specialist police unit and take action within 30 days.*

For several years, filmmakers in India have sought to protect their content from unauthorized online distribution. That has mainly taken the form of so-called 'John Doe' orders.

Back in May 2015 [one such order](#) not only targeted The Pirate Bay, KickassTorrents, Torrentz and TorrentFunk, but also video streaming site Vimeo. As a result, local ISPs were given just 24 hours to stop their subscribers from accessing the sites.

While it seems relatively easy to obtain these kinds of court orders, they have to be obtained each time a film is released to the public. That clearly has cost implications for those obtaining the orders and in recent months there have been calls for a more suitable system to be put in place.



## No internet for Singapore public servants

8 June 2016 | Asia

Share



Public servants in Singapore will be blocked from accessing the internet on work computers from May next year.

The moves aims to plug "potential leaks from work e-mails and shared documents amid heightened security threats," the Straits Times newspaper said.

Officials said employees across government would also be barred from forwarding any work-related information to personal emails.

Singaporeans have responded with shock and scepticism online.

Some people thought the move contradicted Singapore's much-promoted **Smart Nation technology initiative**.

Others thought the suggestion that the measure could also apply to teachers, who do not deal with much sensitive information, was extreme.



# CONTENT FILTERING REQUIREMENT: FROM AUTHORITIES

Taiwan proposes Great Firewall-style blocking of overseas copyright infringing sites



A [proposed amendment](#) to the current Taiwanese law governing copyright could lead to Great Firewall-style internet blocking, according to free speech campaigners.

The amendment, put forward by the Taiwan Intellectual Property Office, would allow IP and DNS blocking at the ISP level through a black list system. The system, designed to block websites which share media protected by copyright law, will also target peer-to-peer tools such as BitTorrent.

Since the proposal was announced, there has been [considerable push back](#) from bloggers and tech industry players in Taiwan.

The proposal would introduce a blacklist similar to that overseen by the Australian Communications and Media Authority (AMCA). Campaigners have demonstrated on numerous occasions that the Australian blacklist is poorly administered and susceptible to abuse. In April [it was revealed](#) that 1,200 websites were inadvertently blocked in attempt to censor one site alleged to be fraudulent by the government. A version of the AMCA blacklist published in Wikileaks in 2009 [included](#) the websites of a "Queensland dentist, a tuckshop convener and a kennel operator".

As Taiwanese commentator CK Hung [points out](#), it is the secret nature of the blacklist which makes it dangerous for free speech, regardless of the high-minded copyright protection ideals behind the proposal (translation by Global Voices):

## Facebook, WhatsApp, Viber blocked in Bangladesh

Ishtiaq Husain, Kamrul Hasan

The government has blocked popular social media platform Facebook and online messaging and calling services WhatsApp and Viber on security grounds, said Dr Shahjahan Mahmood, chairman of BTRC.

The BTRC (Bangladesh Telecommunication Regulatory Commission) chief told the Dhaka Tribune: "Social media platform Facebook and other online messaging and calling services have been blocked in the country on Wednesday on security grounds."

Earlier in the day BTRC issued a letter to different telecom operators and all Internet Service Providers, asking them to stop the services immediately.

**[Read more: PM: Viber, WhatsApp to be blocked temporarily](#)**

The order came around 12:15pm immediately after the Supreme Court upheld death penalty to war criminals Salauddin Quader Chowdhury and Ali Ahsan Mohammad Mujahid.

The letter signed by BTRC Assistant Director (System and Service Division) Touseef Shahriar, reads: "I am directed to instruct you to stop the Facebook, Viber and WhatsApp services in your network with immediate effect until further instruction.

"Please confirm execution."

**[Also Read: SC upholds Salauddin's death penalty](#)**

Seeking anonymity, a high official of one of the leading telecom companies in Bangladesh, told the Dhaka Tribune that the telecom operators acted immediately after receiving the letter.

Last week on November 11, Prime Minister Sheikh Hasina said the government was contemplating to block Viber and WhatsApp Messenger temporarily in the country to track down the cyber criminals.

Various factors (like: national security or socio-political issues; piracy prevention ; blocking pornographic or generally objectionable contents) trigger such requirements from governments or regulatory bodies.

# CONTENT FILTERING REQUIREMENT: FROM CUSTOMERS

## How to Limit Internet Access at Your Business



The Internet provides small businesses with many convenient features to facilitate business, allowing employees to conduct research, access information and view competitors' websites. A serious problem occurs, however, when employees spend time on the Internet doing activities unrelated to business such as shopping, talking in chat rooms or posting on social media websites. According to Staff Monitoring Solutions, American businesses lose up to 40 percent productivity due to Internet usage unrelated to work. It can be more serious if the employee looks at inappropriate websites, commits an illegal activity or shares confidential company information. Businesses can take a number of measures to limit Internet access for employees.

*Limiting Internet access within your business increases productivity.*

## Business Segment



Business entities often require to restrict their employees from **accessing online contents which are unrelated to business.**

## Consumer Segment



## Parental Control Android

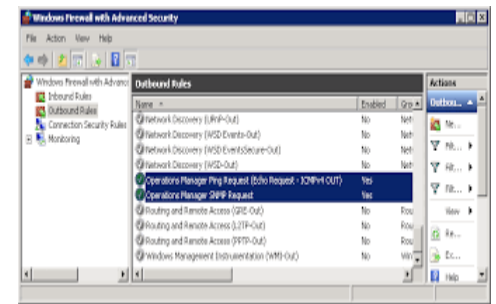


Content filtering, commonly defined as **"Parental Control"**, is a popular requirement in consumer segments as well.



# CONTENT FILTERING REQUIREMENT: FROM OWN ARENA

Mobile Broadband Operators may require to apply content filtering policies for own sake to prevent **charging fraud**, **security threats** and complying **organizational guideline**.



### MMS Overbilling and Fraud Detection

- MMS algorithms continuously audit and parse EOBs for overbilling, fraud, and errors that are the source of inflated and incorrect medical bills.
- Industry reports indicate that up to 80% of medical bills have overcharges. Hospital authority estimates fraud alone at \$270 billion annually.
- MMS can proactively notify employees of irregularities on full privacy protected basis. No need for employee to lift a finger.
- Multiple options for remedy and recovery.
- Money saved (recovered, adjudicated, removed from bill) can be significant and result in positive outcomes for both employee AND employer.



# CONTENT FILTERING REQUIREMENT: FROM A COMBINED PERSPECTIVE



## Mobile Alliance Against Child Sexual Abuse Content

The Mobile Alliance Against Child Sexual Abuse Content was founded by an international group of mobile operators within the GSMA to work collectively on obstructing the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content.

The Mobile Alliance's aim is to help stem and ultimately reverse the growth of online child sexual abuse content.

Through a combination of technical measures, co-operation and information sharing, the Mobile Alliance seeks to create significant barriers to the misuse of mobile networks and services for hosting, accessing, or profiting from child sexual abuse content.

### ALL MOBILE ALLIANCE MEMBERS COMMIT TO:

- ✓ supporting and promoting 'Hotlines' or other mechanisms for customers to report child sexual abuse content discovered on the Internet or on mobile content services
- ✓ implementing 'Notice and Take Down' processes to enable the removal of any child sexual abuse content posted on their own services
- ✓ implementing technical mechanisms to prevent access to websites identified by an appropriate agency as hosting child sexual abuse content.

THE MOBILE ALLIANCE ENCOURAGES ALL MOBILE OPERATORS, WORLDWIDE, TO PARTICIPATE IN THE INITIATIVE.

### THE MEMBERS OF THE MOBILE ALLIANCE INCLUDE:

Deutsche Telekom Group	Orange Group
Dhiraagu	Telecom Italia
Dialog Axtata Telekom	Telefónica Group
3 Europe	Telenor Group
EE	TeliaSonera Group
Meteor	Vodacom SA
Telekom Austria AG	Vodafone Group
Mobitel	Zain Group
MTN Group	

### COLLABORATING WITH KEY EXTERNAL STAKEHOLDERS:

On behalf of the Mobile Alliance, the GSMA also works closely with a number of external stakeholders that are actively engaged in combating online child sexual abuse content:

- The GSMA is a member of the **International Telecommunication Union's** Child Online Protection (COP) Initiative, through which it shares Mobile Alliance knowledge and experience of combating online child sexual abuse content.

## Guidelines for Industry on Child Online Protection

ICTS AND VIOLENCE AGAINST CHILDREN:  
MINIMISING RISKS AND RELEASING POTENTIAL

Expert Consultation, Costa Rica, 9-10 June 2014



Clara Sommarin, Child Protection Specialist Exploitation and Violence  
UNICEF Headquarters

unite for  
children

unicef



*Being implemented through*

- Mobile Operators
- Internet Service Providers
- Content providers & app developers
- National & public service broadcasting
- HW manufacturer & OS developers

# CONTENT FILTERING REQUIREMENT: FROM A COMBINED PERSPECTIVE



Europe

## European Framework for Safer Mobile Use by Younger Teenagers and Children

The European Framework for Safer Mobile Use by Younger Teenagers and Children was developed by the European mobile industry to ensure that children can safely access content on their mobile phones. Endorsed by Viviane Reding, European Commissioner for Information Society and Media, the agreement has led to the roll-out of codes of conduct on safer mobile use in 23 EU Member States to the benefit of 96% of European mobile customers.



As growing numbers of mobile operators offer their customers access to a rich and compelling range of content services, they are faced with the challenge of how to manage content which would have been subject to age restrictions if accessed through different channels.

To address the issue directly and to create a framework within which a wide range of content services can be offered to customers, the European mobile industry developed the European Framework for Safer Mobile Use by Younger Teenagers and Children. The Framework lays down a number of recommendations designed to ensure that children and younger teenagers can safely access content on their mobile phones.

- Classification of commercial content – mobile operators' own and third-party commercial content should be classified in line with existing national standards of decency and appropriateness so as to identify content unsuitable for viewing by children and younger teenagers;
- Access control mechanisms – appropriate means for parents for controlling children's access to this content should be provided;
- Education and awareness-raising – mobile operators should work to raise awareness and provide advice to parents on safer use of mobile services, and ensure customers have ready access to mechanisms for reporting safety concerns;
- Fighting illegal content on mobile community products and the Internet – mobile operators should work with law enforcement agencies, national authorities and INHOPE<sup>1</sup> or equivalent bodies to combat illegal content on the Internet.

INHOPE is the International Association of Internet Hotlines for reporting illegal content online.

The Framework was drawn up by GSMA Europe members in consultation with the European Commission and other child protection stakeholders, and launched in Brussels on Safer Internet Day, 6 February 2007, in the presence of Viviane Reding, European Commissioner for Information Society and Media.

The signatories to the Framework are:

- AS EMT
- Alands Mobiltelefon
- Belgacom
- Bouygues Telecom
- Cosmote
- CYTA
- Deutsche Telekom Group
- Elisa Eesti AS
- Hutchison 3G Europe
- Go Mobile
- KPN
- Mobilkom Austria
- Mobiltel EAD
- Mobitel
- Orange France Telecom Group
- P&T Luxembourg
- SFR
- Tele2
- Telecom Italia
- Telefonica
- Telenor
- TeliaSonera
- TDC Mobil Norden
- Vivatel
- Vodafone
- Wind Hellas

To date, the Framework's recommendations have been transposed by the participating mobile operators into self-regulatory codes of conduct in 23 EU Member States. As a result, 580 million mobile subscribers, representing 96% of the EU mobile customer base, currently benefit from the initiative.

"As mobile broadband networks proliferate enabling Europeans to easily access a rich selection of content via their handsets, our industry is moving in a timely fashion to ensure the necessary safeguards are in place to enable parents to have confidence in their children using these mobile services safely."

Kaisu Karvala, Chair of GSMA Europe

"This agreement is an important step forward for child safety. I congratulate the mobile phone industry for moving towards protecting minors. It shows that responsible self-regulation can work at European level."

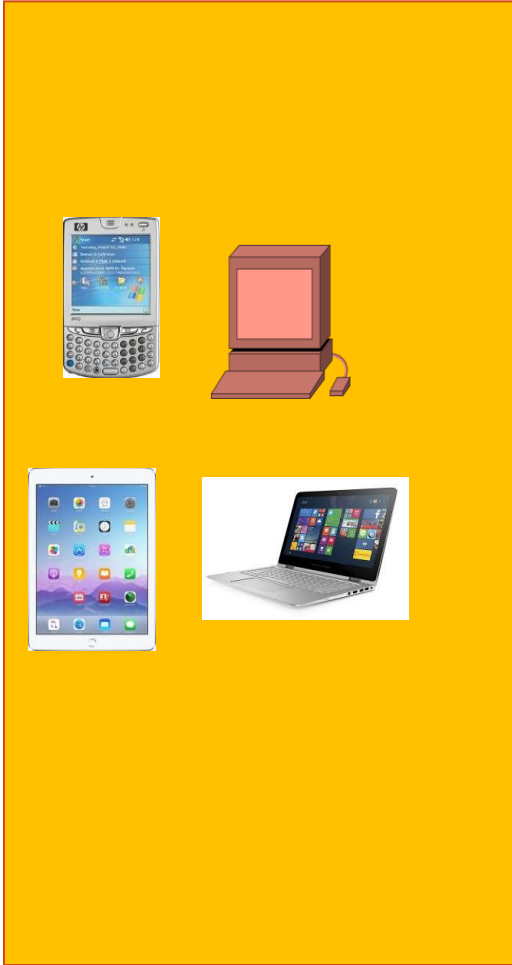
Viviane Reding, European Commissioner for Information Society and Media

For further information about the European Framework for Safer Mobile Use by Younger Teenagers and Children, visit [http://www.gsmeurope.org/safer\\_mobile/](http://www.gsmeurope.org/safer_mobile/) or contact Alice Valvodova at GSMA Europe ([avalvodova@gsn.org](mailto:avalvodova@gsn.org)).

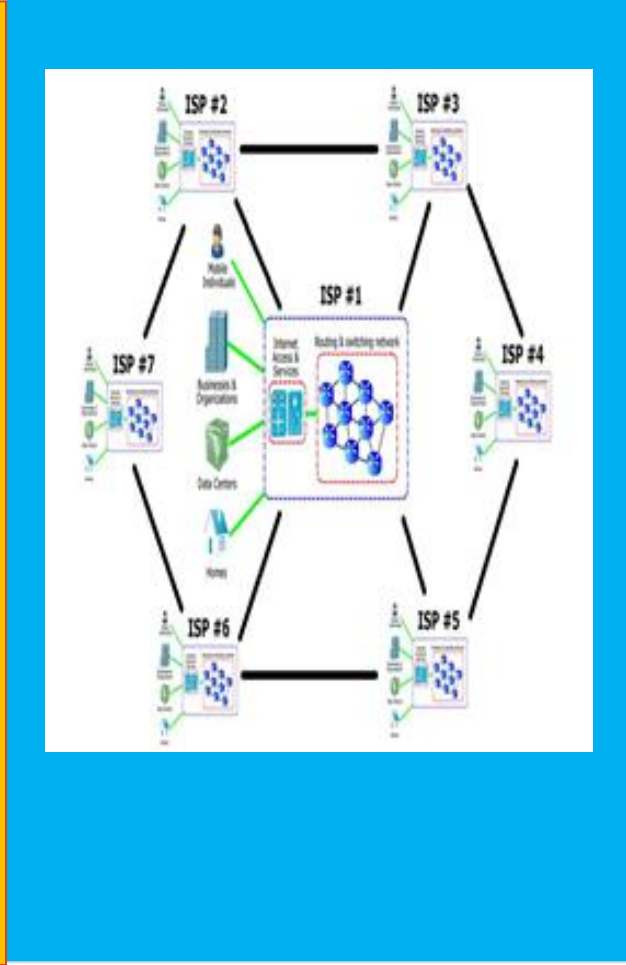


# CONTENT FILTERING: DOMAINS OF EXECUTION

## User Domain



## Network Domain



## OTT Domain



# CONTENT FILTERING: IN USER DOMAIN

Content filtering policy can be applied in devices at user end (like: Wi-Fi routers, mobile handsets, laptop-desktop-tablets) through in-built device settings or appropriate softwares /apps.

### Parental Control Settings

Non-Parental PCs not listed will not be able to access the Internet.

**Parental Control:**  Disable  Enable

MAC Address of Parental PC1: 90-2B-34-1B-36-25

MAC Address of Parental PC2: 8C-89-A5-2F-7F-3C

MAC Address of Parental PC3:

MAC Address of Parental PC4:

MAC Address of Your PC: 8c-89-a5-2f-7f-3c

ID	MAC address	Website Description	Schedule	Enable	Modify
1	6C-62-6D-F7-32-32	Allowed Websites	Allowed Time	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

Current No. 1 Page

### McAfee LiveSafe - Internet Security

#### Parental Controls

Required Settings for: Simon Sage  
McAfee has preset security filtering for every age.

- Select the child's age range: 6-8 years
- Review what your child can see and do online:

Allowed: Kid Safe Websites, Miscellaneous

Blocked: Adult, Anonymizers, Chat or Instant Messaging, Dating

Date of your next scheduled scan: 2015-02-10 4:00 AM

Copyright © 2014 McAfee, Inc. Threat Map | About McAfee SECURE

### Mobile Device Restrictions

Restrictions	Music & Podcasts	Movies	TV Shows	Apps
Allow Music & Podcasts Rated	EXPLICIT OFF	Don't Allow Movies	Don't Allow TV Shows	Don't Allow Apps
Allow Playback of Music, Music Videos and Podcasts containing Explicit Content.		G ✓	TV-Y ✓	4+ ✓
		PG ✓	TV-Y7 ✓	9+ ✓
		PG-13	TV-G	12+ ✓
		R	TV-PG	17+
		NC-17	TV-14	Allow All Apps
		Allow All Movies	TV-MA	
			Allow All TV Shows	

osxdaily.com

### Family Safety

Control Panel Home

Set up Family Safety

Use Family Safety to get reports of your kids' PC activities, choose what they see online, and set time limits, app restrictions, and more.

For use on Family Safety, add a new child's account, or change an existing account to a child's account.

To turn off Family Safety for an account, change the account type from Child to Standard in Accounts.

**Manage settings on the Family Safety website:**  
You can manage this PC's Family Safety settings on the website.

People who can manage these settings online: mrsjanem@msn.com

[More information](#)

This also affects other accounts.

© 2014 McAfee, Inc. All Rights Reserved. McAfee SECURE



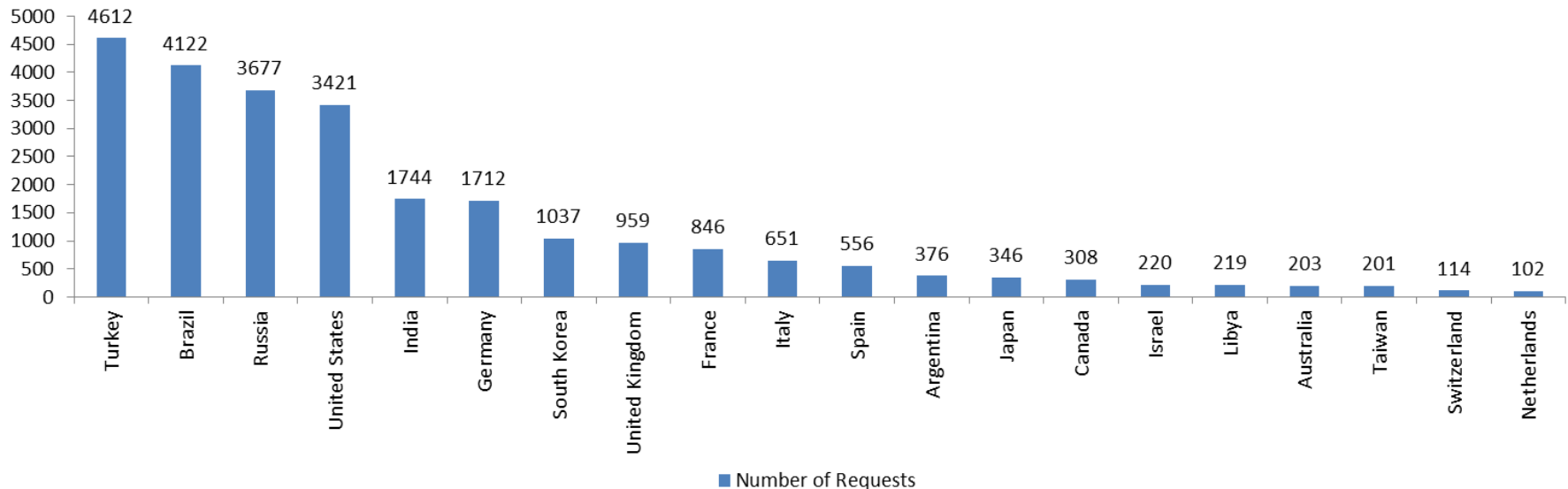
# CONTENT FILTERING: IN OTT DOMAIN

Over-The-Top content (OTT) providers can ensure the most secured mechanism of content filtering as **they host the contents.**

Dominant OTT players (like: Facebook, Google, Microsoft etc.) have an established process for serving content filtering request in accordance with own, regional & international regulations.

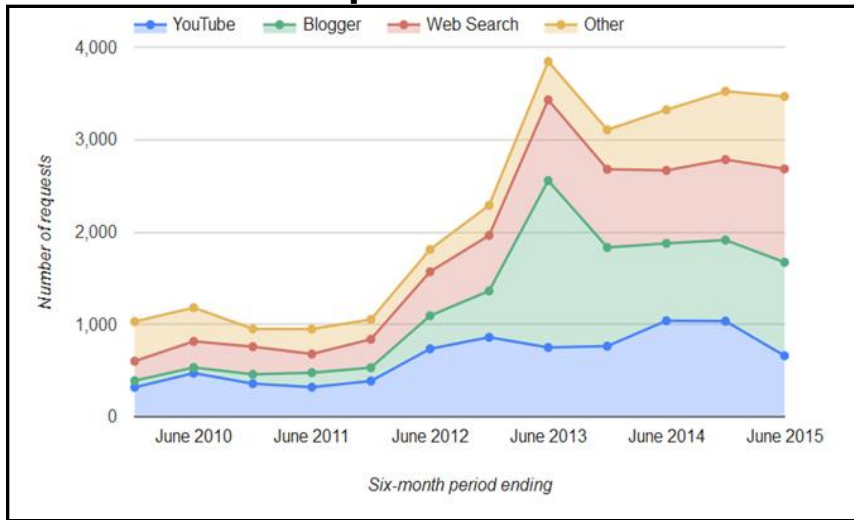
## Recent Statistics on Content Filtering-Google

Countries Placing Highest Number of Content Removal Requests to Google (2010-2015)



# CONTENT FILTERING: IN OTT DOMAIN (Contd.)

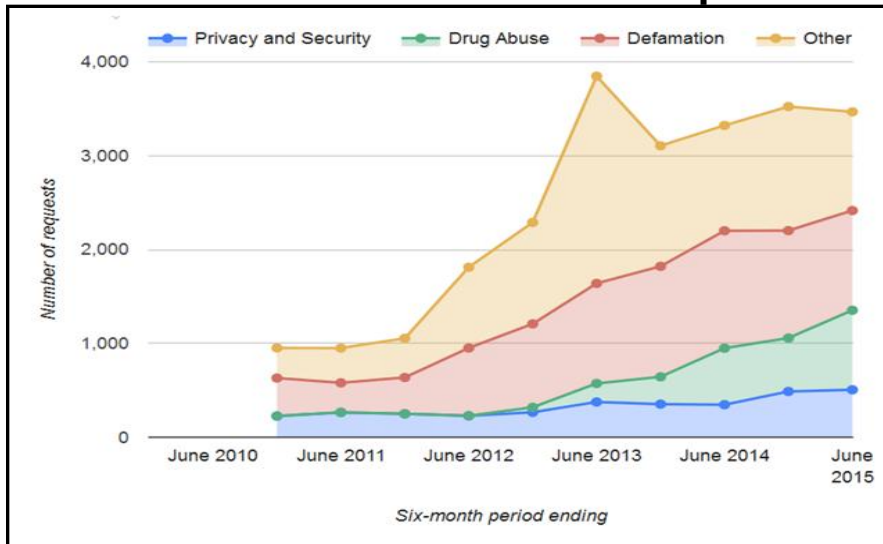
## Domain wise Request Count



## Google domains being blocked in different countries

+	Afghanistan	YouTube
+	Armenia	Google Search
+	Australia	Google Search
+	Bangladesh	YouTube
+	China	Gmail, Google Search, Google Maps, Google Sites, and 3 more
+	Congo (DRC)	YouTube
+	Congo (Republic)	Google Search
+	Egypt	Google Search
+	Georgia	Google Search
+	Hong Kong	Google Search
+	Indonesia	Google Search
+	Iran	Google Sites, Gmail, Google Videos, YouTube
+	Iraq	YouTube, Google Search
+	Kazakhstan	Blogger
+	Kenya	Google Search
+	Libya	Google Search, YouTube
+	Morocco	Google Earth
+	Myanmar (Burma)	Google Search, YouTube
+	Pakistan	YouTube
+	Palestine	Google Search
+	Senegal	Google Search
+	Sudan	Google Search, YouTube
+	Syria	Google Search, YouTube
+	Tajikistan	YouTube
+	Trinidad & Tobago	Google Search
+	Turkey	YouTube, Blogger, Google Translate, Google Books, and 2 more
+	Uzbekistan	Google Search

## Reasons for Content Removal Request



*Total 68 instances of blocking occurred during June 2010-June 2015, Google Search & YOUTUBE were the most affected ones.*

# CONTENT FILTERING: IN OTT DOMAIN (Contd.)

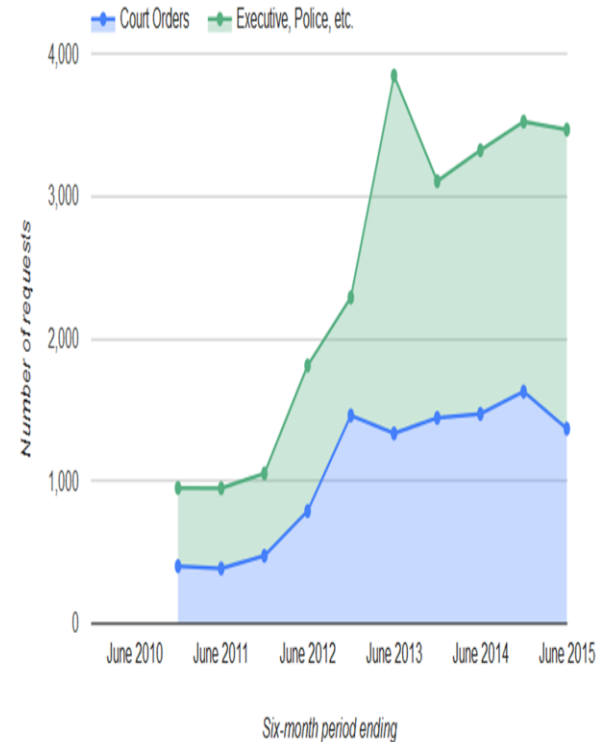
Google regularly receives requests from [copyright owners](#) and [reporting organizations](#) that represent them to remove search results that link to material that allegedly infringes copyrights. Each request names specific URLs to be removed, and we list the domain portions of URLs requested to be removed under [specified domains](#).

### URLs requested to be removed from Search per week



## Removal requests by the numbers

[See all data](#)



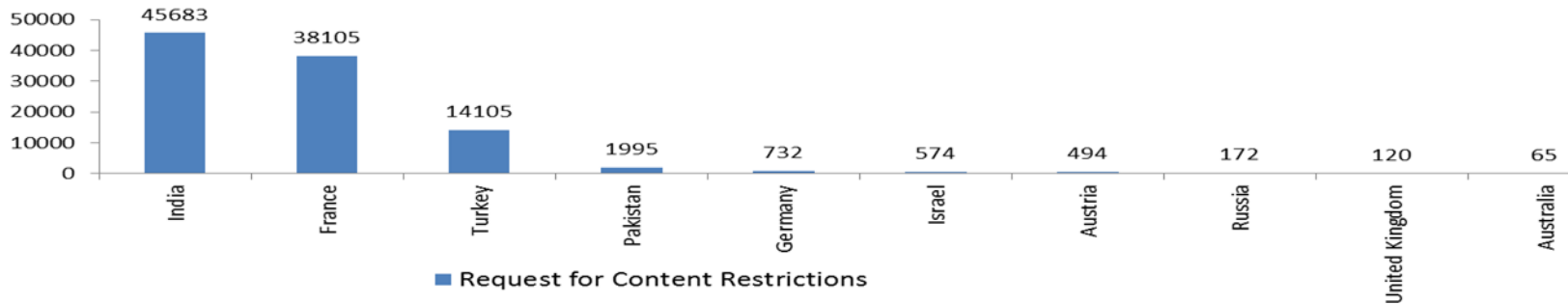
Total removal requests by branch of government that issued a request.

We did not begin providing branch information until December 2010 reporting period.

# CONTENT FILTERING: IN OTT DOMAIN (Contd.)

## Recent Statistics on Content Filtering-Facebook

**Countries Placing Highest Requests for Content Restrictions (2015)**



## Few Examples-Facebook's Policy While Serving Such Requests

- **Country:** United Kingdom
  - **Date:** December 2015
  - **Content:** A number of Facebook groups related to raffles.
  - **Request:** We received a request from the UK Gambling Commission to remove several groups advertising and coordinating raffles.
  - **Result:** We reviewed the pages and determined that the groups did not violate our Community Standards. We restricted access to the groups in the UK, but not in other countries.
- **Country:** United States
  - **Date:** October 2015
  - **Content:** A page protesting a county animal control agency.
  - **Request:** We received a request from a county prosecutor's office to remove a page opposing a county animal control agency, alleging that the page made threatening comments about the director of the agency and violated laws against menacing.
  - **Result:** We reviewed the content and determined that the page did not contain credible threats and therefore did not violate our Community Standards. We took no other action on the page for reasons of the public interest.

- **Country:** France
  - **Date:** November 2015
  - **Content:** Photo of terrorist attack victims.
  - **Request:** Following the November 2015 terrorist attacks in Paris, we received a request from L'Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC), a division of French law enforcement, to remove a number of instances of a photo taken inside the Bataclan concert venue depicting the remains of several victims. The photo was alleged to violate French laws related to protecting human dignity.
  - **Result:** We determined that the photo did not violate our Community Standards when it was shared to denounce the attack or to show compassion for victims. We restricted access to 32,100 such instances of the photo in France, but not in other countries.
- **Country:** India
  - **Date:** September 2015
  - **Content:** Image depicting a boy urinating on the Indian National Flag.
  - **Request:** We received a request from law enforcement in India to remove an image depicting a boy urinating on the Indian National Flag. Law enforcement alleged the content was prohibited by laws regarding respect for the national flag and that the image could cause a serious law and order problem.
  - **Result:** We determined that the photo did not violate our Community Standards. We reviewed the content and made the photo inaccessible in India.



# CONTENT FILTERING: IN OTT DOMAIN (Contd.)

## Recent Statistics on Content Filtering- Microsoft

### Government Requests for Content Removal

When Microsoft receives a government request to remove content, we carefully review and assess the demand to understand the reason for the request, the authority of the requesting party, the applicable policies or terms of use for the affected product or service, and our commitments to our customers and users with regard to freedom of expression. Based on these reviews, we determine whether and to what extent we should remove the content in question. The report includes government requests for the removal of content for Microsoft consumer online services, such as Bing, OneDrive, Bing Ads and MSN.

#### Government Requests for Content Removal by Country, July-December 2015

	Requests	Action Taken	Percentage - Action Taken
China	165	142	86%
France	28	28	100%
Germany	6	6	100%
India	2	0	0%
Russia	1	0	0%
United Kingdom	13	10	77%
United States	2	2	100%
<b>TOTAL</b>	<b>217</b>	<b>188</b>	<b>87%</b>

# CONTENT FILTERING: IN OTT DOMAIN (Contd.)

## Copyright Removal Requests

As an intellectual property company itself, Microsoft encourages respect for intellectual property, including copyrights. We also are committed to freedom of expression and the rights of users to engage in uses that may be permissible under applicable copyright laws. Links to webpages containing material that infringes the rights of copyright owners may be removed from our search results provided we receive a legally sufficient notice of infringement from an owner or an authorized agent acting on that owner's behalf. The following numbers relate to requests to remove links to webpages from our Bing search engine results.

Copyright Removal Requests, July-December 2015				
Requests	URLs Requested	URLs Accepted	URLs Rejected	Percentage of URLs Accepted
976,134	59,473,002	58,487,912	985,090	98%

**Note:** The data above details compliant removal requests received by Bing for removal of algorithmic search results. The report does not include copyright removal requests from the Bing image or video index, from Bing Ads, or requests initially deemed non-compliant during preliminary reviews conducted prior to entry of the request into our standard tracking tools. The data includes more than 95 percent of the copyright removal requests for Bing for the six-month reporting period.

## Requests for Removal of 'Revenge Porn'

In July 2015, Microsoft announced it would remove reported links to photos and videos from search results in Bing globally, and remove access to the content itself when shared on OneDrive or Xbox Live, when we are notified by an identifiable victim of the sharing of nude or sexually explicit images online without that person's consent (also referred to as 'non-consensual pornography').

'Revenge Porn' Removal Requests, July - December 2015			
	Requests Reported	Requests Accepted	Percent Requests Accepted
<b>Total</b>	<b>537</b>	<b>338</b>	<b>63%</b>

**Note:** Numbers are aggregated across Bing, OneDrive, and Xbox Live for which a content removal request was received during this reporting period.

# CONTENT FILTERING: IN OTT DOMAIN (Contd.)

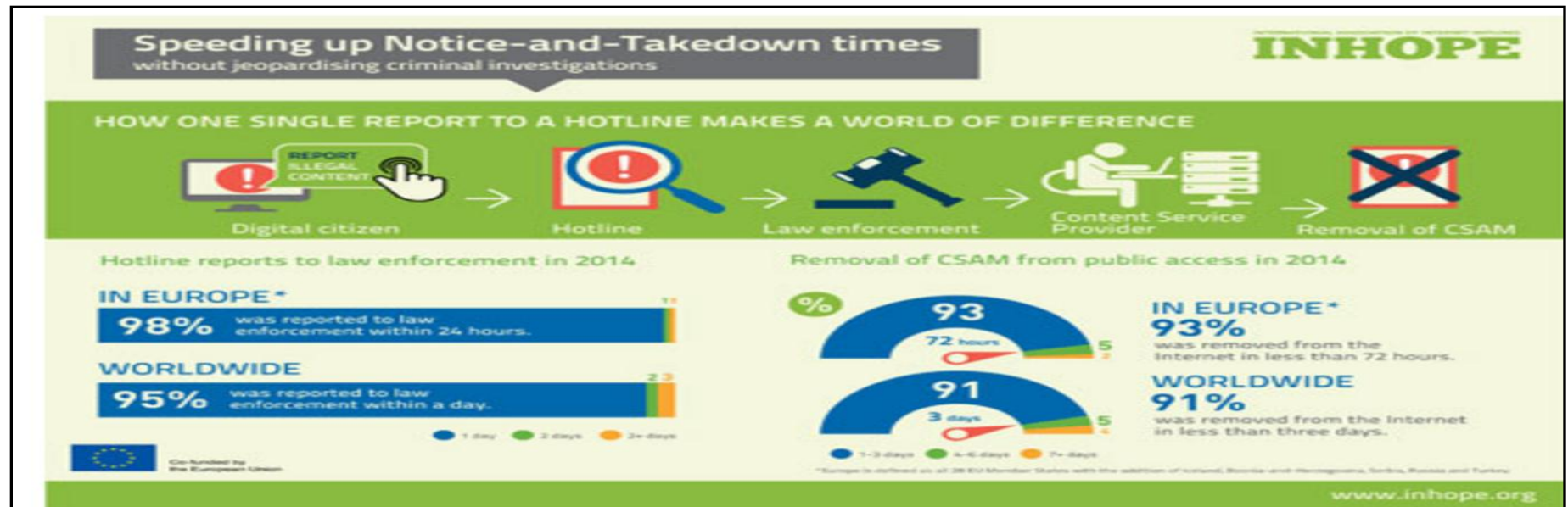
## 'Right to Be Forgotten' Requests

In May 2014, the European Court of Justice ruled that European residents could ask search engines to filter results for queries that include their name if the results are inadequate, inaccurate, no longer relevant, or excessive. As a result, Microsoft has put in place procedures to ensure we comply with the ruling in ways that appropriately balance individuals' rights to privacy with the general public's interest in freedom of expression and the free availability of information online.

### Cumulative 'Right To Be Forgotten' Requests, May 2014 - December 2015

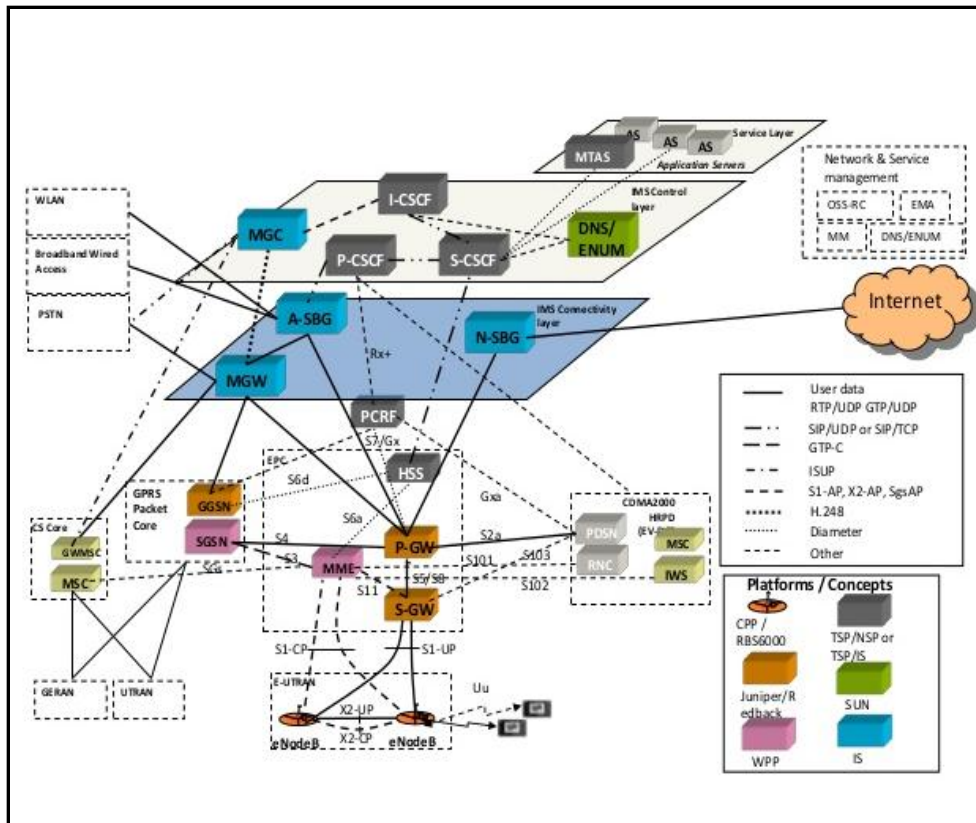
	Requests Received and Processed	URLs Requested	URLs Accepted	URLs Rejected	Percentage of URLs Accepted
<b>TOTAL</b>	<b>9,815</b>	<b>24,812</b>	<b>10,050</b>	<b>13,135</b>	<b>43%</b>

**Note:** This table shows the number of URLs that were accepted and rejected for requests received between May 2014 through December 31, 2015 that were processed as of March 1, 2016. The number of URLs accepted and rejected do not reflect requests still pending review as of March 1, 2016. For example, processing delays may result if more information is needed to complete the review on a request.



# CONTENT FILTERING : IN NETWORK DOMAIN

Content filtering is a usual operation in network domain, performed by **ISPs (wired & wireless)** & associated entities (like: International Internet Gateways, International Roaming Partners).



*A Typical Mobile Broadband Network Architecture*

**Common mechanisms for content filtering in mobile broadband network are:**

- \*Through DPI (standalone/in sync with PCRF)

- \*Through ICAP Server (standalone/in sync with PCRF)

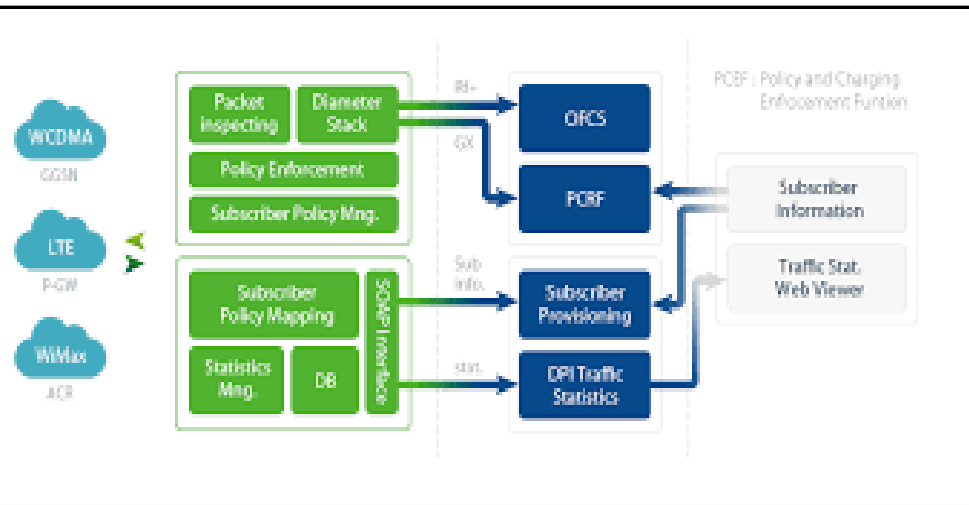
- \*Through DNS

- \*Through FIREWALL

- \* Through multiple nodes (combination of different mechanisms)



# CONTENT FILTERING : THROUGH DPI

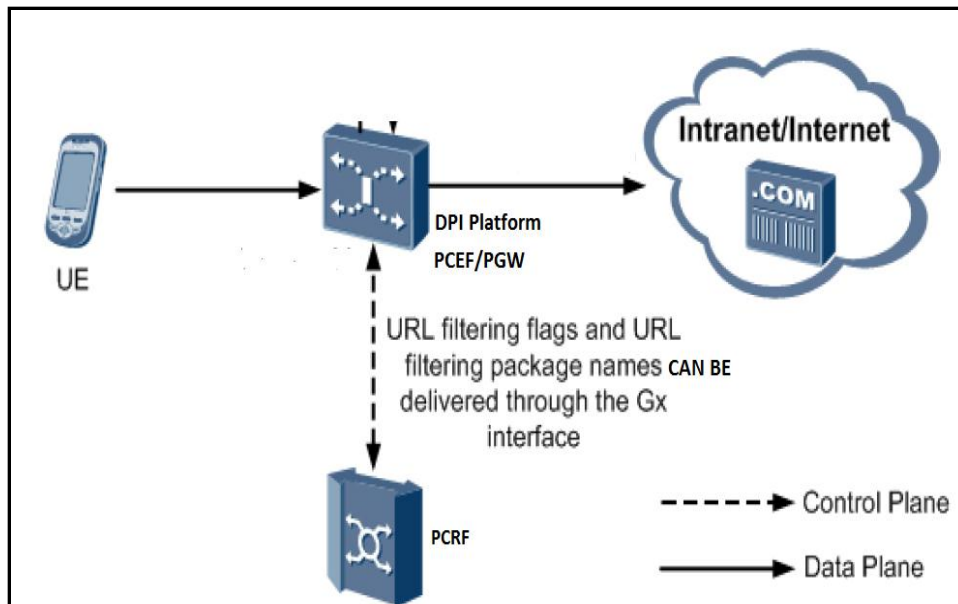


➤ Through relevant DPI platform (standalone DPI like: PCEF or integrated DPI like GGSN/ PGW); entire traffic get checked against pre-defined content filtering rules.

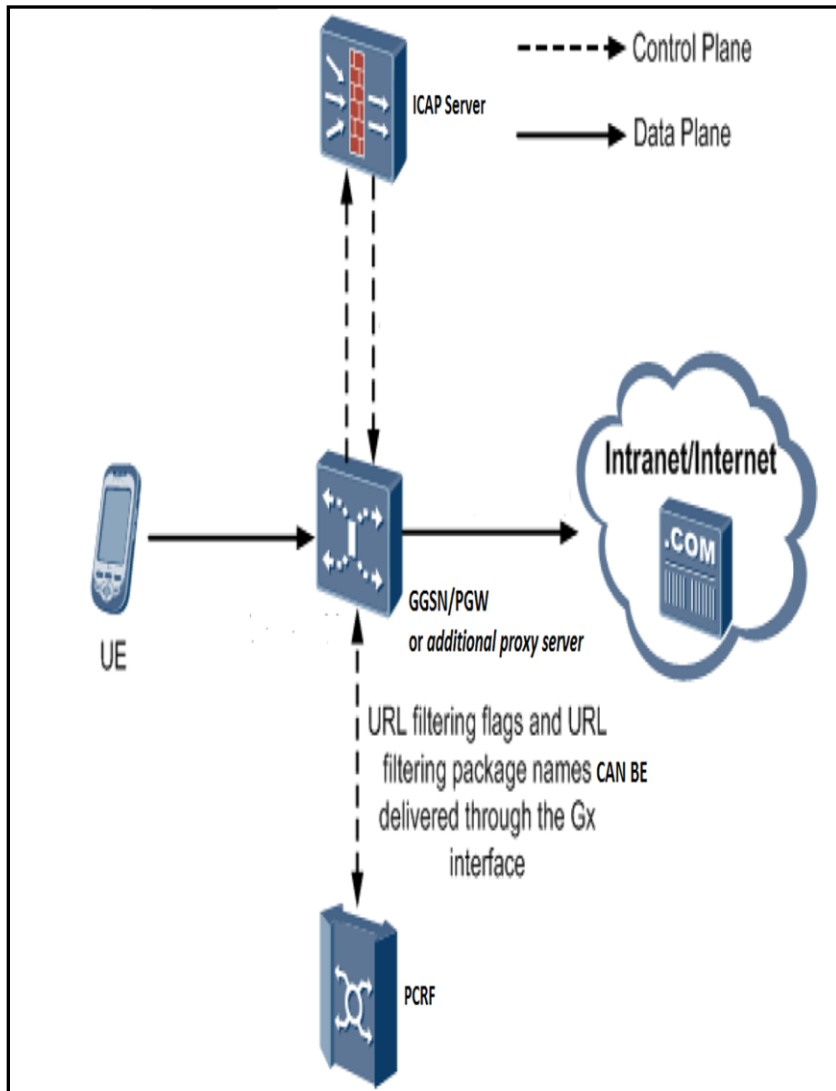
➤ The DPI can be synced with PCRF (or other relevant policy server) to serve segregated (consumer segment based/particular package based) requirements.

➤ Ensures accurate matching of content in most cases through deep level inspection.

➤ Can create extra processing load on DPI node & additional latency for whole traffic.



# CONTENT FILTERING : THROUGH ICAP SERVER

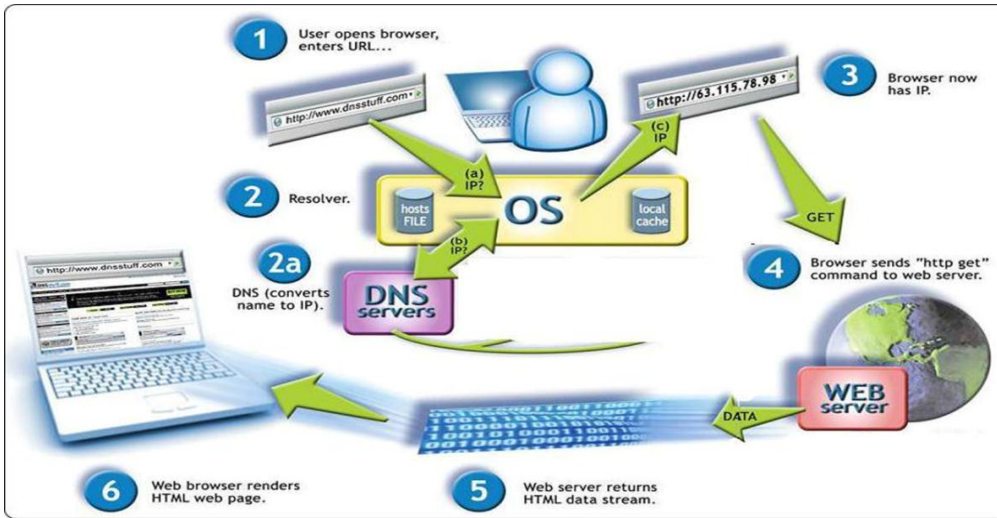


**ICAP- Internet Content Adaptation Protocol (ICAP)** is a lightweight HTTP-like protocol specified in RFC 3507.

**Functionality:** The client sends out a request for a web page and GGSN/PGW or other proxy server redirects that request to the ICAP server. The ICAP server parses the HTML request and performs URL-based filtering by comparing the request URL to a list of "banned" URLs. If the URL is on the "banned" list, then the client's request is modified to request an error message from the origin server or, more likely, from the proxy server (cache). This error message is then supplied to the client. If the origin server URL was not banned, the ICAP server would forward the request to the origin server via the proxy server and the request would be fulfilled.

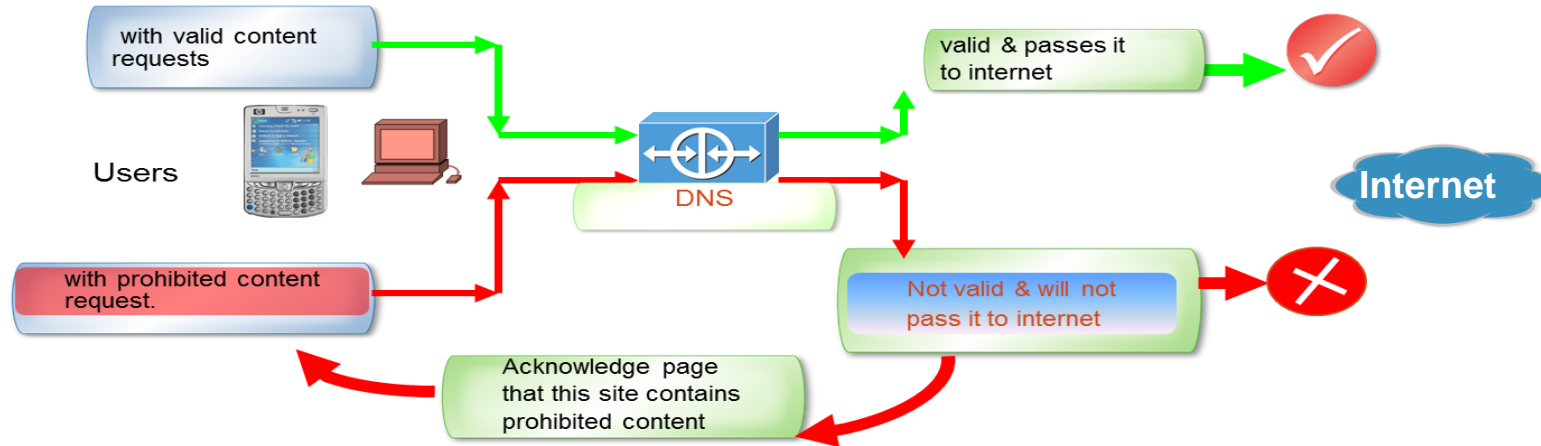
It is a standard solution for serving generalized (mass level subscribers) requirements of content filtering, however it can work for only HTTP traffic.

# CONTENT FILTERING : THROUGH DNS



## Basic DNS Functionality

- Through DNS based static policy, access restriction can be performed for blacklisted URLs & IPs.
- High level of accuracy can be ensured.
- However, it is not an appropriate solution to cater consumer segment based/particular product package based requirements; as in most cases DNS policies apply for full subscriber base, at least for one board service category (APN).



## URL Filtering Through DNS

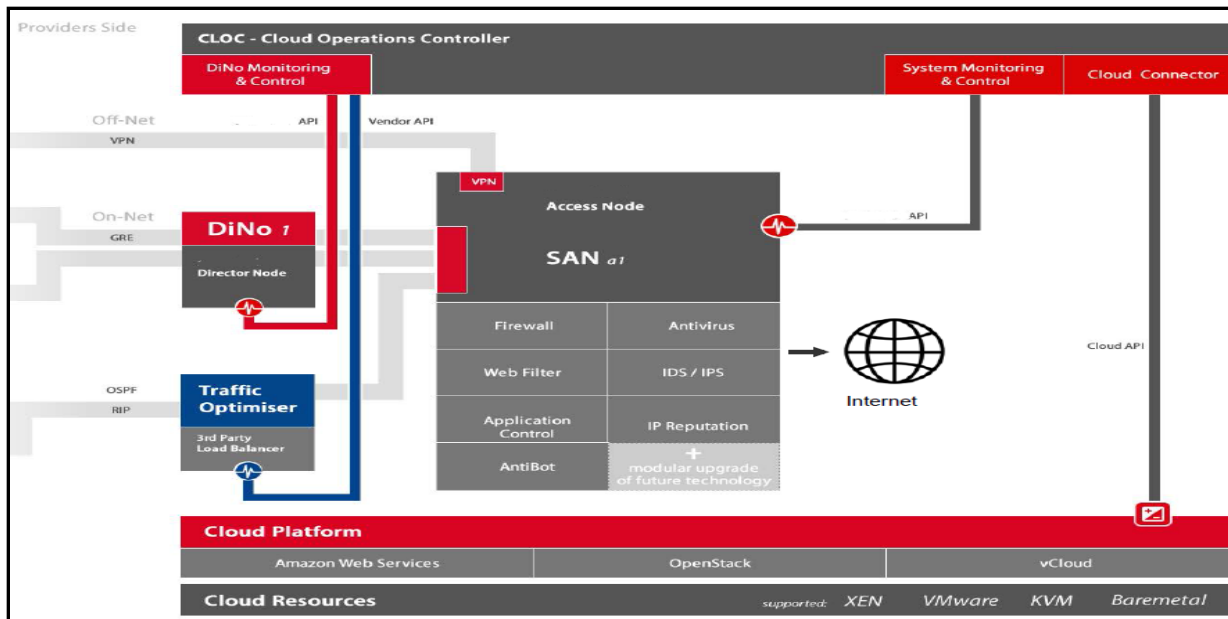


# CONTENT FILTERING : THROUGH FIREWALL



➤ Through access control rules in firewall (or in the routers of aggregation or gateway layer); restriction can be used for certain IP, protocol or port.

➤ However, accuracy level continuously fluctuates as IP of the targeted URLs can change any time. Also, it increases processing load in the corresponding device (firewall/router).



*Customized solution platform for content filtering (combining multiple mechanism in native/ cloud based /virtualized platforms) have emerged as well*

A hybrid solution platform combining multiple mechanisms

# CONTENT FILTERING : COMPARISON OF DIFFERENT MECHANISMS

Factors	DPI Based	DNS Based	ICAP Server Based	Firewall Based
Accuracy in filtering	High	High	High	No URL based policy; works on IP/port/protocol
Filterable content types	Broad	Broad	No HTTPS, only HTTP	Broad
Customization of policy based on subscriber segment/packages	Possible	Limited	Limited	Not Possible
Impact on traffic flow & node	Increase in traffic latency & processing load	Less impact	Increase in traffic latency	Increase in traffic latency & processing load



**Bypassing attempt against any content filtering policy** (attempting to access the restricted content through fraudulent techniques) is a common tendency in user end.

So for content filtering, **continuous challenge remains for mobile broadband operators to chose the best possible mechanism or best combination of different mechanisms to get the most secured outcome while maintaining a positive balance between all related factors.**

# CONTENT FILTERING IN COMBINED MANNER : AN EXAMPLE

During Sep 2012 to May 2013, YOUTUBE was blocked in Bangladesh as per regulatory instruction. To ensure complete blocking of YOUTUBE, a topmost mobile broadband operator of Bangladesh then implemented a multi-layered scheme.

## Bangladesh lifts ban on YouTube, blocked after anti-Islam film

REUTERS — PUBLISHED JUN 05, 2013 08:22PM

Like 0 Tweet Share 9 COMMENTS EMAIL PRINT



— File Photo

DHAKA - Bangladesh on Wednesday lifted a ban on video-sharing site YouTube which has been blocked since September after an online

## Three Layer Blocking

YouTube domain blocked from DNS

```
> youtube.com
Server: uranus.grameenphone.com
Address: 10.10.20.76

DNS request timed out.
        timeout was 2 seconds.
*** Request to uranus.grameenphone.com timed-out
```

L1

Google Global Cache made offline from the network



L2

Google Global Cache

YouTube IP as destination is blocked



L3

Border Gateway Router



# References

- Google Transparency Report: <https://www.google.com/transparencyreport/>
- Facebook Global Government Request Report: [https://web.facebook.com/about/government\\_requests?\\_rdr](https://web.facebook.com/about/government_requests?_rdr)
- Microsoft Transparency Report : <https://www.microsoft.com/about/csr/transparencyhub/>
- GSMA Youth Flier : [www.gsma.com](http://www.gsma.com)
- UNICEF Guidelines for Industry on Child Online Protection: [www.unicef.org](http://www.unicef.org)
- ICAP Whitepaper: [www.icap-forum.org/](http://www.icap-forum.org/)
- INHOPE : <http://www.inhope.org/gns/home.aspx>

*THANK you*