CONTENT FILTERING: PERSPECTIVES & CHALLENGES FOR MOBILE BROADBAND OPERATORS

Azfar Adib
Lead Engineer, Grameenphone Ltd.
Dhaka, Bangladesh
azfar@grameenphone.com

SANOG 28 1ST-9TH 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

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
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


Topic: Military Coup Attempt in Turkey (244)

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.

NNKARA (Sputnik) - Earlier on Wednesday the whisteblowing 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.
MINISTER ASKS INDIAN ISPS TO PERMANENTLY BLOCK HUNDREDS OF ‘PIRATE’ SITES

By Andy On October 29, 2015

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.
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.

Business Segment

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

Consumer Segment

Content filtering, commonly defined as “Parental Control”, is a popular requirement in consumer segments as well.
Mobile Broadband Operators may require to apply content filtering policies for own sake to prevent charging fraud, security threats and complying organizational guideline.
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.

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

THE MEMBERS OF THE MOBILE ALLIANCE INCLUDE:

Deutsche Telekom Group
Dialog Austria Telekom
EE
Mobitel
MTN Group

Orange Group
Telecom Italia
Teléfonica Group
Telmex Group
TeliaSonera Group
Vodacom SA
Vodafone Group
Zain 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.

Being implemented through

- Mobile Operators
- Internet Service Providers
- Content providers & app developers
- National & public service broadcasting
- HW manufacturer & OS developers
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 easy 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 or equivalent bodies to combat illegal content on the Internet.

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
- Alans Mobiletelefon
- Belgacom
- Bouygues Telecom
- Cosmote
- CYTA
- Deutsche Telekom Group
- Eiris Eeth AS
- Hutchison 3G Europe
- Go Mobile
- KPN
- Mobilkom Austria
- MobileEAD
- Mobile
- Orange France Telecom Group
- P&T Luxembourg
- SFR
- Tele2
- Telecom Italia
- Telefónica
- Telefonica
- Telenor
- Telenor Telekom
- 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, 380 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.”

Kaiu Karavela, 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.gsmaeurope.org/safer_mobile/ or contact Alice Valvodova at GSMA Europe (avalvodova@gsma.org).
CONTENT FILTERING: DOMAINS OF EXECUTION

<table>
<thead>
<tr>
<th>User Domain</th>
<th>Network Domain</th>
<th>OTT Domain</th>
</tr>
</thead>
</table>

- **User Domain**
  - Tablets
  - Laptops

- **Network Domain**
  - Diagram showing various ISPs and network connectivity

- **OTT Domain**
  - Various OTT service icons and logos
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.
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**

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turkey</td>
<td>4612</td>
</tr>
<tr>
<td>Brazil</td>
<td>4122</td>
</tr>
<tr>
<td>Russia</td>
<td>3677</td>
</tr>
<tr>
<td>United States</td>
<td>3421</td>
</tr>
<tr>
<td>India</td>
<td>1744</td>
</tr>
<tr>
<td>Germany</td>
<td>1712</td>
</tr>
<tr>
<td>South Korea</td>
<td>1037</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>959</td>
</tr>
<tr>
<td>France</td>
<td>846</td>
</tr>
<tr>
<td>Italy</td>
<td>651</td>
</tr>
<tr>
<td>Spain</td>
<td>556</td>
</tr>
<tr>
<td>Argentina</td>
<td>376</td>
</tr>
<tr>
<td>Japan</td>
<td>346</td>
</tr>
<tr>
<td>Canada</td>
<td>308</td>
</tr>
<tr>
<td>Israel</td>
<td>220</td>
</tr>
<tr>
<td>Libya</td>
<td>219</td>
</tr>
<tr>
<td>Australia</td>
<td>203</td>
</tr>
<tr>
<td>Taiwan</td>
<td>201</td>
</tr>
<tr>
<td>Switzerland</td>
<td>114</td>
</tr>
<tr>
<td>Netherlands</td>
<td>102</td>
</tr>
</tbody>
</table>

Number of Requests
CONTENT FILTERING: IN OTT DOMAIN (Contd.)

Domain wise Request Count

Google domains being blocked in different countries

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

- Oct 15, 2012: 6,000,000
- Jan 13, 2014: 12,000,000
- Apr 13, 2015: 24,000,000

### Removal requests by the numbers

- Court Orders
- Executive, Police, etc.

**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

<table>
<thead>
<tr>
<th>Countries Placing Highest Requests for Content Restrictions (2015)</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
</tr>
<tr>
<td>France</td>
</tr>
<tr>
<td>Turkey</td>
</tr>
<tr>
<td>Pakistan</td>
</tr>
<tr>
<td>Germany</td>
</tr>
<tr>
<td>Israel</td>
</tr>
<tr>
<td>Austria</td>
</tr>
<tr>
<td>Russia</td>
</tr>
<tr>
<td>United Kingdom</td>
</tr>
<tr>
<td>Australia</td>
</tr>
</tbody>
</table>

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 Lée 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.
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.

<table>
<thead>
<tr>
<th>Country</th>
<th>Requests</th>
<th>Action Taken</th>
<th>Percentage - Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>165</td>
<td>142</td>
<td>86%</td>
</tr>
<tr>
<td>France</td>
<td>28</td>
<td>28</td>
<td>100%</td>
</tr>
<tr>
<td>Germany</td>
<td>6</td>
<td>6</td>
<td>100%</td>
</tr>
<tr>
<td>India</td>
<td>2</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Russia</td>
<td>1</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>13</td>
<td>10</td>
<td>77%</td>
</tr>
<tr>
<td>United States</td>
<td>2</td>
<td>2</td>
<td>100%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>217</strong></td>
<td><strong>188</strong></td>
<td><strong>87%</strong></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Copyright Removal Requests, July-December 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>976,134</td>
</tr>
</tbody>
</table>

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').

<table>
<thead>
<tr>
<th>'Revenge Porn' Removal Requests, July - December 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests Reported</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Requested and Processed</th>
<th>URLs Requested</th>
<th>URLs Accepted</th>
<th>URLs Rejected</th>
<th>Percentage of URLs Accepted</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTAL</td>
<td>9,815</td>
<td>24,812</td>
<td>10,050</td>
<td>13,135</td>
</tr>
</tbody>
</table>

*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.*

---

Speeding up Notice-and-Takedown times without jeopardising criminal investigations

HOW ONE SINGLE REPORT TO A HOTLINE MAKES A WORLD OF DIFFERENCE

Digital citizen → Hotline → Law enforcement → Content Service Provider → Removal of CSAM

Hotline reports to law enforcement in 2014

- IN EUROPE: 98% was reported to law enforcement within 24 hours.
- WORLDWIDE: 95% was reported to law enforcement within a day.

Removal of CSAM from public access in 2014

- IN EUROPE: 93% was removed from the Internet in less than 72 hours.
- WORLDWIDE: 91% was removed from the Internet in less than three days.
Content filtering is a usual operation in network domain, performed by ISPs (wired & wireless) & associated entities (like: International Internet Gateways, International Roaming Partners).

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)
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.
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.
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).
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

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

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.**
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.

Three Layer Blocking

YouTube domain blocked from DNS

L1

Google Global Cache made offline from the network

L2

YouTube IP as destination is blocked

L3

Facebook Global Government Request Report:  
https://web.facebook.com/about/government_requests?_rdr

Microsoft Transparency Report:  
https://www.microsoft.com/about/csr/transparencyhub/

GSMA Youth Flier:  www.gsma.com

UNICEF Guidelines for Industry on Child Online Protection:  www.unicef.org

ICAP Whitepaper:  www.icap-forum.org/

THANK YOU