Mobile Operator's Contribution to
Notice and Take Down in the Context of Illegal Child Sexual Abuse Content

Section 1- Introduction and summary

The objective of this paper is demonstrate that the European members of the Mobile Alliance[1] have processes in place to deal with the removal of illegal content[2] that may be hosted on their networks.

The paper focuses on the following areas:

- Defining notice and take down
- Providing a background to European strategy for reporting of illegal content
- Describing how customers report illegal content
- Detailing how the notice and take down process works
- Outlining the mobile industry's relationship with key stakeholders
- Summary and conclusions

Section 2- Defining notice and take down

A notice can be any report from the general public, a customer, a hotline, or a law enforcement agency that alerts the mobile operator to the existence of potentially unlawful content being hosted on their network. The European Union recently updated its laws with regard to the removal of illegal content, making it mandatory across all member states. The relevant directive is the **EC Directive on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA**. Article 25 states that:

> *Member States shall take the necessary measures to ensure the prompt removal of webpages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.*

This Directive ensures that all illegal content is removed promptly, leaving no question that those companies who host content, once informed of the existence of illegal content on their networks are obligated to remove it.

It is also worth noting that the Electronic Commerce (EC Directive) Regulation from 2002 ensures that information society providers are not criminally liable for child sexual abuse content passing across their networks as they are acting as conduits, or for hosting and caching criminal content. This is contingent on the providers acting expeditiously to remove or to disable access to the information stored upon obtaining actual knowledge of the fact or that a court or an administrative authority has ordered such removal or disablement. In practice this means that unless the information comes from an authoritative source, providers will invariably undertake a process to verify the illegality for

[1] The Mobile Alliance against child sexual abuse content is a global voluntary initiative run by the GSMA, where mobile operators sign up to commit to ensure that their networks remain hostile to illegal child abuse content. European members include Deutsche Telekom Group, Hutchison 3G Europe, Meteor, Orange FT Group, Telecom Italia, Telefonica Group, Telekom Austria, Telenor Group, TeliaSonera Group, and Vodafone Group. For more information visit: www.gsma.com/publicpolicy/myouth/mobiles-contribution-to-child-protection/mobile-alliance/

[2] All references in this paper to illegal content refer only to illegal child sexual abuse content.

fear of compromising a police investigation by removing or disabling access which may in turn alert an offender and conceivably jeopardise the rescue of a child at risk.

Section 3 - Background: setting up a European reporting strategy

To properly understand the role that mobile operators play in the notice and take down process, it is also vital to be familiar with the other stakeholders involved in the process. The other key players are hotlines and law enforcement agencies (LEA's). From a strategic perspective the concept of a European network of hotlines for receiving anonymous reports from the public of child sexual abuse content was instigated in 1996 by the EU. This initiative was launched because the public were and remain unwilling to report such material to law enforcement agencies out of a fear that personal details will be used to trace and possibly prosecute those making the reports.

The network of hotlines (INHOPE) has grown incrementally on a global basis with over 41 Hotlines now in existence across 36 Countries. With just one exception[3], all European member states now have at least one hotline. However, the drive to set up a network of hotlines across Europe has led to a patch work of hotlines, some operating under the umbrella of Child Safety/Protection Organisations, some as part of an ISP Trade Association and some like the Internet Watch Foundation (IWF) in the UK are independent entities.

Although a minimum criteria must be reached before a hotline can be admitted to INHOPE and receive EU funding, most hotlines, have their own model of governance based on local legal jurisdiction and their relationship with local law enforcement agencies. Some hotlines are legally indemnified to view reports of illegal content and make judgements on the content based on their national laws. In other cases, hotlines don't have the authority to review content and they act merely as a conduit for passing reports on to law enforcement.

Section 4 - Customer reporting of illegal content

This section covers how mobile operators provide information to customers on how to make a report of suspected illegal content and the role of search engines in the reporting process. Details on how mobile operators deal with the illegal content once a report is made is covered in section 5.

4. 1 - How the mobile industry communicates reporting of illegal content with its customers

Mobile operators provide guidance and information to their customers on how to report illegal content. This information is normally contained on the operator's website or it is made available via customer service agents for telephone enquiries. To demonstrate what information mobile operators make available, some examples of screen shots of webpages are included on the next page.

[3] Sweden does not have a specific hotline for the reporting of illegal child abuse images.

Figure 1- United Kingdom

Figure 2- Italy

Figure 3 - Spain and Germany

4. 2 - Other ways to report suspected illegal content
Hotlines exist to field and process reports of illegal content. Most reports of illegal content received by hotlines do not come from mobile operator's websites**.** Research indicates that the most common method of reporting illegal content is via search engine.

Statistics from the IWF in the UK indicate that in 2011 the majority of referrals to its reporting page came from Google (see figure 4). Overall, 82% of all reports came from sources other than mobile operators. The first mobile operator to feature in the IWF statistics is Orange with 0.04% of referrals to the IWF reporting page. In real terms this equals approximately 31 reports, which illustrates that customers don't naturally think to report illegal content to their mobile service provider.

Figure 4

Referral website	% of referrals (represents a total of 78,729 unique views)
Google	56%
Direct (no referrer)	15%
Facebook	5%
CEOP	3%
Family Online Safety Institute (FOSI)	3%
Orange	0.04%

At Protegeles, the Spanish hotline, 75% of reports are generated via direct traffic, where the user types the URL (www.protegeles.com) directly into the search engine. 12% of its traffic comes from links from other websites, which include reports generated from clicking on an icon (see figure 5) that Spanish operators make available on their websites. Finally, 11% of reports to Protegeles are received via search engine, where users type in words such as "protegeles", or "how to report a website", "child pornography" or "report child pornography".

Figure 5

Section 5 - *Notice and take down- how the process works*
The section covers the steps that mobile operators undertake to implement a take down process within their organisation and provides detail on what a mobile operators does when a report is made.

5.1 - Establishing a notice and take down process
There are a number of steps that mobile operators undertake to implement a notice and take down process within their company. All European mobile operators within the Mobile Alliance have these

processes in place, so this section simply illustrates a general procedure that has already been implemented.

I. Review of *terms and conditions* for operator-hosted user-interactive content services

Company Terms and Conditions (T&Cs) are used to define the 'house rules' that enable organisations to prohibit child sexual abuse content. T&Cs relate to services provided by a company, a mobile operator in this case, giving them the scope to be as specific and inclusive as is appropriate – for example allowing for the inclusion of a definition of child sexual abuse content as spelled out by relevant national legislation. The T&Cs reflect both legal liabilities and customer responsibilities with regard to illegal content. The T&Cs also specify what rights and powers a company reserves to itself (e.g. to investigate reports of content in breach of T&Cs, removal content, informing the police, closing the user's account etc.)

II. Some mobile operators also offer *user guidelines* for their operator-hosted user-interactive content services

These guidelines tend to echo the key points from the T&Cs in user-friendly language in an 'acceptable use guide', which reminds users of how the services should be used, and what will happen if the guidelines are not respected.

III. Implementation of suitable *reporting mechanisms*

Some operators allow for the reporting of the discovery of child sexual abuse content via email, phone, or through a report abuse 'button' that leads to a reporting hotline or law enforcement authority. In some cases the reporting mechanism is tied in with existing processes for reporting e.g. nuisance or malicious calls. In some cases reports of "inappropriate" content are dealt with internally, but reports of potential child sexual abuse (or other types of illegal) content, are referred directly to the national hotline / law enforcement agency for review.

IV. Development of back-end *processes* for handling reports and *removing child sexual abuse content*

The notice and take down processes followed by mobile operators focuses on the removal of illegal content, and ties in with the 'house rules' presented in the T&Cs. It is also dictated by national laws. In some cases, those that host suspected illegal content cannot remove it, until they are given clearance by law enforcement to do so. Mobile operators also adopt any national terms that may exist for notice and take down (e.g. for response times for removal once a notice is issued). Operators also have structures in place to decide how to respond to complaints, clarify where different types of content are reviewed and how decisions are reached on whether or not it is acceptable.

Additionally, mobile operators have developed procedures to ensure that their front line / contact centre staff are well-prepared for dealing with complaints. In all cases, the priority for mobile operators is the swift isolation and removal of illegal content when notified of its presence (i.e. when issued with an NTD notice) by the relevant law enforcement or hotline.

V. 3rd Party contracts

The final consideration taken by mobile operators is the review of existing contracts to ensure that they contain a requirement for 3rd parties to follow the company process for notice and take down.

5.2 - How a report is dealt with

Mobile operators that are part of the Mobile Alliance are required to implement notice and take down processes to enable the removal of child sexual abuse images from public view that are hosted on their services as soon as they are reported or requested to do, whether this is through a national hotline, or law enforcement. Each operator follows a different process based on company policy and national legislation.

In terms of customer communication, in some companies, the operator will place a phone call to the customer who makes a report, and in other companies a more formal email is sent. One operator, as an example, sends the following note to whoever submitted the report:

Figure 6

Response to report of child at risk / criminal activity

Dear [*insert name*],

Thank you for your report to the x team. We take all reports of this nature very seriously and will look into this matter urgently. We may get back to you with further questions.

We appreciate your help in keeping the x a safe place for all of our users.

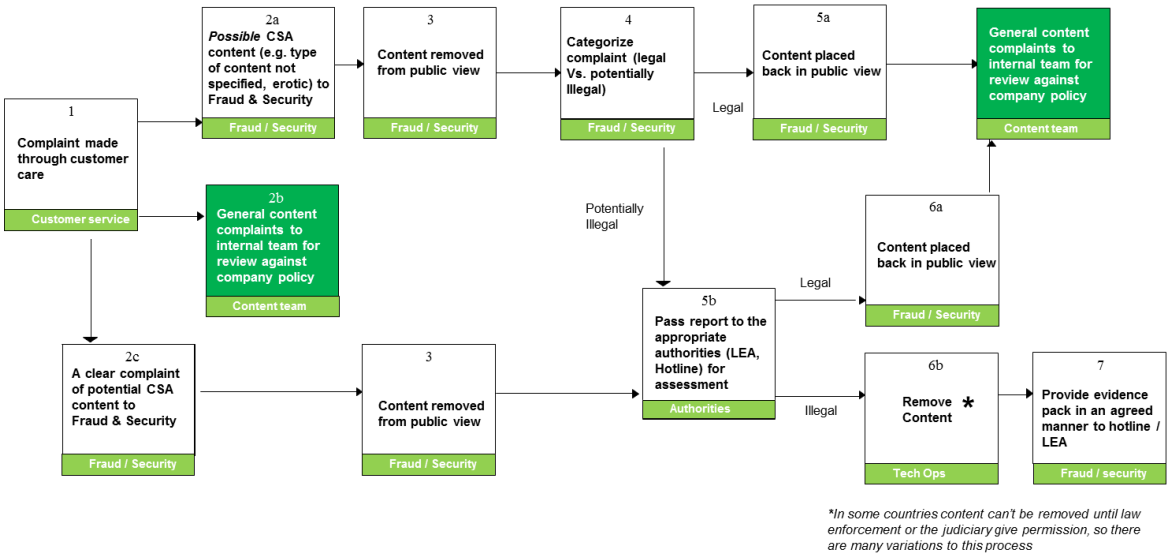
Kind regards,
X Customer Services

In Europe, an operator's notice and take down process is guided by national law and is linked to the appropriate national authority (hotline organisation or law enforcement agency) so the responsibility for assessing if an image is illegal is taken by the authorities and not the mobile operator.

Mobile operators also ensure that their notice and take down processes protect staff from inappropriate exposure to the images and include liaising with and supporting law enforcement in the event of an investigation. When a notice is received from a member of the public, the mobile operator is obligated to pass the relevant information on to the local hotline or law enforcement agency. In some countries there is specific legislation to guide how illegal content is dealt with and in other countries there may be no specific legislation but accepted norms in place for how the process works.

Whilst few customers actually report illegal content to their mobile provider, all mobile operators have the relevant processes in place in the event that a customer does report illegal content. The chart below (figure 7) is a representation of a process followed by a mobile operator in a country where it is expected that content is immediately removed as soon as a report is made. In other countries, those hosting any suspected illegal content cannot take it down until advised by law enforcement to do so.

Figure 7



Section 6 - *The mobile industry's relationship with stakeholders*

Efforts for collaboration between industry and law enforcement are supported by the Council of Europe's **Guidelines for the cooperation between ISP's and law enforcement agencies** (LEA's)[4]. These guidelines may help law enforcement authorities and Internet service providers (ISP's) structure their interactions in relation to cybercrime issues. These guidelines are based on existing good practices and can be applied in any country around the world in accordance with national legislation. They respect the freedom of expression, privacy, the protection of personal data and other fundamental rights of citizens.

In addition, there are instances where industry, including mobile operators, goes beyond what is required by law to develop stronger relationships with their local hotlines and law enforcement. For example, in the UK, all IWF Members are bound by a Code of Practice[5] which requires them to remove or disable access to child sexual material hosted on their networks upon receipt of a notice from the IWF. In other European Countries alternative arrangements are in place but they very much depend on trusted partnerships between the hotline and industry.

In terms of going beyond what is required by law, in the Spanish code of conduct for safer mobile use, mobile operators have committed to display an icon on their website, which provides a link to the national hotline (see figure 5).

Furthermore, many mobile operators are committed to devoting resources to their criminal compliance units to ensure there is a professional structured approach to dealing with judicial investigations and requests for access to data.

Some areas for improvement have been identified. These include:

- A more streamlined operating framework across Europe for hotlines would be advantageous to companies that have multiple operations across Europe. Currently operators have to establish different relationship and polices in each country where they operate.

[4] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/default_EN.asp

[5] http://www.iwf.org.uk/members/funding-council/code-of-practice

- Mobile operators could benefit from law enforcement agencies structuring their resources along similar lines as industry. This could foster more effective and efficient relationships and understandings between the respective parties.

Section 7 - S*ummary and conclusions.*

In summary, this paper provides an explanation on how mobile operators deal with notice and take down processes across the different European countries. It also seeks to illustrate that legal frameworks dictate that industry follows different processes in each of the 27 European member states. There is no one simple model that can be applied to how the mobile industry deals with notice and takedown, although all members of the Mobile Alliance follow the general process of removing content.

Notice and takedown is an area of shared responsibility and mutual dependencies of hosting providers, Law Enforcement Authorities and hotlines. European mobile operators have well established practices and structures in place for effective notice and take down. To the knowledge of Mobile Alliance members, there is no issue with the timeframe in which they remove illegal content, once informed of its existence.

There are potential areas for improvement that could be made across all stakeholder groups, which should be taken into consideration by the European Commission. Such improvements could further improve the efficiency of notice and take down. The mobile industry remains committed to fighting illegal child abuse content on its networks and will continue with existing process and where any shortcomings are identified, the Mobile Alliance will work to improve on them.