Telefónica

Child pornography on internet Investigation and suppression

Marta Villén Sotomayor
Director of Logical Security and Internet Fraud Prevention

1. Introduction

At the present time, anyone in Europe with a computer and an internet connection can access images of the sexual abuse of children.

Internet has changed the child pornography market to the extent that it has a practical monopoly as a result of the advantages it presents to users, from the ease with which it is possible to download files, to the reduced financial costs, along with the possibility of reaching a high number of internet browsers which will permit exchanges to take place and provide the guarantee of anonymity.

Part of the material containing child abuse distributed online belongs to paying websites. These web sites normally display sample images of sexual abuse of children, inviting the user to pay a specific amount to become a member of the site and access further images and videos of child pornography. An analysis of paying websites offering this type of material has shown that these activities are developed by organised bands of criminals.

In the remaining material available the child pornography trafficker is replaced by consumers who associate informally on a non- profit basis acting in coordination to download large numbers of photographs or videos to their computers. This type of exchange replaces purchase from the trafficker and it is in this type of relation that the dissemination of privately produced pornography acquires relevance.

Furthermore, by using the same programme (eg P2P) the web permits the sharing of pornographic material in a computer with other users connected to the web without the need for any direct relation between them. This activity of users sharing material could

be considered to be distribution, as despite the fact that they do not send pornographic material to the rest of web users, they have nevertheless made it available to them by permitting third party access to their computer.

There has also been a considerable growth in the traffic of child pornography which means that there is an increase in demand.

2. Current Internet situation and successful cases

At present, all the European police forces are receiving a number of complaints and communications from the public and from NGOs concerned with this type of website. European citizens want action taken against this type of website, thus both police forces and companies in the sector need to prevent the indiscriminate advertising of this type of content or the involuntary redirection of users to these websites.

Initiatives carried out by alliances between the police and industry are basically designed on one hand to ensure that internet users throughout Europe and, in particular, parents and children, can enjoy a safer web and on the other, they are designed to destroy the bases of the demand for this kind of illegal material which will in turn lead to a decline in the amount of material produced and distributed.

In Europe one of the best examples of practices carried out to combat illegal content of sexual abuse of children online is that of British operators, (O2, Vodafone, Orange, 3 and T-Mobile, among others) who for some years now have been blocking URLs containing this type of content, with the result that since 2003 the United Kingdom only accounts for 1% of the global content currently circulating online, which implies a considerable reduction since 1997 when the United Kingdom was responsible for 18% of world content.

The Spanish company TERRA provides another example. By the end of 2002 the number of complaints or information received on sites containing child pornography through TERRA was quite alarming. In the month of September alone they received and processed as many as 226 items of information and throughout the whole of 2002 approximately 1200 personal web pages hosted by the company contained child pornography. TERRA's reaction in Spain was effective in that it closed and cleansed the approximately 300,000 personal web pages it currently hosted at that time.

Following TERRA España's reaction the change was radical and from 226 items of information in September 2002 the number dropped to 11 complaints received in December of the same year. In December 2003 only 5 items of information were received relating to child pornography which had managed to infiltrate personal web pages hosted by TERRA España. The figures speak for themselves.

3. Notice and Takedown

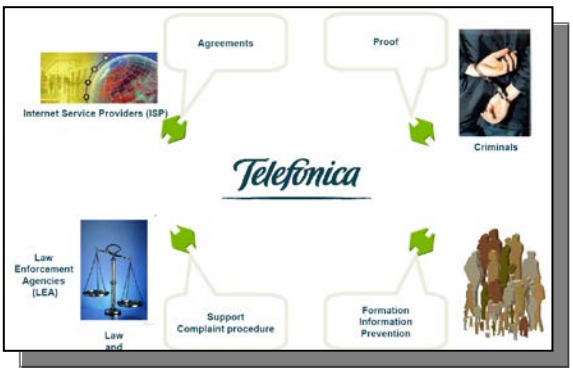
In 2008 a group of European operators: Telefónica, Hutchison, Mobilkom Austria Group, Orange FT Group, Telecom Italia, Telenor Group, Telia Sonera, T-Mobile, Vodafone y DotMobi, formalised an agreement to combat images of sexual abuse of children on internet. It was launched with the approval and support of Viviane Reding (Information Commissioner at the European Commission).

This alliance aims to pursue the following targets:

a) The creation of sufficient barriers which will prevent the use of networks and mobile services to store, access or make us of sexual child abuse content.

(b) To contribute to halting the growth of sexual child abuse content, creating a safe environment for our clients.

The purpose of this alliance involves Telefónica on four main points: Agreements with other IPS for the removal of content when they are not hosted in their servers. Obtaining and conserving the Chain of Custody of the material withdrawn. Agreements with the Armed and Safety Forces of the State, for their investigation and prosecution. Training and divulgation to users concerning risks on internet.



The specific requirements established for all operators in order to be part of the Alliance were as follows:

1. Development of technical mechanisms required to block URLs with content involving images of sexual abuse of children.

2. Implementation of a Notice and Takedown system.

3. Collaboration and development of a national hotline or other mechanisms for making complaints

Three types of content are differentiated:

- Child pornography

- Graphic content of child pornography on personal or rented web pages

- Terrorist content
  - Explicit content defending terrorist activity

- Xenophobia/ racist content

For child pornography

The content may be deleted by the internet provider and all the related data (communications, images, etc.) should be stored in order to facilitate investigations. Information should be delivered immediately to judges and the forces of law and order for investigation and prosecution.

Terrorism, xenophobia and racism:

The content should be evaluated by a judge in order to decide on its elimination. The ISP is not authorised to decide on withdrawal of contents.

In order to withdraw child pornography content the main sources of reference, without prejudice to lists which may be provided by the judicial authorities of each country are the "Internet Watch Foundation" , a non-profit making organisation founded in 1996 by the European Union and by the internet industry which collaborate on an international level with "INHOPE" and other relevant authorities and bodies committed to combating sexual abuse content on line , all of whom seek a global response to this kind of cross border crime.

Given that the majority of the illegal content of this type is hosted outside the United Kingdom, the association provides dynamic lists of URLs with images containing sexual abuse of children so that they can be blocked.

4. Technical possibilities of removal and blocking

In general, there are two types of ISP on internet:

- Access providers. These only transport data from the computer to the website provider. They are transparent regarding the data which will pass through them.

- Hosting providers. They store web pages and serve these when requested by a browser.

- A combination of both types: They provide access and content

In some cases it is difficult to remove the illegal content as either the hosting supplier country does not consider the content to be illegal or because there may be a lack of regulation in the content.

In addition in some countries judges and/or the security forces of a country are very slow or simply do not work due to the fact that no operating procedures exist.

Finally, there are "Hosting Paradise" countries located in Africa and Asia.

For these cases, the following actions can be addressed in order to block contents:

- Agreements with remote access providers of web hosting.
- Agreements with international carriers.