What is Filtering & Blocking?

And how it is used for child sexual abuse material

How does it work?

Many Internet Service Providers (ISPs) and other online service providers are keen to prevent their users from accessing web addresses that are known to contain child sexual abuse images. Alternatively they might want to prevent their users from uploading, exchanging or storing child sexual abuse images or videos. To do this they use filtering and blocking technologies.

Web addresses that are known to contain child sexual abuse material are placed on a list that is circulated directly to companies which might incorporate this list into a security policy for their service. Any attempt to reach an address on that list will be filtered out or blocked. The lists are compiled and provided by bodies such as hotlines and police agencies (such as INTERPOL). In a number of countries it is a legal requirement for ISPs to block child abuse material.

Where an individual image is already known to the police, hashing technologies such as PhotoDNA, can be used to create a hash* or digital fingerprint of an image. These hashes are then placed in a database and systems can subsequently identify any copies of that image that a user might attempt to upload, download, exchange or store on their service.
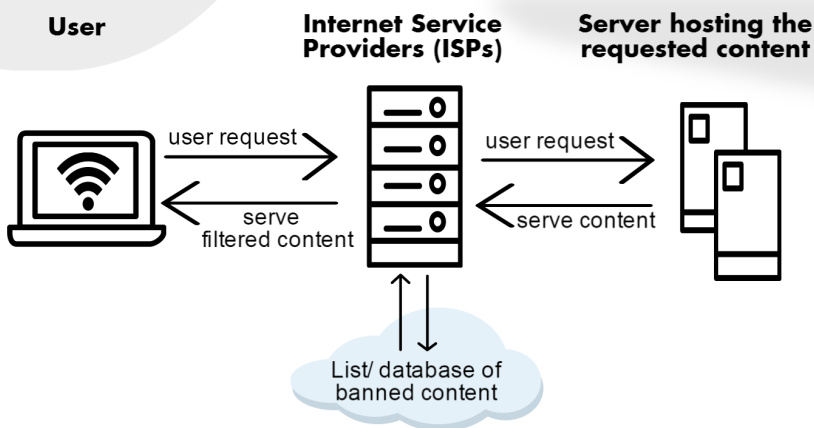
FACTS

The goal of filtering and blocking is to limit the availability of particular content online

Filtering and blocking only impacts the material on the part of the Internet indexed by search engines

Filtering and blocking can be based on: key words (e.g. search terms); banned URLs (e.g. websites); and hashes.

User

Internet Service Providers (ISPs)

Server hosting the requested content

user request

user request

serve filtered content

serve content

List/ database of banned content

Caution

Filters cannot always distinguish between a match that refers to illegal content and those that do not. This creates the risk of content being wrongfully blocked (over-blocking)

* See factsheet - What are hashes? What is PhotoDNA?

Filtering & blocking Child Sexual Abuse Material

The net effect and intention behind filtering and blocking technologies is to reduce or limit the availability of child sexual abuse material online. It contributes to a safer Internet by preventing unwanted exposure to this type of illegal content. Moreover it obstructs offenders attempting to access and share child sexual abuse materials.

Filtering and blocking also has an important benefit to the victims depicted in the images. By making the images inaccessible, filtering and blocking mechanisms protect victims' privacy and human dignity and reduce the possibility of further harm being inflicted on the child.

ecpat