- ECPAT Internet & Technology Factsheet -

What is TOR?

The Onion Router

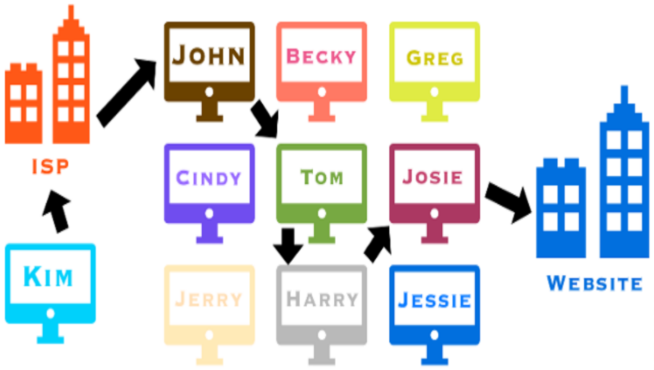
FACTS

- TOR is short for The Onion Router
- TOR software was developed by the US Naval Research Laboratory to protect US intelligence communication
- TOR aims to conceal user identities and their online activity from surveillance and traffic analysis
- TOR has legitimate uses for users who want to maintain privacy; circumvent censorship; or protect themselves from repressive regimes or targeted monitoring

How does it work?

TOR diverts online traffic through a network in a way that conceals a user's location or identity. Instead of transporting traffic such as visits to websites or instant messages, through a fixed predictable route [from user 'Kim' to the Website], TOR goes through a dynamically assigned route that becomes untraceable.

The TOR connection is encrypted. An unencrypted link is exposed to surveillance, allowing someone to learn what websites you visit by tracing back your IP-address*. However, TOR uses an encrypted connection which means that at any point on the route from the origin Internet user to the destined location, it is not clear where the data is coming from or where it is going.



When Kim visits a website via the TOR network her traffic takes a random path through other people's computers to get to the website. At each intermediate point the source and destination information is stripped to make identification of the user extremely difficult. As a result, Internet Service Providers cannot track who she is and what sites she is visiting. Or TOR misleadingly presents the last exit node [Josie] as the communication source.

** an IP-address reflects the identity of the user of a device [see factsheet: What is an IP-address?]*

TOR applied to Sexual Exploitation of Children Online

Child sex offenders use TOR to share child sexual abuse images or other content that facilitates and perpetuates a culture of child sexual abuse. Moreover, TOR allows them to connect with potential victims anonymously. Also TOR's hidden services allow for perpetrators to communicate secretly amongst each other. By using TOR, offenders avoid revealing their location or identity, thereby avoiding detection by Internet Service Providers (ISPs) and law enforcement. This way TOR complicates victim and offender identification.

TOR is the most popular software program used to access the parts of the Internet which are deliberately constructed not to be widely available nor easy to use. This is also referred to as the DeepWeb or Darknet (the latter indicating the [illegal] nature of conduct executed there). This more 'hidden' or anonymous network of computers can only be accessed by using a special piece of software, such as TOR.

This factsheet was produced by ECPAT International - Programme Combating Sexual Exploitation of Children Online