Fighting to free the world of CSAM.

Learn more and get involved:
Inhope.org

Notice & Takedown

INHOPE

What is a Notice and Takedown order?

A Notice and Takedown order is a procedure for asking an Internet and Electronic Service Provider (ISP/ESP) or search engine to immediately remove or disable access to illegal, irrelevant or outdated information hosted on their services.

INHOPE hotlines send Notice and Takedown orders to ISPs/ESPs when a member of the public sends them a URL containing illegal images and videos depicting child sexual abuse and exploitation, often referred to as child sexual abuse material—CSAM.

Notice and Takedown time is the time from when an INHOPE hotline receives a CSAM report from the public, to the time a hotline reports it to the national Law Enforcement Agency (LEA), the Internet Service Provider (ISP) and ultimately the time the content is removed from the internet.

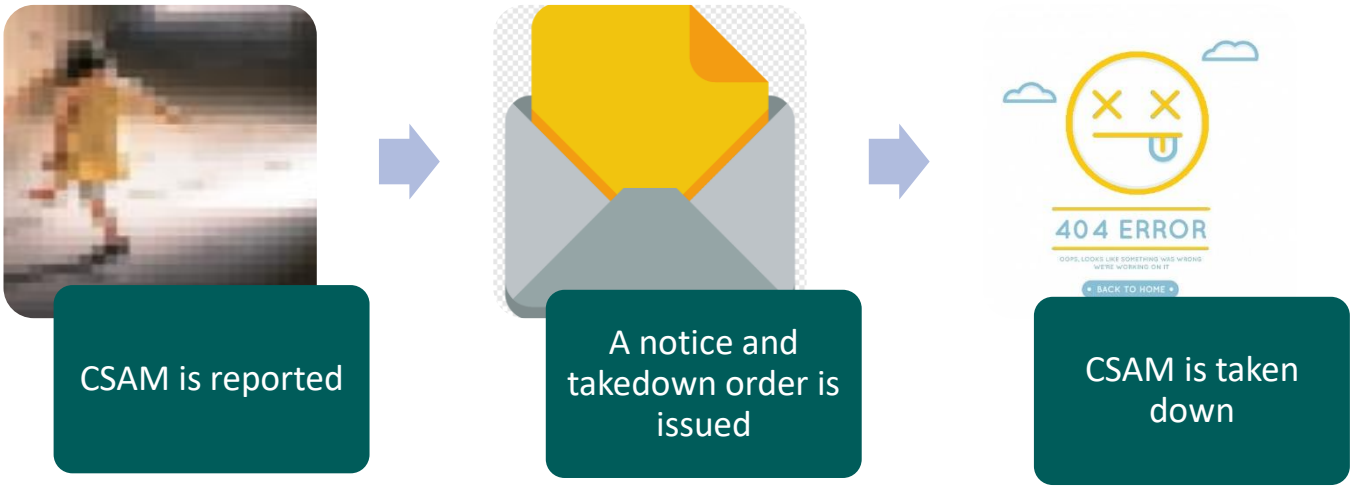
This publication looks at Notice and Takedown procedures in the countries where INHOPE member hotlines operate, and explains the complexities of calculating the Notice & Takedown times.

How is CSAM removed from the internet?

We take a look at public perception versus reality.

Child Sexual Abuse Material (CSAM) is found online by the public, industry, etc. These reports are reviewed by analysts who classify the illegality of the material, which is then shared with the national Law Enforcement Agency, and in many cases the relevant Internet Service Provider will receive a Notice and Takedown order. This Is done in partnership with the local Law Enforcement Agency to make sure their Investigations aren't compromised.

The public perception of the process:



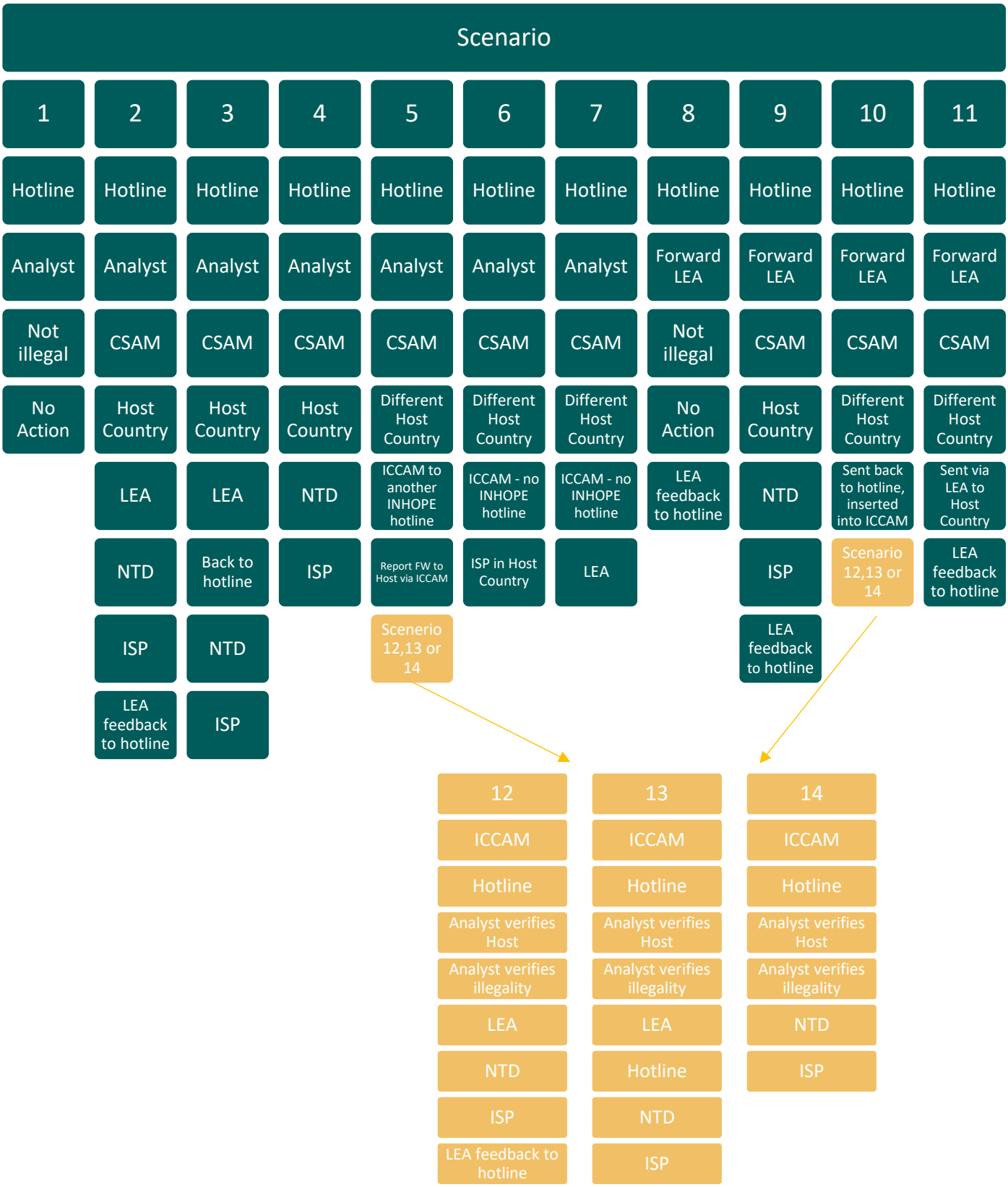
Unfortunately, the reality of the situation is not that simple. Different countries follow different procedures, which involve different stakeholders, who process the report in different orders, using different approaches, whilst applying different laws.

In order to visualise the complex framework of Notice and Takedown procedures, we have looked at all the countries that INHOPE's member hotlines represent and their respective scenarios on the following page.

Notice and Takedown Scenarios:

Scenarios 1 through 11 start with a report from the public which is received by the hotline in that country.

Note: Analyst refers to the hotline's own analyst. Host country refers to the current hosting country, as this is subject to change.



Descriptions of scenario elements:

Scenario 1

- **Hotline** = Hotline receives a report from the public containing one or more URLs potentially containing CSAM
- **Analyst** = Authorised and trained hotline analyst assesses the images and videos found on the reported URL/URLs and classifies illegality according to international and national laws
- **Not illegal** = The hotline analyst classifies the images and videos on the reported URL/URLs as not illegal according to international and national law
- **No Action** = The hotline analyst takes no further action on the report. Report Is kept for administrative purposes.

Scenario 2

- **CSAM** = The hotline analyst classifies the images and videos on the reported URL/URLs as child sexual abuse material according to international and national law
- **Host Country** = The reported URL containing CSAM and the URLs of the illegal images and videos are hosted In the country where they were reported
- **LEA** = The hotline analyst sends the reported URL containing CSAM to the national Law Enforcement Agency
- **NTD** = Notice and Takedown order Is issued by hotline analyst or LEA (see box before NTD box)
- **ISP** = The hotline analyst sends a Notice and Takedown order to the Internet Service Provider
- **LEA feedback to hotline** = LEA provides feedback to the hotline about the outcome of the NTD order or status of the report

Scenario 3

- **Back to hotline** - LEA confirms illegality of the reported images and videos and sends the report back to the hotline analyst so that the analyst can issue an NTD to the ISP

Scenario 5

- **Different Host Country** = The reported URL containing CSAM and the illegal images and videos are hosted In a different country than the one where they were reported
- **ICCAM to another INHOPE hotline** = The hotline analysts inserts the reported URL containing CSAM into ICCAM and the system automatically sends a notification to the hotline where the videos and images are hosted
- **Report FW to Host via ICCAM** =

Scenario 6

- **ICCAM- no INHOPE hotline** = The hotline analysts inserts the reported URL containing CSAM Into ICCAM. There Is no INHOPE hotline where the images and videos are hosted

- **ISP In Host Country** = The hotline analyst sends an NTD to the ISP in the hosting country

Scenario 8

- **Forward LEA** = The report is sent/forwarded to the national Law Enforcement Agency without being assessed and classified by the hotline analyst

Scenario 10

- **Sent back to hotline, inserted into ICCAM** = LEA confirms that images and videos are CSAM and hosted In a different country. LEA sends the report back to the hotline so that the hotline analyst can Insert the URL in ICCAM
- **Sent via LEA to Host Country** = LEA sends the report to the LEA In the hosting country via law enforcement channels such as INTERPOL or EUROPOL

Scenario 12

- **ICCAM** = The hotline analyst receives URL containing CSAM hosted in their country through INHOPE's secure platform ICCAM
- **Analyst verifies Host Country** = The hotline analyst verifies that the images and videos are hosted in the country and checks whether the hosting has moved to another location
- **Analyst verifies illegality** = The hotline analyst verifies that the images and videos are illegal according to international and national law

Which scenario do INHOPE's member hotlines use?

An overview of INHOPE's member hotlines and the scenario they follow in their respective country.

Scenario	Applicable Countries within the INHOPE Network			
1	All			
2	Belgium	Estonia	Lithuania	Portugal
	Bulgaria	Finland	Luxembourg	Romania
	Croatia	Germany (x3)	Malta	South Africa
	Cyprus	Hungary (NMHH)	New Zealand	Taiwan
	Denmark	Latvia		
3	Australia	Czech Republic	Russia	Sweden
	Austria	Japan	Slovenia	United Kingdom
	Colombia	Netherlands		
4	Canada	Ireland	Poland	South Korea
	France	Latvia	Portugal	Turkey
	Germany (x3)	Lithuania	Romania	United States
	Greece			
5	Australia	Finland	Luxembourg	Slovenia
	Austria	France	Malta	South Africa
	Belgium	Germany (x3)	Netherlands	South Korea
	Bulgaria	Greece	New Zealand	Sweden
	Canada	Hungary (NMHH)	Poland	Taiwan
	Colombia	Ireland	Portugal	Turkey
	Croatia	Japan	Romania	United Kingdom
	Denmark	Latvia	Russia	United States
	Estonia	Lithuania		
6	Canada	Hungary (NMHH)	Lithuania	South Korea
	France	Japan	Poland	Turkey
	Germany (x3)			
7	Australia	Estonia	Japan	Romania
	Austria	Finland	Latvia	Russia
	Belgium	France	Malta	Slovenia
	Bulgaria	Germany (x3)	Netherlands	Sweden
	Colombia	Greece	New Zealand	Taiwan
	Croatia	Ireland	Portugal	United Kingdom
	Denmark			
8	N/A			
9	Bosnia			
10	Cyprus			
11	Bosnia	Cyprus		
12	Belgium	Estonia	Lithuania	Portugal
	Bulgaria	Finland	Luxembourg	Romania
	Croatia	Germany (x3)	Malta	South Africa
	Cyprus	Hungary (NMHH)	New Zealand	Taiwan
	Denmark	Latvia		
13	Australia	Czech Republic	Netherlands	Sweden
	Austria	Japan	Russia	United Kingdom
	Colombia			
14	Canada	Ireland	Portugal	South Korea
	France	Latvia	Romania	Turkey
	Germany (x3)	Lithuania	Slovenia	United States
	Greece	Poland		

Exceptions to NTD Scenarios

- Important to note is that the NTD scenarios presented apply specifically to CSAM reports received from the public. A few hotlines use different methods of identifying CSAM, such as proactive search, crawling or receiving reports from the internet industry.
- In South Korea and Cyprus, when a received CSAM report is hosted in a different country, the national hotline notifies all national ISPs in order to block access to the material nationally, and it also uploads the report to ICCAM.
- In Lithuania and Australia, an application request is submitted to the national classification board to have the content formally classified as illegal.
- In Austria and Belgium, when a CSAM report is hosted in a different country, despite inserting the report into ICCAM, the hotline also sends the report to the national LEA. (Scenario 5)
- When CSAM is found to be hosted in Canada, the hotline notifies the ISP which then must notify the national LEA.
- In Austria, Belgium, Estonia, France, Greece, Ireland, Malta, Portugal, Russia, Slovenia and Spain, when a report is received of CSAM hosted in another country within the INHOPE network, the hotline enters the URL into ICCAM but also sends the report to the national LEA.
- In Finland, if the material is assessed as not illegal but violates the rights of the child in a so called “grey area,” the hotline will send a Notice and Takedown to the ISP hosting the material.
- In Finland, when a CSAM report is received which is hosted in a different country where there is no INHOPE hotline, the report is inserted into ICCAM and the national LEA is notified. The national LEA consequently informs the ISP in the hosting country to block the content.
- In France, the hotline follows scenario 7 only if the hosting country applies GDPR or is recognised by the European Commission as providing adequate protection of personal data. The hotline then notifies the hosting provider in this country for removal.
- For the German hotlines eco and FSM, if a report of CSAM hosted in another country that is part of the INHOPE network has been forwarded to the partner hotline, but the material hasn’t been removed after 48 working hours, the hotlines will notify the hosting ISP. This is also a practice used by other hotlines.
- The hotline in Iceland receives very few reports and all reports hosted within the country and internationally are processed by the national LEA. The hotline just forwards the reports to the national LEA.

Complexities of Notice and Takedowns

When we discuss Notice and Takedown, we make the process sound simple and cohesive—a hotline sends out a notice and the respective ISP takes the content down. However, things are just not that simple.

We first must consider the variety of stakeholders that could be involved in an NTD: the hotline, the analyst, national law enforcement, the ISP, (CDN and others), an ethics board, and in certain cases, larger approval associations. The number of stakeholders will inevitably impact how quickly CSAM is removed.

Secondly, we need to accept that the order of an NTD process varies per country and that effects how information is being shared, as can be seen in the scenarios. This not only influences once again the time it takes for the hosting country to remove the material, but also for the material to reach the responsible LEA and for the LEA to open and investigate to identity and rescue the victim. The national LEA may even request that a hotline does not issue an NTD because of an ongoing investigation. Here are specific examples from Bulgaria, Lithuania and Italy:

- In Bulgaria, a hotline will receive a report and assess the legality. If a report is classified as illegal, the hotline will send this report to the national LEA. The national LEA is then responsible for sending an NTD request to the ISP as well as confirming that the material has indeed been removed. The LEA will not inform the hotline if the NTD request has been issued or if the NTD has been successful. This is common practice in most countries and impacts a hotline's ability to verify NTD times.

- In Lithuania, one of the stakeholders involved in an NTD is an ethics board. Before a hotline can confirm and classify content as illegal, they must first send it to a designated ethics board for review. An NTD will only be issued to the ISP with the approval of the board.

- In Italy, a hotline is not allowed to assess or classify a report, acting only as a recipient and passing it to national LEA, which results in the hotline not knowing how many of the reports were classified as illegal or not.

These three examples provide a glimpse into the world of NTDs and the obstacles faced by hotlines.

Thirdly, in addition to the variation in national processes is the variation in how hotlines use ICCAM: INHOPE's secure software solution to collect, exchange and categorise reports of child sexual abuse material. Used by all INHOPE hotlines, ICCAM is a key part of the NTD process. Once a report is received by a hotline it is entered into ICCAM using basic or full access of the software (for example, Italy uses the basic version as they do not need to access content). If a report is entered into ICCAM using basic access, it will influence the quantity of data the system can track, as details like report follow-ups will not be recorded. The national context of the hotline influences how ICCAM is used, so while ICCAM is the common tool, it does not cover the exceptions within a hotline and the different NTD processes that are taken. Certain hotlines also use an internal software—in fact, nine hotlines within the INHOPE association use an API (automating the connection between the hotlines system and ICCAM) which consequently impacts the information share among stakeholders; any data gathered by a hotline using an API does not reach INTERPOL.

This means there are significant differences in how ICCAM is used and the data that is collected.

And, finally we must consider the responsiveness of the respective ISP. If a hotline receives a large number of reports and has little to no collaboration from the ISP, then their workload is immediately increased by having to follow-up and confirm that content has been removed. This impacts the removal of material in the country in question and the NTD time. Automating systems could support the hotline in these cases by reducing the workload. However, the different structures and NTD processes often challenges automation. INHOPE works closely with hotlines and national governments, LEAs and ISPs to standardise and unify processes, but the reality remains complex.

For more Information visit: www.inhope.org

Or contact: secretariat@inhope.org

Published: 2020