NOTICE AND TAKEDOWN

Company policies and practices to remove online child sexual abuse material

GSMA™

unicef

About the GSMA:
GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organizations in adjacent industry sectors. It also produces industry-leading events, such as the Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at <www.gsma.com>.
Follow the GSMA on Twitter: @GSMA

About the GSMA Mobile Alliance Against Child Sexual Abuse Content:
The GSMA Mobile Alliance Against Child Sexual Abuse Content was founded by an international group of mobile operators within the GSMA to work collectively on obstructing the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content.

The GSMA Mobile Alliance's aim is to help stem, and ultimately reverse, the growth of online child sexual abuse content around the world. Through a combination of technical measures, co-operation and information sharing, the GSMA Mobile Alliance seeks to create significant barriers to the misuse of mobile networks and services for hosting, accessing, or profiting from child sexual abuse content.

For more information, please visit: <www.gsma.com/mobilealliance>

Writing and editing:
Author: Pat Walshe
UNICEF: Eija Hietavuo, Amaya Gorostiaga
GSMA: Natasha Jackson, Jenny Jones
Editor: Catherine Rutgers

May 2016

FOREWORD

The Convention on the Rights of the Child sets out the specific rights that all children, everywhere, are entitled to in order to survive and thrive, to learn and grow, and to reach their full potential.

Among these basic rights are children's right to protection from sexual exploitation and violence and the right to privacy. Children who have experienced sexual abuse, and had evidence of that abuse recorded and shared online, have been denied both of these rights. Many of them speak of the traumatic effects of knowing that evidence of their abuse continues to circulate online long after the direct, physical abuse took place.

By implementing the procedures known as 'notice and takedown' to rapidly remove this material from view as soon as it is discovered, the re-victimization of those children is minimized, as are the opportunities for others to access the material online, whether deliberately or inadvertently.

In countries where the Internet service provider (ISP) industry is able to work with law enforcement or a national hotline that specializes in handling discoveries of child sexual abuse material, notice and takedown is a first defence in keeping digital services free from child sexual abuse material.

We look forward to a world where these processes are universally in place – and all discoveries of child sexual abuse material are processed efficiently so that content is removed from view, and potential evidence is managed correctly and securely to maximize the chances of rescuing children from abusive situations.

This publication is offered in the spirit of collaboration to members of the international ISP community seeking to prevent the misuse of their services for sharing child sexual abuse material. We encourage the industry to implement such processes at the earliest opportunity.

We also urge collective action from all stakeholders. We call on governments to create an enabling environment for industry by ensuring that appropriate legislation is in place, that dedicated Internet hotline reporting facilities are established, and that law enforcement is trained and empowered to act, both nationally and internationally.

Only by working together can we truly support the survivors of child sexual abuse and create an Internet environment that is free from child sexual abuse material.

Natasha Jackson,
Head of Public Policy and Consumer Affairs, GSMA

Eija Hietavuo,
Corporate Social Responsibility Manager, UNICEF

CONTENT

GLOSSARY

Child sexual abuse material (CSAM), also known as 'child sexual abuse content', refers to any material that visually depicts a child in real or simulated explicit sexual activities, or any representation of the sexual parts of a child for primarily sexual purposes, by any means, including photography, video, drawings, cartoons and live streaming. Although the term 'child pornography' is used commonly in legislation and international conventions, it is often understood to be associated with depictions of sexual activity between consenting adults; therefore, use of the term 'child pornography' can mischaracterize sexual representation in which children are involved. To avoid misunderstanding, this document refers to 'child sexual abuse material', reflecting the wide spectrum of child sexual abuse materials and emphasizing the abusive and exploitative aspects of this phenomenon.

A key issue to address is that current legal frameworks that outlaw the sexual exploitation of children often refer to 'child pornography', but as highlighted by INTERPOL, 'pornography' is often perceived as consensual acts between adults and not the sexual abuse of a child.[1] Therefore, a key challenge remains to enshrine into national laws and international conventions a definition of child sexual abuse material that carries legal certainty and effective penalties to prevent its creation and circulation, and that supports self-regulatory notice and takedown frameworks.

It is important for all those engaged in combating child sexual child abuse material to use precise and consistent definitions in their policies and procedures, as recognized and advanced by the Interagency Working Group that has adopted global terminology guidelines on sexual exploitation and sexual abuse of children.[2]

Hotlines may be operated by a government agency or a recognised self-regulatory organization that receives and evaluates reports of child sexual exploitation and child sexual abuse material hosted online. A hotline will report child sexual abuse material to the relevant online service company and/or law enforcement requesting its removal from access and circulation by the public.

Notice and Takedown, known as NTD, refers to a company's procedures for receiving reports that may come from customers, employees, law enforcement or hotlines that child sexual abuse material has been discovered on the company's networks or services, and for preventing further access and distribution.

1 INTERPOL, 'Appropriate Terminology', 2016, <www.INTERPOL.int/Crime-areas/Crimes-against-children/Appropriate-terminology>.
2 ECPAT, 'Interagency Working Group Adopts Global Terminology Guidelines for the sexual exploitation and sexual abuse of children', 2 February 2016, <www.ecpat.net/news/interagency-working-group-adopts-global-terminology-guidelines-sexual-exploitation-and-sexual>.

INTRODUCTION

The Internet provides unprecedented opportunities for adults, youth and children to share ideas and express opinions, and to access information, learn and communicate. However, the online environment also creates avenues for the sexual abuse and exploitation of children, and the circulation and consumption of child sexual abuse material (CSAM).

This document provides insights to help companies establish policies and practices to support the prompt and effective removal of child sexual abuse material. In particular, it provides high-level guidance on:

- Establishing a dedicated function to investigate and take appropriate action against CSAM.
- Putting in place policies and operational procedures for acting on notices to take down CSAM after it is reported and investigated, including removal from access and circulation.
- Establishing policies and practices for staff training and welfare.
- Developing relationships and working with key stakeholders such as law enforcement and national hotlines.

References and links to a range of materials that may assist companies to understand better the role and value of notice and takedown in combating child sexual abuse material online are also offered, in addition to other valuable tools and approaches.

Robust and effective practices for removing the availability of CSAM help prevent the re-victimization of children, make companies less attractive to those involved in its creation, publication and distribution, and help identify and prosecute offenders. By working together, the industry, hotlines and law enforcement can significantly reduce the amount of this abusive content online and the time it takes to remove such material.

The Internet Watch Foundation (IWF)[3] reports that, as of 2015, less than 0.2 per cent of worldwide CSAM was hosted in the United Kingdom, down from 18 per cent in 1996, and 38 per cent of web pages containing CSAM are removed in response to takedown notices within 60 minutes or less, and 59 per cent were removed within 120 minutes or less.[4] INHOPE, the International Association of Internet Hotlines, reports that, in 2014, 93 per cent of CSAM in Europe and 91 per cent worldwide was removed from public access on the Internet in less than 72 hours.[5] A task for industry is to reduce removal times even further to eliminate 'space' for CSAM online, and to speed up the process of identifying and recovering children from abuse.

3 Established in 1996 by the Internet industry, IWF operates the 'UK Hotline', <www.iwf.org.uk/hotline>, as a way for the public and technology professionals to report criminal online content securely and confidentially.

4 Internet Watch Foundation, 'New Tactics Mean 137% Increase in Identified Child Sexual Abuse Imagery'. IWF, Cambridge, United Kingdom, 13 April 2015, <www.iwf.org.uk/about-iwf/news/post/407-new-tactics-mean-137-increase-in-identified-child-sexual-abuse-imagery>; and IWF, Annual Report 2015, p. 11, <https://www.iwf.org.uk/assets/media/annual-reports/IWF%202015%20Annual%20Report%20Final%20for%20web.pdf>.

5 INHOPE, '2014 Facts, Figures & Trends: The fight against online child sexual abuse in perspective', 2015, <www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx> .

1. WHAT IS NOTICE AND TAKEDOWN?

'Notice and takedown' is considered to be a vital tool in removing CSAM at its source, keeping the Internet free of this content, and disrupting the cycle of sexual exploitation and abuse of children and their re-victimization.[6] It refers to a company's procedures for handling reports that may come from customers, employees, law enforcement or hotlines that child sexual abuse material has been discovered on the company's networks or services.

A notice received from law enforcement or a hotline that asks a company to "take down" CSAM may be incorrectly perceived – it is important to understand that a takedown notice does not automatically mean a request to delete the material. 'Takedown' means acting promptly to identify whether the reported material is illegal, and if so, to remove and isolate the content from being viewed or circulated by the public. Deleting CSAM may compromise an ongoing criminal investigation that is unknown to the company, and also prevent the identification of children who are being abused.

If CSAM is confirmed, it should be securely isolated within the company's networks and services and accessible only to those employees authorized to investigate and take action on CSAM reports. Companies should check the law applicable in their jurisdictions on handling child sexual abuse material.

2. KEY STEPS FOR ESTABLISHING NOTICE AND TAKEDOWN CAPABILITIES

As reflected in the *Guidelines for Industry on Child Online Protection* developed by the International Telecommunication Union (ITU) and UNICEF,[7] an increasing number of responsible companies are taking fundamental steps to help prevent their networks and services from being misused to disseminate child sexual abuse material or to facilitate the sexual exploitation of children. This section highlights key steps you can take to establish effective and practical notice and takedown capabilities.

In the first instance, there are five fundamental steps a company can take to help ensure there is 'no space' for CSAM in the services it offers:

- First, **seek board-level commitment**, support and sign off to outlaw and combat CSAM. This will send a clear message to employees and any person using the company's networks and services that child sexual abuse material will not be tolerated and that the company will cooperate fully with law enforcement and other stakeholders to combat CSAM.[8]
- Second, **develop a clear policy** that sets out the company's commitment and position on CSAM. This is important for setting a company's internal direction.
- Third, **assign responsibility for putting that policy into practice, and develop clear documented procedures** and capabilities for removing CSAM from public access and further circulation. Ensure these procedures are accessible within the company and also apply to third parties used by the company and who have a role in notice and takedown.
- Fourth, **establish a dedicated function** staffed by trained employees. This minimizes the impact on other employees from exposure to CSAM and helps avoid a company's liability from possible prosecution where possessing or viewing CSAM is illegal even for employees (*see Section 4.2*).
- Fifth, **seek to establish a memorandum of understanding** between the company, national law enforcement and your national hotline that gives protection to employees acting in a professional capacity to investigate, report and remove CSAM.9 This will help address employees' concerns and anxieties over possible prosecution for simply doing their jobs.

6 See, for example: Internet Watch Foundation, Annual Report 2015, <https://www.iwf.org.uk/assets/media/annual-reports/IWF%202015%20Annual%20Report%20Final%20for%20web.pdf>.

7 International Telecommunication Union and United Nations Children's Fund, Guidelines for Industry on Child Online Protection, ITU and UNICEF, 2014, <www.unicef.org/csr/COPguidelines.htm>. Also see: UK Council for Child Internet Safety, Child Safety Online: A practical guide for providers of social media and interactive services, UKCCIS, 29 February 2016, <www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-parents-and-carers>.

8 For example, see: Twitter Inc., 'Help Center: Child sexual exploitation policy', 2016, <https://support.twitter.com/articles/37370>.

9 As noted in the example of the United Kingdom, "Individuals or organisations who accidentally discover criminal activity or to whom such activity is reported require protection from the risk of prosecution where, in order to report it, they make a copy." – Crown Prosecution Service and Association of Chief Police Officers, *Memorandum of Understanding between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003*, CPS and ACPO, United Kingdom, 4 October 2004, p. 3, <www.cps.gov.uk/publications/docs/mousexoffences.pdf>.

3. POLICY AND PROCEDURES

3.1. Develop policy

It is important to develop a policy and clear documented procedures and processes for handling notice and takedown requests, and ensuring the prompt isolation and removal of CSAM from public access and further circulation. The policy and procedures should reflect national law, as in some countries it may be illegal to remove CSAM without first receiving authorization from law enforcement.

The policy and procedures should be clear and easy to understand, set out staff responsibilities and provide clear guidance on how to process CSAM reports, and include key Do's and Don'ts. For example, staff should be advised not to circulate or share CSAM and to process such material strictly in accordance with the policy and procedures.
The procedures should reflect not only the requirements of the dedicated CSAM investigation function, but they should also provide clear guidance to customer services and frontline staff to ensure reports are handled in a compliant and effective manner.

A good policy and effective procedures are vital to ensuring the integrity of the process, and provide the foundations for ensuring the swift removal of CSAM from circulation and to supporting the flow and collation of intelligence to help identify and rescue children who appear in CSAM and to prosecuting offenders.

3.2. Implement procedures for notice and takedown

It is important that CSAM is handled in accordance with the law for a number of key reasons. These include protecting companies and employees from liability, ensuring the swift removal of materials and the recovery and safekeeping of children, and to maintaining the evidential integrity of the process and data in support of the prosecution of the offenders.

There is no uniform law on notice and takedown of child sexual abuse material or content – each country may have its own laws defining CSAM and outlining obligations for notice and takedown. Therefore, it is necessary to establish and follow a policy and process based on national legislation.

In 2000, the European Parliament and the Council of the European Union issued a directive on 'electronic commerce', under which Internet service providers become liable once they have knowledge of illegal activity on their networks.[10] The directive does not prescribe specific notice and takedown procedures; rather, it has led to successful voluntary self-regulatory schemes for notice and takedown in countries including Germany and the United Kingdom.[11]

In the United States, companies are required to report CSAM to the National Center for Missing and Exploited Children (NCMEC), which has operated the CyberTipline reporting function since 1998. The hotline accepts and actions reports of suspected child exploitation, including CSAM, and works with industry to establish good practice and ensure effective processes.[12]

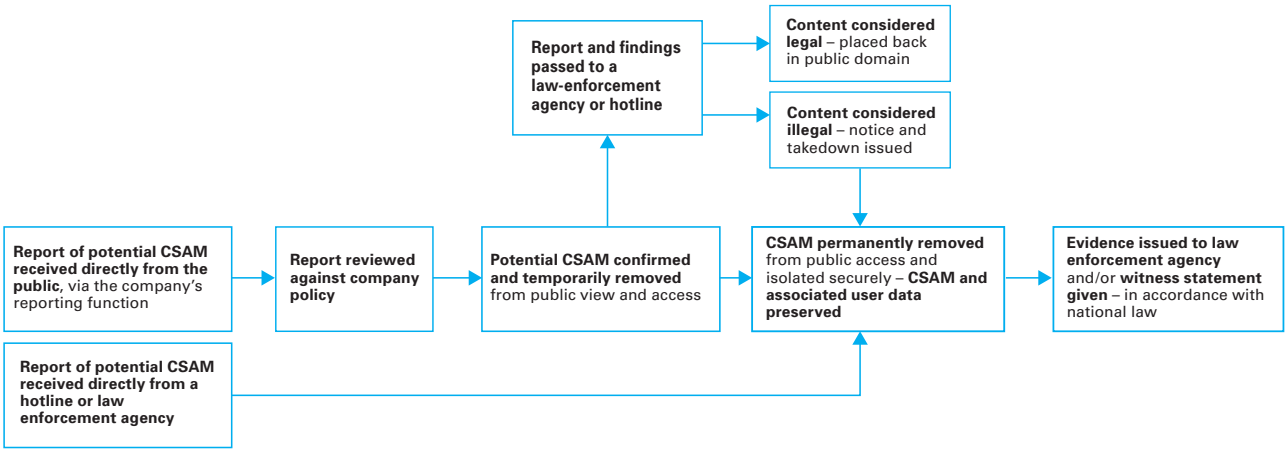
A notice and takedown process may take three key forms:

- A report may be received directly from a member of the public about potential CSAM hosted on the company's network or services; in this case:
  - Local law may permit the company to isolate and/or remove from public access the reported material.
  - A company may then immediately refer the potential CSAM to law enforcement or a national hotline, pending formal instruction for the permanent removal from circulation or deletion from the company's networks.
- A notice may be received directly from a national hotline requiring the takedown of reported CSAM, or removal of a URL that provides access to the CSAM.
- A notice may be received directly from law enforcement demanding and authorizing the takedown of CSAM.

10 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>.
11 Wei, Weixiao, Online Child Sexual Abuse Content: The development of a comprehensive, transferable international Internet notice and takedown system, Nominet Trust and Internet Watch Foundation, 2010, <www.iwf.org.uk/resources/independent-report>.
12 National Center for Missing and Exploited Children, 'CyberTipline', 2016, <www.missingkids.org/cybertipline/>.

The figure below illustrates an example of the process flow.

Example of a process for removing CSAM after reports from customers, or from hotlines and law enforcement agencies



3.3. Provide a standardized function for reporting CSAM

Many companies provide a simple and easy-to-use mechanism, often via their websites, for reporting CSAM directly to the company or to law enforcement or hotlines.[13] Ensure customer services are aware of the process and how to advise people to follow it.

It's a good idea to publish information alongside the reporting function that explains in clear, simple terms the company's position on CSAM and how the reporting process works, including liaison with law enforcement and hotlines. It is important that people have confidence and trust in the process and that it is easy to find and quick and simple to use.

If possible, enable anonymous reporting to encourage people to come forward to report CSAM without fear of secondary legal repercussions. Anonymity helps capture "child sexual abuse material which may otherwise have gone unreported."[14] If you choose to allow anonymous reporting, make it clear that the company will not be able to acknowledge or follow up the report directly.

If the reporting tool refers reports internally, these should go directly to a dedicated CSAM function within the company and not to customer services or other general business areas (see Section 3.5, on employee considerations). The function may reside with the team that handles police enquiries, or with other security functions.

The reporting tool should ask users for information to help identify and confirm the existence of CSAM. This information may include the nature of the materials, the URL of the website hosting the material, whether they became aware of it via email, messaging or social media, the use of live video, and the date and time of discovery or receipt of CSAM. Examples[15] of various approaches to reporting online content can be found in the Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU[16] and Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services.[17]

It is recommended that you liaise with your national law enforcement agency and hotline to develop a consistent approach and to support any subsequent investigation and prosecution. It is also good practice to 'white list' the email address of hotlines and law enforcement agencies from whom you may receive a CSAM notice and takedown request. It is also best practice to establish nominated points of contact between the company and applicable hotlines and law enforcement – the company point of contact should be accessible out of hours.

13 INHOPE members' hotlines, for example, are found at <www.inhope.org/gns/our-members.aspx>.
14 Smith, Sarah, Global Strategies for Tackling Child Sexual Abuse Material Online (2014) report produced for the Winston Churchill Memorial Trust, 2014, n.p., <www.wcmt.org.uk/sites/default/files/report-documents/Smith%20Sarah%20Report%202014%20Final%202.pdf>.
15 Mobile Operator's Contribution to Notice and Take Down, the Mobile Alliance Against Child Sexual Abuse Content (May 2012) <www.gsma.com/mobilealliance>.
16 ICT Coalition. <http://www.ictcoalition.eu/commitments>.
17 UK Council for Child Internet Safety, 2016, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final__3_.pdf>.

3.4. Preservation of CSAM and associated customer data

Where a report of CSAM is confirmed and the material removed from public access and circulation, the law or industry practice may require the preservation of CSAM in a secure environment, accessible only to authorised employees. This may include the preservation of the report itself, and associated customer data relating to the CSAM. The data may be required to support any investigation or prosecution pursued by law enforcement.

The period for which CSAM and associated data is retained should be determined with law enforcement only in accordance with applicable national law.[18]

3.5. Employee considerations: legal liability, training and support

There are crucial considerations and steps that companies can take to ensure the effective takedown of CSAM and to protect the welfare of staff.

First of all, viewing child sexual abuse material may be a criminal offence. In order to facilitate notice and takedown, legal frameworks should exempt designated industry staff from prosecution. Check to see if your employees are exempt and how best to protect them. Protection in law from strict legal liability is an important element in encouraging commitment and action on removing CSAM within industry and addressing employee anxiety and distress over potential prosecution for processing CSAM reports. If no exemption applies in your country you may wish to consider working at an industry level to press for such protection.

Ensure that designated employees are comfortable with the role of investigating and removing CSAM. It is also good practice to ensure staff are vetted and assessed for their suitability for the role that they agree to regarding the review and takedown of CSAM.

Make sure the recruitment process is transparent and that employee contracts set out their role and the support offered by your company. Hotlines such as the Internet Watch Foundation use the interview process to assess "whether applicants have the personal attitudes and qualities appropriate to the role prior to progressing to the more formal stages of interview."[19]

Constant exposure to child sexual abuse material can be stressful and even traumatic for employees.[20] You can equip and help protect your staff by following some simple steps:

- Engage with other industry peers, hotlines and law enforcement to identify training and resource requirements to ensure employees are equipped to do their jobs effectively and feel empowered to combat CSAM.
- Conduct testing to ensure staff understand and effectively implement company policy and specified processes.
- Limit the amount of time employees are exposed to CSAM.
- Provide a dedicated workspace to the team that handles reports of CSAM.
- Provide privacy screens for desktop or laptop monitors to help prevent accidental exposure of CSAM and related reports to other employees.
- Establish an employee support programme and provide access to confidential counselling services.

Adopting these measures can help reduce employee turnover, illness and sick leave related to this challenging task.[21]

18 See for example, 'Guidelines for Law Enforcement' adopted by Twitter <https://support.twitter.com/articles/41949#5>
19 Smith, Sarah, Global Strategies for Tackling Child Sexual Abuse Material Online (2014) report produced for the Winston Churchill Memorial Trust, 2014, n.p.
20 See, for example: Reisman, Judith, 'Picture Poison: Viewing pornography for a living can be deadly', Salvo, Autumn 09, pp. 23–25, <www.practicalhomicide.com/Research/ReismanSV10.pdf>.
21 *For more information on supporting employees, see:* Technology Coalition, *Employee Resilience Guidebook for Handling Child Sexual Abuse Images*, March 2013, <www.technologycoalition.org/wp-content/uploads/2012/11/EmployeeResilienceGuidebookFinal7-13-1.pdf>; and INHOPE, *Staff Welfare Best Practice Paper*, 2013, <http://inhope.org/Libraries/Best_Practice_Papers/Best_Practice_-_Staff_Welfare_2013.sflb.ashx>.

3.6. Clarify customer terms and conditions

Terms and conditions offer a crucial way for a company to make clear what content and behaviour is acceptable and to prohibit illegal activities such as the circulation of CSAM. Clearly state details on the following items in terms and conditions:

- Note that offering or distributing illegal materials such as CSAM or other actions to sexually exploit children are not allowed.
- Specific actions that will be taken by the company, such as reporting CSAM to law enforcement or hotlines, and cooperation with any investigation and prosecution, including the preservation and disclosure of associated data.
- Whether you will suspend or close accounts and services if the terms and conditions are violated.
- The redress process that is available if customers wish to challenge a decision to remove or otherwise act on reports of CSAM.

It may also be useful to provide hyperlinks to information about the company's position on CSAM and an acceptable use guide, and/or links to guidance or resources provided by law enforcement or a national or international hotline organization.

The intent is to leave customers in no doubt about their responsibilities and the rights and powers of a business to deal with reports of potential CSAM.

4. DEVELOP RELATIONSHIPS AND WORK WITH KEY STAKEHOLDERS

Liaison with industry, government, law enforcement and hotlines is invaluable in developing robust practices for combating CSAM. While national laws generally make the production and distribution of CSAM illegal, such acts take place across borders and legal jurisdictions. Combating CSAM in a globally connected world requires cross-border cooperation and enforcement – it is a shared responsibility.

Engagement and cooperation are crucial to achieving a number of key aims and joint responsibilities, including:

- Swift removal of CSAM from circulation.
- Supporting the flow and collation of intelligence to help identify and rescue children who appear in CSAM, as per INTERPOL's International Child Sexual Exploitation image database.[22]
- Ensuring there is 'no space' online for CSAM and that people work together to protect children's right to privacy and freedom from sexual exploitation and violence.

4.1. Industry relationships

Consider establishing relationships with industry peers and developing an industry-level code of practice that sets out policy and standardized practices on notice and takedown of CSAM. This encourages the sharing of best practice and strengthens actions against CSAM at the national and international levels. An example of this is the global Mobile Alliance Against Child Sexual Abuse Content, which has produced a range of guidance and advice and created a network of invaluable relationships to help keep mobile services free from CSAM.[23]

In the United Kingdom, a broad coalition of industry engaged with the national hotline, the Internet Watch Foundation, and agreed on a code of practice that defines the notice and takedown procedure by which service providers remove or disable access to potentially illegal content hosted on their networks after receiving a notice from the IWF.[24]

22 INTERPOL, 'Victim Identification', 2016, <www.INTERPOL.int/Crime-areas/Crimes-against-children/Victim-identification>.
23 GSMA, 'Mobile Alliance', <www.gsma.com/mobilealliance>.
24 Internet Watch Foundation, 'IWF Funding Council Code of Practice for Notice and Takedown of UK Hosted Content within IWF Remit', <www.iwf.org.uk/members/member-policies/funding-council/code-of-practice>.

4.2. Hotlines

Dedicated national and international hotlines play an increasing and vital role in identifying and issuing reports of CSAM, in liaising with law enforcement and in issuing notices to industry for the effective takedown of abuse materials. As a company, you may wish to identify the national hotline and engage with it to help establish good practice and a dedicated line of communication to ensure the effective receipt and action of a takedown notice.

Information about, and links to, national and international hotlines is offered by INHOPE,[25] a collaborative network of 51 hotlines in 45 countries worldwide dealing with illegal content online. If no hotline is available in your country, you can consult the joint GSMA and INHOPE publication on setting up a hotline, or the INHOPE Foundation's interactive 'Hotline Development Guide'.[26]

4.3. Law enforcement

Engagement with law enforcement will help foster strong relationships that support knowledge sharing and the development of best practice, and help ensure notice and takedown procedures are effective and operate in accordance with national legal frameworks. Your national and regional law enforcement agencies may have dedicated units and specific policies regarding the investigation, and prosecution when appropriate, of CSAM.

A good place to start would be the website of your specific law enforcement organization, and those of international law enforcement agencies and hotlines that handle notice and takedown for CSAM. Links to related information and resources include the following:

- INTERPOL helps provide training and promote best practice for police forces in its member countries on combating CSAM. Information on Internet crimes against children can be found at <www.INTERPOL.int/Crime-areas/Crimes-against-children/Crimes-against-children>.
- The Virtual Global Task Force represents national, regional and international law enforcement agencies that have come together to combat online child sexual abuse worldwide. Its also provides links to regional law enforcement and CSAM reporting hotlines, at <http://virtualglobaltaskforce.com>.
- The Council of Europe's *Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime* was developed to help service providers and law enforcement in any country establish effective working relationships. It is available, in more than a dozen languages, at <www.coe.int/en/web/cybercrime/lea-/-isp-cooperation>.

25 International Association of Internet Hotlines, <www.inhope.org>.
26 GSMA Mobile Alliance Against Child Sexual Abuse Content and INHOPE, Hotlines: Responding to reports of illegal online content – A guide to setting up an Internet hotline, August 2014, <www.gsma.com/mobilealliance>; and INHOPE Foundation, 'Hotline Development Guide', <www.hotlinedevelopmentguide.org>.

5. COMPLIMENTARY TOOLS AND CAPABILITIES

Notice and takedown is but one crucial tool to combat child sexual abuse material. When you develop products and services, it is good practice to identify in what ways they could be exploited and misused to sexually exploit children and create or distribute CSAM. Asking such questions helps identify solutions and has led to the development of a number of other tools, resources and practices to help prevent and disrupt the availability of CSAM online. Some of these tools and resources include:

- List of URLs containing CSAM are maintained by a number of hotlines, such as IWF and NCMEC,[27] and made available to member organizations, which can choose to block access to any listed URL.
- INTERPOL maintains and makes available a 'Worst of' list of URLs that can be used to limit the distribution and availability of CSAM on access networks.[28]
- BASELINE, which is being deployed by INTERPOL, is a scheme that will allow industry to scan its systems for CSAM by sending hash signatures to a server over an application programming interface for a 'hit/no hit' response to help identify and remove the material from their networks.
- PhotoDNA, developed by Microsoft, is a technology that automatically helps detect and report the distribution of child exploitation images.[29] PhotoDNA can help reduce costs and make notice and takedown more efficient, making it possible to remove images of child sexual abuse more quickly.
- In the industry initiative 'Hash Value Sharing', hotlines such as the IWF,[30] NCMEC and INHOPE are creating unique digital fingerprints, or 'hash values', from identified child sexual abuse images. Lists of the hash values are made available to member organizations and may also support international or national initiatives. The Government of the United Kingdom, for example, is using this technology in its newly established Child Abuse Image Database.[31]

27 IWF, <www.iwf.org.uk/members/member-policies/url-list>; NCMEC, <www.missingkids.org/Exploitation/Industry>.
28 INTERPOL, 'Access Blocking', 2016, <www.INTERPOL.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list>.
29 Microsoft, <www.microsoft.com/en-us/photodna>. Also see: INTERPOL, '<www.INTERPOL.int/News-and-media/News/2015/N2015-041>.
30 IWF, 'Hash List "could be game-changer" in the Global Fight against Child Sexual Abuse Images Online', 10 August 2015, <www.iwf.org.uk/about-iwf/news/post/416-hash-list-could-be-game-changer-in-the-global-fight-against-child-sexual-abuse-images-online>.
31 Government of the UK, 'Guidance: Child abuse image database', 16 November 2015, <www.gov.uk/government/publications/child-abuse-image-database>.

6. SUMMARY AND CONCLUSIONS

To be effective, notice and takedown requires national, regional and international cooperation and the sharing of information, knowledge and best practice, as evidenced by the tremendous efforts of industry, hotlines, law enforcement and non-governmental organizations in various jurisdictions. Such efforts should inform the revision and development of legal frameworks to ensure strong foundations for action in an increasingly connected world. Interoperability between legal frameworks across borders is necessary to ensure there is no space online for child sexual abuse material.

Combating child sexual abuse material and keeping children safe from sexual exploitation is everyone's responsibility, and needs us all to play our part. You can help ensure your organization supports the identification and elimination of CSAM by using the guidance in this document – and forging relationships with industry colleagues, hotlines and law enforcement to create a better world for children.

Further information and guidance on approaches to combating CSAM

Child Pornography: Model legislation & global review, 8th edition, International Centre for Missing & Exploited Children, <www.icmec.org/child-pornography-model-legislation>

Child Safety Online: A practical guide for providers of social media interactive services, UK Council for Child Internet Safety, <www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-parents-and-carers>

Global Strategies for Tackling Child Sexual Abuse Material Online, Sarah Smith, Winston Churchill Memorial Trust, <www.wcmt.org.uk/sites/default/files/report-documents/Smith%20Sarah%20Report%202014.pdf>

Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, Council of Europe, <www.coe.int/en/web/cybercrime/lea-/-isp-cooperation>

Guidelines for Industry on Child Online Protection, ITU and UNICEF, <www.unicef.org/csr/COPguidelines.htm>

Hotlines: Responding to reports of illegal online content – A guide to setting up an Internet Hotline, GSMA and INHOPE, <www.inhope.org/tns/resources/UsefulDocuments.aspx>

Mobile Operator's Contribution to Notice and Take Down in the Context of Illegal Child Sexual Abuse Content, GSMA Mobile Alliance Against Child Sexual Abuse Content, <www.gsma.com/mobilealliance>

Sound Practices Guide to Fight Child Sexual Exploitation Online, Thorn, <www.wearethorn.org/sound-practices-guide-stopping-child-abuse>

Child Online Safety Assessment Tool, UNICEF, <http://www.unicef.org/csr/childrensrightsandinternet.htm>


GSMA™


unicef