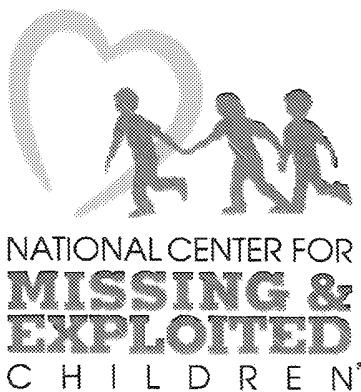


EXHIBIT 9



CYBERTIPLINE ROUNDTABLE: ESP INFORMATION REPORT

FACEBOOK and INSTAGRAM

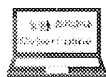
CREATION DATE: MAY 10, 2019

This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC's records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC's nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.

META3047MDL-050-00020036
METANMAG-007-00020093



OVERVIEW



Facebook and Instagram submitted a total of **17,366,320** reports to the CyberTipline in 2018, containing a total of **42,189,807** uploaded files (23,470,087 uploaded files were reported files; 18,719,720 were supplemental).



The CyberTipline received feedback from law enforcement regarding **26,819** of these reports, including **584** that appear to be related to an arrest. This report further details features or trends seen in CyberTipline reports submitted by Facebook and Instagram.



Facebook will be represented as **ESP #5** and Instagram will be represented as **ESP #20** on any anonymized group presentations shown during the 2019 CyberTipline Roundtable. The specified or named information in this report has only been shared with the Facebook and Instagram representative(s) in attendance.



ESP REPORT AND NOTIFICATION BREAKDOWN – 2018

REPORT OVERVIEW

	Total Reports	ESP Escalated Reports	Meme Reports ¹
Facebook	16,857,881	870	5,779,668
Instagram	508,439	1	79,175

REPORTS BY NCMEC PRIORITY

	Priority 1	Priority 1 – ECD Escalations	Priority 2	Priority 3
Facebook	16,854,578	1,752	1,234	317
Instagram	508,077	313	41	8

¹ Defined as a report where all reported files have been tagged as Potential Meme by the reporting ESP.

This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC's records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC's nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.



UPLOADED FILES OVERVIEW

	Total Files	Images	Videos	Other	Potential Memes ²	Supplemental ³
Facebook	41,521,716	20,739,990	20,765,890	15,812	7,331,901	18,719,720
Instagram	668,091	247,268	420,643	180	111,246	0

VISIBILITY OF UPLOADED FILES

	Total Reported Files	Reviewed by ESP	Publicly Available	Override by NCMEC Analyst	Not Viewable	Total Reports with No Viewable Files
Facebook	22,801,994	1,625,350	0	5	49,396	26,539
Instagram	667,732	166,446	0	0	2,962	1,998

NOTIFICATIONS

	Total Notices	First	Second	Thirds	Fourth	Average Days to Take Down
Facebook	8	5	3	0	0	4.50
Instagram	69	40	25	4	0	4.40

ESP REPORT FEATURES

ESP REPORTING PRACTICES

Uses ISP/WS?	Submits Supplemental/Deep Dive Reports?	Submits ESP Escalations?	Provides Incident Date/Time Description?
✓	✓	✓	x

UTILIZATION OF UPLOADED FILE FEATURES

Industry Classification	Potential Meme Tag	File IP Events include Timestamp	Labels File Upload IP Events
✓	✓	✓	✓

² Count of files tagged as Potential Meme by the reporting ESP.

³ Count of files tagged as Supplemental by the reporting ESP.

This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC's records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC's nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.



UTILIZATION OF XML UPDATES

Updated File Tags ⁴	Indication if EXIF Viewed by ESP	Phone Number Verification	Multiple Phone or Email Fields
x	x	x	x

ESP HASH INITIATIVES

	Access	Date of Last Ingest	Date of Last Entry
NGO Platform	✓	April 30, 2019	
Industry Platform	✓	April 10, 2019	May 09, 2019
Exploitative List	✓		

ESP FEEDBACK PROVIDED TO NCMEC BY LAW ENFORCEMENT - 2019

FEEDBACK FROM DOMESTIC LAW ENFORCEMENT AGENCIES

	Total	Conviction	Arrest	Ongoing Investigation	Closed
Facebook	20,418	1	493	2,571	17,353
Instagram	6,029	0	64	625	5,340

FEEDBACK FROM INTERNATIONAL LAW ENFORCEMENT AGENCIES

	Total	Conviction	Arrest	Ongoing Investigation	Closed
Facebook	346	0	27	22	297
Instagram	26	0	0	1	25

⁴ Updated file tag options include Anime/Virtual/Hentai, Viral, Possible Self-Production, Physical Harm, and Violence/Gore. This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC's records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC's nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.



APPENDIX – CYBERTIPLINE BEST REPORTING PRACTICES

This appendix overviews five improvable ESP reporting trends seen in CyberTipline submissions and details NCMEC’s feedback and suggested best practices. This appendix may be referred to when reviewing the “ESP Report Features” section of this information report.

LACK OF CONTEXT OR PERTINENT INCIDENT INFORMATION PROVIDED IN REPORTS

- Trend:
 - o Submitted reports do not contain enough context or pertinent incident information to be actioned by law enforcement.
- Feedback:
 - o Reports that do not contain incident information cannot be actioned because it is unclear how the report was generated or when incident occurred.
 - Example: report does not contain a description to indicate what the incident date and time reflect.
 - Example: IP events are unlabeled so it is unclear if an upload occurred.
 - Example: IP events do not contain timestamps, so it is unclear when an event occurred or who was associated with the IP address at that time.
 - o Reports that do not contain enough context cannot be actioned because it is unclear what incident occurred.
 - Example: possible enticement where there is no indication that the victim is a potential minor.
- Best Practice:
 - o Include a description of any incident times, label IP events, provide timestamps for IP events, and provide clear context for the incident that is being reported.

LACK OF FILE ANNOTATION BY REPORTING ESP

- Trend:
 - o Submitted uploaded files are not labeled with industry classifications or other available reporter tags.
- Feedback:
 - o Use of industry classifications and reporter tags assists in the initial triage of reports by providing context of what the uploaded files depict.
 - o When files are not annotated, international law enforcement agencies do not receive any uploaded file contextual summary for auto-referred reports.
 - Example: if the files are not annotated, the summary of an auto-referred report containing 500 images of anime would appear the same as the summary of an auto-referred report containing 500 images of egregious CSAI.
 - o When files are not appropriately tagged by the reporting ESP, any automated processing or triaging systems are unable to occur. This can cause a disproportionate amount of time to be spent working on a large volume non-actionable reports.
 - Example: When a report resolves internationally and contains untagged Potential Meme images, it is auto-referred as an actionable report to international law enforcement.

This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC’s records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC’s nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.



- Example: When a report contains untagged Potential Meme images, CyberTipline analysts must manually review and process the reports.
- Best Practice:
 - Utilize the available uploaded file reporter tags (Potential Meme, Viral, Possible Self-Production, Bestiality, Violence/Gore, Physical Harm, and Anime/Drawing/Virtual/Hentai) and industry classifications when submitting uploaded files.

NON-REPORTABLE CONTENT

- Trend:
 - Reports containing adult content, inanimate objects, or other non-reportable incidents are being submitted.
- Feedback:
 - CyberTipline analysts spend a disproportionate amount of time identifying and manually processing these reports, which are not sent to law enforcement as they are not actionable. This takes time away from processing actionable, high valuable reports.
 - These reports may be auto-referred to international law enforcement agencies, which similarly affects their triaging and takes time away from processing actionable reports.
- Best Practice:
 - Ensure reports submitted to the CyberTipline concern child sexual exploitation.

STRUCTURED REPORTING FIELDS NOT BEING UTILIZED

- Trend:
 - Submitted reports contain pertinent information in free text fields rather than the available structured fields.
- Feedback:
 - Reports contain free text templates indicating the reporting ESP has viewed the uploaded files submitted in the report, but the structured File Details field does not contain this information. These files must be manually overridden by a CyberTipline analyst to be viewed, and as they are initially unviewable they do not receive initial triage by automated system alerts (such as unique PhotoDNA clusters or alerts concerning available EXIF metadata).
 - Reports contain free text templates indicating the reporting ESP has viewed EXIF metadata associated with the uploaded files, but the structured File Details fields do not contain this information. When this information is not provided in a structured field it will not receive initial triage by automated system alerts (such as EXIF metadata alerts for a recent create date or EXIF metadata alerts for included GPS information).
 - Reports contain free text templates indicating the uploaded files appear depict anime or were shared for comedic effect, but the structured File Details fields do not contain this information. This prevents automated report triaging from occurring, and CyberTipline analysts must manually process these reports. Similarly, these reports may be auto-referred as actionable to international law enforcement agencies.
 - Reports contain additional identifiers associated with a reported user in a free text field rather than available structured fields. This prevents automated system alerts from running (such as a suspicious

This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC's records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC's nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.



email domain or suspicious IP address), and slows down CyberTipline analyst processing as information must be manually deconflicted from free text fields.

- Best Practice:
 - o Enter report information into the available structured fields whenever possible.

SUBMISSION OF MULTIPLE SINGLE IMAGE REPORTS RELATED TO THE SAME USER

- Trend:
 - o Multiple reports related to the same user are submitted in quick succession, and each report only contains one uploaded file.
- Feedback:
 - o This creates more work for law enforcement when they are referring reports out for investigation, and some agencies must treat each separate report as an individual write up.
 - o Some law enforcement agencies' downloader or triage systems are unable to receive large volumes of reports at once, which can cause referrals to span over several days and prohibits their ability to receive other reports.
 - o Reporting statistics are skewed when numerous single image reports are generated for the same user.
 - o This slows down report processing for the CyberTipline, as analysts must identify related reports, group them together for law enforcement, and access them individually to review the reported information.
- Best Practice:
 - o Rather than submit numerous related reports in quick succession that contain a single image, submit one report with multiple images.

This Report is provided to the attendee of the 2019 CyberTipline Roundtable whose attendance represents the Electronic Service Provider (ESP) that the Report describes. The information contained in this Report is derived exclusively from NCMEC's records and is current only as of the creation date indicated above. The information contained in the Report may not be comprehensive. This Report is intended solely for informational purposes in furtherance of NCMEC's nonprofit mission to operate the CyberTipline. Please treat the information in this Report as sensitive and confidential and do not reproduce or further distribute this Report.