Understanding NCMEC CyberTipline Reports

August 30, 2019 | Steven

Investigations into child pornography offenses often begin with the receipt of a CyberTipline Report from the National Center for Missing and Exploited Children (NCMEC). Both prosecutors and defense attorneys should be familiar with these reports and the information they can contain.

The NCMEC is a non-profit organization established by Congress to help prevent child abduction and sexual exploitation. One of the functions of the NCMEC is to manage the CyberTipline, a clearinghouse for complaints of child sexual exploitation and child pornography. In 2018, the CyberTipline handled over 18 million reports. NCMEC reviews incoming reports and refers them out to the appropriate law enforcement agency, typically a regional Internet Crimes Against Children (ICAC) task force.

Anyone can make a CyberTipline Report, but the majority of the reports will be from electronic service providers (ESP), i.e. web sites and online services. ESPs are required to report child pornography when it is brought to their attention and many of them actively flag or search for this material using software such as PhotoDNA (which Microsoft donated to the NCMEC). It may not be clear from a CyberTipline Report whether an individual reported the offending material, or the ESP detected it on its own.

A CyberTipline Report is a complaint. In most cases, additional information will need to be acquired via a warrant or subpoena in order to get the account details, logs, and other context needed to ultimately support charges for the distribution of child pornography.

The first page of a CyberTipline Report will contain the date it was received, its assigned report number, and an executive summary. The executive summary will say what type of incident the report refers to, such as “Apparent Child Pornography”, and the number of files that were uploaded.

The first section of a CyberTipline Report, Section A, will contain contact information for the electronic service provider making the report. It may also contain information about how to request additional information. In most cases, additional content, logs, accounts records, etc. are available with a warrant or a subpoena. It is important that investigators pay attention to this section and follow up in a timely manner as ESPs may have relatively short retention periods for this data.

Section A will also include a brief incident description, the time of the incident, the webpage involved, and the email, username, and IP address of the person reported. The IP address will only be the address directly related to the report (e.g. the address used to upload the offending files). The company may have historical

logs showing other addresses that were used to access that account. They may also have additional information about the user such as their user profile, billing information, etc.

At the end of Section A is the "Additional Information Submitted by the Reporting ESP." This section may be used to submit notes, log entries or other information that would be relevant to investigators. It's important to understand, however, that any log entries included here may not be the original or complete logs associated with the event. More likely, it is a summary. For example, the reports from one ESP include entries similar to this:

Post ID 555123456: IP 10.5.1.147 on 2019-07-03 at 14:31:46 EDT.

This only shows the ID assigned to the posted content, the IP address the upload was received from, and the date/time; this is less information than is typically recorded by a web server or web application. The complete log entries might include additional information such as the web browser that was used (or whether it was a mobile app), how much data was transferred, the username associated with that action, the name of the file, etc. This is important for two reasons. First, the missing information could help to implicate or exculpate a defendant. Second, there could be evidentiary issues if the logs given in the NCMEC report, rather than the originals, are used in court due to their being modified, summarized, combined, and/or interpreted.

At the end of Section A, there should be some information provided about each of the files that were uploaded. For each file, it should say whether the reporting ESP viewed the file and whether the file was publicly available. If the ESP did not report this information, it will say "(Information Not Provided by Company)". This is important because if the file was not publicly available, a distribution charge may not be warranted.

Section B is short and includes geolocation information for the offending IP address given in the report. This location should be considered approximate and is appropriate for locating the correct law enforcement agency or task force but not for securing a warrant or identifying a suspect. The latitude and longitude given are usually based on the state and/or city associated with the IP address and usually represent the midpoint of the city or another arbitrary location rather than a specific address. The Internet Service Provider who owns or controls the IP address will also be listed. If the address is controlled by a residential ISP, investigators should be able to use a subpoena to get the subscriber information and service address for the account associated with the IP address at the time of the offense.

Section C is for any additional information. It may reference other CyberTipline Reports associated with the same username or IP address. It may also include unverified information from public websites.

Section D lists the law enforcement contact information for the agency the report was submitted to by the NCMEC.

The images or videos associated with the CyberTipline Report are provided to the appropriate agency along with the report, but they are NOT shown in the body of the report. The report itself should be able to be shared with defense counsel without any restrictions arising from the Adam Walsh Act. Remember, these pictures may or may not have been reviewed by the report ESP or the NCMEC.

Key Terms:

National Center for Missing and Exploited Children (NCMEC): a non-profit organization established by Congress to help prevent child abduction and sexual exploitation.

CyberTipline Report: A report of child exploitation received by the NCMEC and shared with a law enforcement agency.

Electronic Service Provider (ESP): An online service or website.

Geolocation: The location associated with an IP address. Provided as a latitude and longitude but usually represents the midpoint of a city or state rather than a specific address.