Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection

# Details

## Year

2017

## DOI

10.5281/zenodo.495775

## Issued

2017

## Language

English

## Volume

11

## Issue

1

## Start Page

## End Page

## Authors

Açar K.V.

## Type

Journal article

## Journal

International Journal of Cyber Criminology

## Topics

Online safety and policy regulation

## Implications For Policy Makers About

Fighting against child sexual abuse and child exploitation

# Abstract

Webcam child prostitution is an emerging form of online child sexual abuse which the victim simply sells his/her lives sexual images through Voice-over-IP (VoIP) applications. Although it doesn’t directly create some negative effects of traditional child prostitution like sexually transmitted diseases, it may provide future offenders and victims to the traditional crimes such as child prostitution and child sex tourism. Therefore, appropriate and effective prevention strategies for this heinous act should be introduced accordingly. In this respect, this article discuss the efficiency of current methods of detection and propose some futuristic methods such as metadata and content data analysis of VoIP communications by the private sector and the use of fully automated chatbots for undercover operations. The applicability of such new methods in real life heavily relies on legal amendments and requires further research on technical aspects in particular.

# Outcome

For metadata and content data analysis of communications by VoIP companies, there are major challenges in practice. To begin with, the private sector has greatly helped LEAs for individual online child sexual abuse cases, but they have never done big data analysis for this purpose. Considering the global response to the revelations of Edward Snowden, companies wouldn’t be eager to conduct massive scale analysis on their users’ data even for a noble cause like the prevention of WCP. Even though it is known a company is technically capable, it is impossible to compel them to actualize this idea in case the company is unwilling to cooperate. Moreover, if a company is willing to do such an analysis for WCP at the moment, there might be similar operational ideas for other types of crimes in the future. The possibility of such operational expansion would compel the private sector to avoid involvement in the current operations. Furthermore, in case the frightening capability of such power on users’ data is revealed to the public, even though the company declares they never use it again, privacy concerns regarding mass surveillance would grow and customer base of the related VoIP product might shrink consequently. Lastly, unlike intelligence gathering, legal background of these proactive and highly intrusive approaches does not exist for criminal investigations. Particularly for content data analysis, there needs a predefined and strict legal procedures to prevent misuse of such analysis both for LEAs and the companies