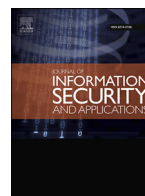




Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A forensic examination of the technical and legal challenges surrounding the investigation of child abuse on live streaming platforms: A case study on Periscope

Graeme Horsman

School of Science, Engineering & Design, Teesside University, Middlesbrough, Tees Valley, United Kingdom



ARTICLE INFO

Article history:

Keywords:

Live streaming
Digital forensics
Investigations
Policing and crime act 2017
Child sexual exploitation
Periscope

ABSTRACT

Video streaming provision are now widely used and whilst commercialised platforms face challenges with accessing and protecting copyrighted media, the emerging popularity of personalised live streaming services has resulted in a number of additional recorded abuses. In 2017, reports of personal live streaming platforms being used in acts of harassment, offences against the person and vehicle incidents have surfaced in the media. Of significant concern is the apparent use of streaming connected with acts of child abuse, where following the enactment of the Policing and Crime Act 2017, acknowledgement for the use of streaming for child sexual exploitation has been made in England and Wales. Whilst a positive step towards closing an apparent gap in legislation caused by this technology, practical enforcement of the offence may be difficult. This article investigates the challenges posed by the live streaming platform 'Periscope', offering an examination methodology for this application to support those investigating cases of abuse via Periscope. The results of a digital forensic analysis of Periscope's usage both in a web browser, Android and Apple mobile device platform presented. Periscope's footprint on Android and iOS is documented with key artefacts denoting a user's behaviour via the application are examined in order to support practitioners configure existing mobile forensic tools to extract and interpret resident Periscope application data, with analysis limitations noted. Findings are provided and discussed inline with their impact upon regulatory practices and live streaming investigations.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

Personal streaming technologies now feature prominently in the lives of many, increasing both the public's access to individuals, and an individual's potential ability to communicate *en-masse* with the public [44]. Whilst streaming offers a number of commercially viable incentives and benefits to the customer it has inherently lead to subsequent abuses, particularly with the increase in popularity of 'live streaming' in connection with social media services. The involvement of live streaming has been reported in cases of vehicle accidents [1,4], robbery [25], copyright infringement and piracy [9,13], assaults [16] and, trolling and harassment [11]. In addition, in 2017 a number of incidents involving the live streaming of child abuse have, and continue to be reported [5–8,10,12,14,43]. As a result, the National Crime Agency [30] commented in December 2017 stating that 'dangerous offenders are capitalising on the immediacy of contact that live streaming offers, as well as the ability to target children with a large number

of comments in real time'. Periscope, (Twitter's live streaming platform) and other streaming services such as Facebook's 'live' function have both been singled out for their use in a number of recent child abuse incidents [2,6,18,31,32,40].

This article presents the findings of a documented digital forensic examination of the live streaming provision Periscope on Android, iOS and computing (accessed via a web-browser) platforms. Artefacts left behind after each device has been used to generate and engage with live streams are identified and examined for the purposes of establishing 'accountability' (defined by Kafali and Singh [26] as the 'actions of an entity can be traced solely to that entity') and attributing Periscope behaviour to an identified suspect. Practitioners can utilise this information to configure existing commercial mobile forensic tools which are currently validated and used within their laboratories in order to identify, extract and interpret Periscope application data based on key file locations, type and structures noted in this investigation. Findings are discussed for the purpose of evaluating the practical enforceability of new legislation and offences surrounding live streaming. Contributions include an evaluation of the recent enactment of an offence of sexual exploitation which acknowledges acts of online streaming un-

E-mail address: g.horsman@tees.ac.uk

der Section 176 of the Policing and Crime Act 2017 in England and Wales. Further, a documented methodology for approaching Periscope investigations, the identification and explanation of potentially relevant application files and their associated metadata, and a discussion of the limitations of Periscope streaming investigations are all offered.

The remainder of this article is structured as follows. Section 2 provides a discussion of the problems caused by streaming and the regulation of it, with an analysis of the sexual exploitation offences of the Sexual Offences Act 2003, as amended by Section 176 of the Policing and Crime Act 2017, provided. Section 3 presents the findings of a Periscope investigation when operated using a computer web browser, and via an Android and iOS application platform. Section 4 offers the discussion of the benefits and limitations of a live analysis of a device and Section 5 discussions regulatory issues surrounding streaming before conclusions are drawn in Section 6.

2. Background

Despite often attracting negative press, it is necessary to first state that not all live streaming is associated with contentious acts. Live streaming can exhibit the potential to act as a crime deterrent where knowledge of use in society may seek to prevent those from engaging in crime due to a fear of being identified by a passive observer. Live streaming platforms have recently been perceived as a method of protection and way of documenting live events for a user's protection, with cases of police violence and shooting in the United States [17]. However, often subsequent abuses attract greater attention.

Whilst it must be noted that most live streaming platforms maintain detailed usage policies documenting the acceptable uses of their service, regulating content in real time (as live streaming offers) is an arguably impossible task for vendors, leading to the inevitable inclusion of content in breach of its terms and conditions within their platforms. Reliance is often placed on self-regulation where fellow users who 'stumbleupon' unsavory streams or those in breach of law can draw attention to it by following designated reporting procedures. Pringle [38, p. 102] suggests organisations such as Twitter (the reported acquirers of Periscope) perceive it to be a 'slippery slope when a public company becomes the morality police'. Live streaming has increased in popularity, providing what Birmingham and David [15] describe as an 'open to all' platform, with potential vast, unregulated audiences as opposed to friend-to-friend style platforms. It also provides real-time access to events for participants who are not actively engaging or participating in themselves, with examples including the Baltimore riots and the use of Periscope to document the behaviour of all involved [37,38].

Following discussions in the UK House of Lords it was highlighted that 'the National Crime Agency reported that a new threat has emerged on the internet. While the number of static images of child abuse remains stable, there is a sharp rise in live streaming of videoed child abuse' [35]. Live streaming platforms provide a unique regulatory challenge and the act itself can cross multiple offence barriers where a single streaming act could result in liability for a range of offences in England and Wales. This has been acknowledged by the National Crime Agency [29, p.4] where 'the practice of live streaming is one example of how offenders can simultaneously create indecent images of children (IIOC) online, view IIOC, and commit contact abuse by proxy overseas'. In 2015 (p. 29–30), Europol highlighted live streaming as a key threat surrounding child sexual abuse online stating the following.

Child sexual abusers continue to exploit technology that enables the streaming of live images and video in many differ-

ent ways. This includes use of live streaming methods in sexual extortion cases, organising invitation-only videoconferencing of contact abuse among members of closed networks, as well as the trend reported in 2014 concerning the profit driven abuse of children overseas, live in front of a camera at the request of Westerners. The low cost to consumers of pay-per-view child sexual abuse makes it possible to order and view the abuse regularly without the need for downloading. This represents a significant driver for such a modus operandi to become even more widespread. The frequent small amounts of money being transferred through intermediaries minimises any red flags from financial transaction monitoring agencies.

Streaming can be a spontaneous or planned act, where child victims may be groomed to stream content in set locations at specific time periods [42]. Access to the content may range from public (allowing individuals to passively view content) to password protected forums and platforms where monetary exchange is provided for access [20,22]. From a single child abuse stream, content may be subsequently captured, fragmented and distributed a potentially unlimited number of times. As a result, a child victim has not just suffered physical harm as a result of the streamed video, but the likelihood of both short term and long term mental harm is increased [23]. Nasıroğlu and Çimen [28] document the case of child sexual abuse between brothers, which was subsequently documented on the Periscope platform. Whilst Periscope allowed a live broadcast of the original abuse, subsequent recordings were reported to be found by Interpol on a pornographic website in the United States. Such cases provide an example of the implications of live streaming being further distributed, essentially transforming it from a live broadcast to a captured video, for non-live streaming (or download) from an additional host service. In such situations, content can subsequently 'go viral' leading to an inability to contain it online.

Europol [21, p. 30] note a connection between 'live streaming and hands-on abuse, where live-distant abuse is followed by travel to another country to contact abuse the same children'. The use of live-streaming in cases of child sexual abuse is expected to increase as the technology develops and underlying broadband infrastructures allow for its use [21]. The regulation of such platforms can be hampered by the use of end-to-end encryption protocols preventing surveillance of transferred content, making it difficult to identify offenders and implement early intervention measures to prevent or possibly reduce the harm suffered by a child [22]. Whilst the rate of development of new technologies has led to a volatile sector, where applications have a short lifespan (see for example reports on the streaming application Meerkat [3]), Periscope's functionality has continued to strengthen their position in the market. There is no doubt that rigour regulation of live streaming should take place to avoid child abuse from occurring on such platforms, and in 2017 the United Kingdom's government took steps to acknowledge this need.

2.1. The law:- streaming and child abuse imagery offences in English law

Whilst streaming is in itself not a new form of technology, its subsequent popularity and involvement in the exploitation of children has prompted regulatory action from the UK government in the context of child sexual abuse. During preliminary discussion surrounding the Policing and Crime Bill, MP Karen Bradley noted despite previously having thought not possible, live streaming is now an issue [36]. Following Section 176 of the Policing and Crime Act 2017, acknowledgment for the inclusion of streaming as a form of 'sexual exploitation' has been made, amending the existing sex-

Download English Version:

<https://daneshyari.com/en/article/9952284>

Download Persian Version:

<https://daneshyari.com/article/9952284>

[Daneshyari.com](https://daneshyari.com)