No images? Click here

IPPC

Managing Digital Media Players for Persons Under Supervision

Brian J. Kelly, Cyber Analyst - IPPC Technologies

***DISCLAIMER OF ENDORSEMENT.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favor of IPPC Technologies.*

The Internet of Things (IoT) has introduced a plethora of devices into the home for entertainment, convenience, security and much more. Some devices are limited in their capabilities, while others rival that of personal computers. Digital Media Players (DMPs) have replaced VHS and DVD players, as well as standard cable boxes. DMPs allow users to access all types of entertainment content, almost instantaneously. DMPs can also allow users to access social networks, streaming video providers and web content (via browser). Being aware of the presence of and managing these devices is an important component to any Computer/Internet Management & Monitoring Program (CIMP).

DMPs include devices such as the Amazon Firestick, Apple TV, Roku Express, Chromecast with Google TV, etc. These manufacturers also embed their DMP platform into "smart" TVs. Current gaming consoles such as the Microsoft XBox and Sony Playstation can also function as DMPs. According to a survey reported in Statista.com regarding streaming device ownership in North America from 2017-2020 (https://www.statista.com/statistics/496117/streaming-to-tv-capabilities-devices-usa/) “In the fourth quarter of 2020, 28 percent of respondents to a survey held among Americans and Canadians reported owning a smart TV, up from 27.6 percent in Q2 2019. Amazon Fire TV Stick has seen a significant uptake in usage and ownership, with nearly 18 percent owning a player in 2019, compared to 30 percent in 2020.”

For identification purposes, please see images of popular DMPs below:

AMAZON FIRESTICK

APPLE TV

ROKU PLAYER

CHROMECAST WITH GOOGLE TV

In order to consider management/restriction options for DMPs, officers should be aware of the operating system of the device. For example, Amazon’s Firestick OS (Fire OS) is an Android-based OS; Apple TVs use tvOS which is based on Apple’s iOS. Each DMP OS platform allows users to download and configure apps to access content. Device settings, which include parental controls, can be configured within the device to control features such as installing new apps, level of content (i.e. TV-MA), etc. Implementing parental controls on a DMP can be an effective way to manage the device. Officers should be well-versed on the capabilities of the device, what a PUS may need/want to use a DMP for, what the parental controls allow and restrict, as well as possible alternatives (i.e. "dumb" TVs). Please see the links below for guidance on setting up parental controls on various DMP platforms:

Amazon Firestick:
https://www.techsolutions.support.com/how-

to/how-to-set-up-parental-controls-amazon-fire-tv-stick-12276

Apple TV
https://www.lifewire.com/set-up-parental-controls-apple-tv-4685513

Roku
https://www.alphr.com/manage-parental-controls-roku-device-complete-guide/

Chromecast with Google TV
https://support.google.com/googletv/answer/10070481?hl=en
Examination of DMPs, even in controlled environments, can be a challenge. Two physical methods are JTAG (Joint Test Action Group) and chip-off examinations. Both examination methods require direct access to a device circuit board, which can permanently damage the device. JTAG exams involve connecting to the test points on a device's circuit board. These points allow the examiner to access the internal components of the device for data extraction. Chip-off exams involve physically removing flash memory chips from the device's circuit board. The flash memory chip contains the device's data. There are white papers and other materials relating to other methods of examinations of specific DMPs. See the links below for discussions on the examinations of DMPs:

"Forensicast: A Non-intrusive Approach & Tool for Logical for Logical Forensic Acquisition & Analysis of the Google Chromecast TV" by Alex

Sitterer, Nicholas Dubois, and Ibrahim Baggili - University of New Haven

https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1100&context=electricalcomputerengineering-facpubs

“Amazon Fire TV Stick: A First Look” by Logan C. Morrison, Huw O. L. Read, Konstantinos Xynos, Iain Sutherland

thttps://www.researchgate.net/publication/319390292_Forensic_Evaluation_of_an_Amazon_Fire_TV_Stick

While not forensically-sound, a manual examination option would be for officers to take custody of a device, bring it back to a controlled setting and navigate directly through the device, taking notes and photos of relevant information. There may be limits to what is able to be recovered depending on the device and there is always the risk of changing crucial information such as date and time stamps. Examiners should be adequately trained in digital forensics and be aware of such risks before engaging in any examination.

At minimum, officers should note the make, model and serial number of any DMPs in a PUS residence and where the DMP is located. From there, officers can make determinations if the device should be completely removed from the residence, moved to another location (i.e. family member bedroom), “locked down” both physically (i.e tamper tape) and digitally (i.e. enabling parental controls) and plan for possible future examinations. Conducting periodic

Internet Household surveys of a PUS residence should be standard operating procedure for any case with computer/Internet management/monitoring/restriction conditions. IPPC Technologies' computer & Internet monitoring solutions, which include robust artificial intelligence tools and services such as Spotlight and Express Scan, will assist officers throughout the supervision process. IPPC Technologies' training offerings include discussions on the risks and management of "smart devices" which include DMPs. We at IPPC continue to strive towards predictive and proactive solutions so officers can intervene early and address areas of concern. For more information on IPPC's services such as Spotlight, please call IPPC at (888)-WEB-IPPC or contact me directly at bkelly@ippctech.net or by calling (516)341-4201.

Share

Tweet

Share

Forward

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET