### Police live streaming

The future of Artificial Intelligence in live, mobile broadcasting



Seliton

### Police use Artificial Intelligence (AI) with live stream mobile video: The future of law enforcement

Artificial Intelligence (AI) is shaping the way in which we see and analyse the world. New smart device applications are giving people the insight of computer learning and intelligence. Interest in AI is booming as are applications for customer experience enhancement, unprecedented efficiency in analysis and big data application.

Many people can name examples of AI in consumer markets; such as self-driving cars, in-house connected homes and smart speakers like Amazon's Alexa or Apple's Siri. However, many people struggle naming an application in the B2B market, never mind specifically in law enforcement.

Al in law enforcement is still in its infancy, but it is growing up fast. Every day new possibilities are uncovered, and new ways in which it can be applied are explored. Innovation is pushing the boundaries in policing and public safety. This e-Book will focus on Al's recent and potential application in law enforcement.



### About this eBook

Artificial Intelligence (AI) can take many forms from machine learning to pattern recognition.

In order to fuel the imagination for AI in law enforcement, this eBook incorporates examples of innovative applications and future plans from police forces around the world. It addresses pain points for effective public safety and law enforcement and show smart remedies.

As AI can be present in many forms, this eBook focuses on law enforcement's application of pattern recognition, trend analysis and data mining.

The second eBook focuses on two examples of machine learning (or learning algorithms) in crime deduction, the role of IoT (Internet of Things) in evidence gathering and the launch of robotic police.

Soliton Systems Europe N.V. Gustav Mahlerplein 2, 1082 MA Amsterdam, The Netherlands | +31 20 301 2166 | emea@solitonsystems.com | www.solitonsystems.com 2018 0 Al information herein was carefully gathered and examined, however, Soliton Systems cancer be held responsible for mitatives of incompleteness of contents. Soliton 2018 to Al information herein was carefully gathered and examined, however, Soliton Systems cancer be held responsible for mitatives of incompleteness of contents. Soliton 3018 to Al information herein was carefully gathered and examined, however, Soliton Systems cancer be held responsible for mitatives of activities underske based and the contents.

## Data analysis of pedestrians and street crime suspects

Police and public services can improve surveillance efficiency through profiling analytics. Law enforcement agencies can effectively support policing through running data analysis on livestream videos to review suspicious activity.



Promotional image from the BodyWorn body camera company, Utility, Inc./Flickr (CC BY-SA 2.0)

For example, if the police receive a tip that there is a drug dealer on a street. The police can set up a covert camera and broadcast footage from that street to a command centre VMS (video management software).

This live footage can be analysed in real-time with AI to track pedestrian movements on the street. They can analyse all traffic and pedestrian activity in view. The data analysis tool can show the most popular addresses in the street. This gives the local police an indication of which houses were most frequently visited, and consequently, which houses they should call at. As well as gathering evidence, this analysis focuses police time on addresses with the highest chance of finding the dealer.

If there is a drug dealer operating on a particular street, his walking patterns can be monitored and analysed in the same way. The locations where he chooses to stop, or to linger, can be analysed remotely from the livestream footage. The most frequent stopping places could be either where he hopes to meet his customers, but could also be the areas where he chooses to hide his stash of drugs.

A dealer may not to carry all the drugs on him, as it's too risky in case he was arrested. It is more likely that he has only a selection of drugs physically on him at any one time. By successfully learning from his movements through AI, the likelihood of discovering his full stash of drugs is increased.

Soliton's Zao-S is a mobile video encoder that can encrypt video (AES256) and live stream reliably over multiple 4G connections using the latest compression technique of H.265. The video quality is high and can transmit in full HD. It can be used with another layer of Artificial Intelligence, such as pattern analysis.



**Se**liton<sup>®</sup>

### **AI Traffic Analysis**

Imagine a crime was committed by a person in a car with fake number plates. The criminal then successfully switches number plates after the crime and disappears.



Al can help retrace the steps of the criminal for the previous eight hours, before the crime was committed. The police Al tools can analyse hundreds of CCTV and security cameras footage, which were streamed to central command.

This huge video analysis can focus on the number plates across all recorded videos in the area. This work would be too time-consuming to be done manually and at normal viewing speed. Once the correct vehicle has been located, the police can see where the criminal has travelled from. They could also see with whom he has met (to increase the number of people of interest in the case). The law enforcement agencies can connect the criminal with the car, possibly before the licence plates were changed.

Analysis of all the CCTV and broadcast data becomes more difficult for humans, as the sheer volume of videos recorded increases. It soon becomes impossible for a human eye to track suspects over hours of footage, especially if reviewed at speed. An AI system can quickly scan multiple collections or archives of footage, much faster than humans in real-time. AI can focus the search for the right footage to assist in cases. By having videos streamed in full HD (1080i/1080p) in broadcast quality, facial recognition can be used to improve tracking of the criminal once his vehicle is identified. Facial recognition software can then scan further video archives for evidence of involvement from similar crimes.



john-cameron-757626-unsplash

Read more in Soliton's whitepaper on Facial Recognition with Secure, Accurate Facial Recognition (SAFR).





#### **Crowd safety with AI**



Police and public services can also improve surveillance efficiency through pattern analytics. Law enforcement agencies can run pattern analysis and facial recognition on livestream HD videos.

Around the world police are striving to improve prediction in their counter-terrorist measures. The German police for example, are looking into ways to detect abnormalities in crowd behaviour. With motion and speed trackers, it becomes possible to focus in on more suspicious people. Such as people running through crowds.

Individual suspect's direction and speed can be tracked and analysed with AI tools. The police can add to their learning software certain questions, such as, 'are people running towards or away from an incident's epicentre?' The police can focus on the people who are running in a non-conform direction (opposite direction to the main crowd) or people who were running before the incident.

Nowadays, the police can track down criminals using a multiple of set of tools, including livestream facial recognition. This facial recognition software can work on live streams from HD cameras including CCTV, mobile body cams, mobile phone streaming or from cameras mounted on drones. This can cross-check with suspected terrorists or criminals in their database.

Read more about Soliton's Live Mobile Broadcasting for Crowd Safety or Mobile Surveillance in the Public Domain

#### **Click Here**

### Al privacy challenges



matthew-henry-87142-unsplash

Law enforcement will face many challenges, when they progress from theoretical ideas (of what they can achieve with AI) to actual, physical implementation of AI, especially in the area of data privacy.

The increased use of CCTV remains a controversial subject with both pro's and con's. In China, private companies have access to a government facial recognition database of 700 million people (half its population in 2017). Almost everyone with identification in China and is over the age of 18 is on the national face recognition database. People offer their facial recognition compliance in exchange for convenience, e.g. To unlock their phone, but increasingly to pay bills, gain access to work and other secure premises...

It will remain a challenge to use all tools available without breeching national privacy and non-discrimination laws. In the EU most CCTV footage is deleted 30 days after it's recorded. You can request to the owner of the CCTV system to share their footage. Your image is seen as your personal data in the EU (more info here).

Soliton's Zao-S is a mobile video encoder that can encrypt video (AES256) and live stream reliably over multiple 4G connections using the latest compression technique of H.265. The video quality is high and can transmit securely in full HD, without the fear of hacking the footage. It can also be combined with many applications with another layer of Artificial Intelligence. Click here for our free white paper on Facial Recognition.

# Police profiling eliminating prejudice

Any use of large-scale monitoring will need to be unbiased towards ethnicities etc, instead new technologies can focus on spotting anomalies of behaviour and movement.



Shutterstock

This is not as easy as it seems. The AI algorithms, used to scan and review millions of hours of footage or documentation, are created by humans. AI will encounter many learning steps as it develops. By sharing these experiences, it will only serve to build better systems in the future.

Al is based on the quality of information entered to create that learning algorithm. If a higher weighting is given to a certain ethnicity, for example, even if based on historical data, it will create a future higher prejudice to this group. This was seen in the cited Pro Publica investigation in 2016, which revealed how the COMPAS software – created by Northpointe– was biased against black offenders. 'The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants.' In the British Durham Constabulary, they use an AI system called HART. HART uses data from 34 different categories – covering a person's age, gender and offending history – to rate people as a low, moderate or high risk of re-offending. Within these data categories is postcode information. While postcode information initially seems harmless, it was called out by Andrew Wooff, a criminology lecturer at Edinburgh Napier University, who specialises in the criminal justice system. Wooff said that including location and sociodemographic data can reinforce existing biases in policing decisions and the judicial system.



Getty Images

See further uses of Soliton's Live Mobile Broadcasting for Law Enforcement.

### **Policing Social Media**

Research and skimming online activities and web traffic have increased in complexity. AI can be focussed on social media grooming to track down on suspect profiles, such as online paedophile groomers. AI is used to sift out all the noise on social media to target in on suspicious activity and help the research teams to track the suspect's activity.

Facebook uses PhotoDNA, a tool developed by Microsoft, to spot known child pornography images and video. Google has developed its own open source version of that tool. They use AI to detect blood and guts and also use audio detection to search for key wording.





Analysis of unusual social media has reduced martyrdoms. By analysing visits, comments and traffic to illegal organisations and promotional material, which haven't been confiscated and could be used as 'bait', they can build their own list of potential empathisers.

Major social channels are encouraging social media's self-policing to block illegal websites, videos and other onlinecontent. Thereby, they restrict inadvertently finding illegal material.



Microsoft Cybercrime Center

### **S**aliton

Download Soliton's white paper on Facial Recognition with live mobile broadcasting

## Criminal use of Social Media to promote activism

At least 50 people were murdered at two mosques in Christchurch, New Zealand in March 2019. The shooter apparently posted warnings on Twitter and 8chan before livestreaming the rampage on Facebook for 17 repulsive minutes. Almost immediately, people copied and reposted versions of the video across the internet, including on Reddit, Twitter and YouTube.



Facebook and Google have automated tools that can detect and remove photos, videos, and text that violate their policies. These programs generate digital signatures known as hashes for images and videos known. This aims to block the content from being reuploaded. As they block the initial video, people re-film the footage, or alter the video in some way and try to upload a seemingly new video. Facebook adds each banned video to a shared database, which enables technology companies to detect and automatically remove copies of the videos when uploaded again on these shared platforms.

What's more, Facebook and others have machine learning technology, which blocks suspicious visual content such as a video with an ISIS flag, a weapon or blood. Facebook is deploying the same AI for audio detection technology (crying, pleading, begging). All of that is in addition to AI tools that detect more down-to-earth issues, like copyright infringement. Automated moderation systems are imperfect, but can be effective. At YouTube, for example, the vast majority of all videos are removed through automation and 73 percent of these are removed before a single person sees them<sup>\*</sup>. Facebook said that during the 24 hours after the shooting, the company blocked more than 1.2 million attempts to upload the video. It took down more than 300,000 copies of the video that had been uploaded. Videos that included "praise or support" from the attack were also removed, she said, using a mix of automated technologies — like audio detection — and human content moderators.

\*The WIRED Guide to Artificial Intelligence



As a legal discouragement and impose more than self-regulation, the New Zealand government has condemned the sharing of video and arrested suspects face up to 14 years in prison for trying to share this unsavoury content. They also limited naming of the murderer to reduce martyrdom.

The livestreamed murderous rampage publicity may encourage further martyrdom in the social media era. Law enforcement and the self-regulated technology companies understand the necessity to stop future exploitation, by ensuring the technology stays ahead of the criminals seeking acclaim.

### **Predictive Policing with Big Data**



One such instance was when a serial arsonist was setting fire to parked trains. The police worked with a big data and AI analysis team to analyse the train times needed to get to those trains which were damaged.

They cross-checked all the travel card check-ins for people travelling by public transport to those destinations on the days a train was set alight. Through this thorough data analysis they managed to find a match. They identified the public transport travel card of the person responsible. The police were able to track him down and arrest him prior to another arson attempt.



#### Smart speakers and chatbots increase police efficacy

Privately we're used to asking Siri or Alexa to change our environment (put on music, change the lighting...) and to answer our questions (what's the time, what's the weather forecast list, why is the earth round?). Not only does AI help kids with homework, but it can dramatically overcome many public service admin headaches (such as retrieving the right file in the archive.)

Chatbots can't respond to emergency calls directly but they can quickly give call prompt information and direct the agent to ask the most vital questions. The technology is constantly learning and improving, as befits AI, but it can develop. Many online services can be supported via data analysis and response.





Think of automatically linking up the emergency helpdesk to live CCTV footage to the crime location and using the witness description or current activity to accurately enable police officers to find the perpetrator and suspects quicker. In high risk situations, by using fixed or mobile cameras the trained call centre staff can accelerate follow up, if facial recognition is available in the IT eco-system. The suspects can be followed on CCTV until the police arrive, who are using live streaming body cams.

By using GPS overlay on the live video streaming, the police can optimise the location of their staff and resources. Click here to see other examples of Soliton specifications.

https://www.kisspng.com/png-logo-clip-art-map-gps-5813749/



### Smart image and footage archive

There is vast potential of advanced analytics linked to AI. We already know that there are powerful search engines. Imagine linking these powerful searching tools with image selection. Google images can do this on a global website scale and Google photos can allow you to do this with image recognition on your own photos.



Imagine the ability to tag all criminal arrest photographs, and search on archives to find them.

Imagine software tools auto-select profiles based on witness descriptions and ID sketches. If they can select on all physical appearances including matches to eye colour, hair colour, scars and tattoo location and images, with relevant past history and known geographic areas.

There are also automatically ageing tools, so that old footage can be used to predict what someone would look like now. Maybe in the future, this can enable the police to track current criminals in live streamed footage. Currently software can recognise one face from millions, within a second. It also can see the differences between identical twins. In China in 2017 there were around 170 million CCTV cameras and an estimated 400 million new ones will be installed in the next three years. China has what it calls "the world's biggest camera surveillance network".



'The Chinese government expects to integrate private and public cameras, leveraging the country's technological expertise in facial recognition technology to build a nation-wide surveillance network. After taking camera shots on the streets, the government uses an artificial intelligence system and facial recognition technology to identify each person captured and create an activity profile for the person.

See Soliton's white paper on Facial Recognition with its partner Real Networks

### Who is Soliton?

Soliton Systems have their mobile transmitters deployed with law enforcement and first responders across the globe. Their ability to provide secure, full HD quality and highly reliable video streaming, from a remote location or a moving vehicle, has made them a favourite choice with many companies and government agencies.

Soliton can livestream over multiple 3G and 4G networks direct from a mobile camera. It can stream a fully encrypted HD video back to a command centre from remote locations, with a latency of less than one second delay end-to-end. Milestone's Xprotect Video Management Software (VMS), can select, monitor and record incoming video streams, and allows orgnaistion a secure and scalable platform for managing all their live surveillance needs.

For more information on Soliton please refer to their website:



http://solitonsystems.com/solutions/public-safety-broadcasting

See further uses of Soliton's Live Mobile Broadcasting for Law Enforcement.

Click here

Soliton Systems Europe N.V. Gustav Mahlerplein 2, 1082 MA Amsterdam, The Netherlands | +31 20 301 2166 | emea@solitonsystems.com | www.solitonsystems.com

2018 © All information herein was carefully gathered and examined, however, Soliton Systems cannot be held responsible for mistakes or incompleteness of content. Soliton Systems may change or modify parts at any time without notification and accepts no liability for the consequences of activities undertaken based on the contents.