Information security and privacy protection aspects of CCTV systems

28th March 2018

Professor Dr. Milan Marković of Paneuropean University Apeiron, Republic Srpska, Bosnia and Herzegovina, discusses the impact of CCTV systems on information security and privacy.

Closed-circuit television (CCTV) is a TV system in which signals are not publicly distributed, but are monitored, primarily for surveillance and security purposes. CCTV systems rely on

strategic placement of cameras and observation of the camera's input on monitors. As the cameras communicate with monitors and/or video recorders across private coaxial cable runs, or wireless communication links, they gain the designation "closed-circuit" to indicate that access to their content is limited to only those with authorisation to see it.[1]

The effectiveness of video surveillance technology is continuously improving, and it has already established itself as a vital security tool for the police, private companies and many public sector organisations.. An effective CCTV system contributes to the detection and prevention of crime, as well as protecting towns, cities and transport networks from the threat of terrorism.[2]

Advances in CCTV technologies – especially from analog CCTV cameras to internet protocol (IP) ones – certainly improves the safety and security that CCTV systems provide, but also increases information security and privacy concerns. Having in mind that the new EU privacy protection regulation, General Data Protection Regulation (GDPR), will be applied from 25th May 2018, information security and privacy protection concerns of CCTV systems are being recognised.

Applications of CCTV systems

There are three primary ways to use CCTV systems:

- As a deterrent;
- For forensic purposes; and
- As an interdictive device.[3,4]

Originally, CCTV surveillance systems were simply a deterrent. The notion that "Big Brother" was watching was often enough to keep people from misbehaving.

On the other hand, as recording and storing technologies and software, such as video analytics, have become more efficient, CCTV systems have evolved into a forensic surveillance tool, enabling the collection of evidence after an event has taken place.

Finally, as CCTV surveillance systems become more easily integrated with monitoring devices, alarm systems and access control devices, a third use of CCTV is related to help security personnel to identify and interrupt security breaches as they're occurring, or even before they take place.

CCTV systems are commonly used for a variety of purposes, including:[1,3]

- Maintaining perimeter security in medium- to highly-secure areas and installations;
- Observing the behaviour of incarcerated inmates and potentially dangerous patients in medical facilities;
- Traffic monitoring;
- Overseeing locations that would be hazardous to humans, for example, highly radioactive or toxic industrial environments;
- Building and grounds security;
- Obtaining a visual record of activities in situations where it is necessary to maintain proper security or access controls, for example, in a diamond cutting or sorting operation, banks, casinos, or airports;
- Home security;
- Public transportation;
- Crime prevention;
- Business surveillance;
- School protection;
- Body worn;
- Sporting events;
- Monitor employees; and
- CCTV for Open Data purposes.

We should have surveillance cameras in public places because they ensure public safety. Rarely will anyone attempt to harm anyone else when they know their actions are being recorded on camera. Cameras keep the public and their personal property safe.[5]

The police can identify criminals through recordings on camera. Through surveillance cameras, the police can both prevent crimes from happening and can quickly solve criminal cases with material evidence.

Surveillance cameras protect against property theft and vandalism. It is very difficult for criminals to get away with stealing if there are cameras in operation. Therefore, the thief will often get caught. Surveillance cameras will catch the thief before, or during, the process of committing the crime.

Cameras, through video analytics, now have a zoom feature, allowing the camera to reveal someone's identity, which can be beneficial to crime prevention when used in the correct way. As a result, the criminal can be apprehended quickly. For instance, in abduction cases a video would be a great way of tracking down a person quickly, and may even prevent a death.

In industrial plants, CCTV equipment may be used to observe parts of the process from a central control room, for example when the environment is not suitable for humans. CCTV systems may operate continuously, or only as required to monitor a particular event. A more advanced form of CCTV utilises digital video recorders (DVRs), providing recordings for many years potentially, with a variety of quality and performance options and extra features, such as motion detection and email alerts. More recently, decentralised IP cameras, some equipped with megapixel sensors, support recording directly to network-attached storage devices, or internal flash for stand-alone operation.

Advances in CCTV Technologies

CCTV surveillance systems have made tremendous technological progress in the last decade, not only in individual capabilities, but also in the ability to interact with other security technology.

Some of the key advances in the domain of CCTV systems are:[2,3,4,5,6,7,8]

- Video content analysis (VCA);
- Automatic number plate recognition (ANPR);
- High definition (HD) CCTV;
- Sophisticated motion detection algorithms;
- Facial recognition;
- Wide dynamic range;
- Internet of Things (IoT);
- Cloud technology;
- Big Data;
- Video management systems (VMS); and
- Wireless technology.

Video content analysis

A key area where CCTV is rapidly developing is that of VCA. This impressive technology is already contributing to the security of a range of high-level facilities, such as city centres, transport facilities, and utilities. The costs of the technology are falling and the capability increasing to the extent that it is becoming a cost effective option for commercial premises.

VCA is the automatic analysis of CCTV images in camera or centrally, utilising advanced algorithms to create useful information about the content. Generally, these systems need a static background and, consequently, tend to operate with fixed cameras or pan, tilt, zoom (PTZ) cameras at set positions, as they are looking to identify changes or movement at a particular

scene. The scope of VCA is considerable and can be used in the detection of intruders, abandoned packages, wrongly parked vehicles or as a means of counting people.

One particular area that VCA can be especially effective is around the perimeter of a site. Securing a perimeter can be seen as one of the most crucial steps in any security plan. An early detection of a threat also means that there is more time and space available to formulate the necessary response, potentially preventing an intrusion alltogether.

Automatic number plate recognition

Using CCTV in conjunction with ANPR software can also be beneficial at large sites, as it allows for the identification of vehicles moving in and out of a site. If an intruder does happen to be successful, this integration can provide the police with valuable information in order to track down the suspect.

HD CCTV

HD CCTV is another area that is expanding across a wide range of video surveillance applications. HD CCTV signifies:

- An unprecedented revolution in the quality of images that can be delivered;
- The ability to more easily identify suspects and make sense of their actions; and
- The potential to improve successful conviction rates on the ground.

HD cameras also open up the possibilities to cover a much wider area without having to use multiple different cameras. Operators of these cameras will also be able to pan, tilt and zoom the camera with the use of a joystick, adding flexibility to the monitoring process. When employed in the right contexts, cameras like these can allow for more widespread coverage and observation in larger areas.

Intelligent video algorithms

Intelligent video algorithms, such as sophisticated motion detection algorithms, can identify unusual walking patterns and alert a guard to watch a particular video screen. Object recognition algorithms can identify someone who might simply be loitering, or even a briefcase or other suspicious object that is left somewhere that it shouldn't be. Again, the system can alert a monitoring guard so that appropriate action can be taken.

The most advanced intelligent video algorithm is facial recognition. However, most experts agree that use of this technology as an efficient tool in the private sector is still several years down the road.

Wide dynamic range

Wide dynamic range is another technology that is becoming a more prevalent feature of CCTV cameras. Wide dynamic range means cameras can provide detail when there's a tremendous amount of both light and dark areas in the same scene. Meanwhile, traditional cameras can't do that.

The Internet of Things

IoT services will allow for combined systems which integrate previously disparate devices into a common management console providing a single pane overview across entire buildings and sites. This includes:

- Video surveillance cameras;
- Smoke detectors;
- Access control panels; and
- Loudspeakers.

In the last few years, IoT has grown rapidly across the world. No longer is the internet confined to computers and mobile devices, it is now available to nearly every device that has an IP address – from microwaves and refrigerators to wearable devices and headphones. IoT systems can be integrated with, and supported by, video to provide information for facility, operational, or business needs. Video analytics, like heat mapping and person counting, can also help businesses gather more business intelligence and strengthen their security.

The result is a huge opportunity for security solutions that are purpose built to share useful data with other connected devices, all of which can be monitored remotely. This connectivity between devices will provide end-users with more complete situational awareness across multiple locations. With the advent of Cloud technology, the notion of connecting any and every device to the internet with an on and off switch became a reality.

Big Data

There still remains a significant challenge to effectively manage and use the endless amounts of video data being generated, so-called Big Data. Big Data is difficult to process through traditional data processing applications. This technology can put structure around vast amounts of unstructured video data, helping better understand significant patterns and trends. In the coming years, look for improvements in, and greater use of, VMS to search Big Data in order to pull up relevant events, people, locations, times, colors and keywords. Such tools will assist business operators to turn Big Data into critical information that supports loss prevention, marketing, operations and customer service.

Wireless technology

Wireless technology has transformed our lives in many ways, from mobile phones, to WiFi connectivity. We have already seen the benefit and convenience of remote security monitoring

via smartphones and tablets. Video surveillance systems of up to ten network cameras can be managed entirely via mobile devices, no longer requiring a desktop PC to run video management software. This significantly lowers the technology hurdle, as users are more open to using a smartphone app than having to overlook a more comprehensive and detailed video management software on a desktop PC, whilst also reducing overall system and maintenance costs.

Information security and CCTV

Today, security safeguards generally fall into one of three categories:[9]

- Physical security;
- Information security; and
- Operational security.

Physical security involves measures undertaken to protect personnel, equipment and property against anticipated threats. It includes both passive and active measures. Passive measures include the effective use of architecture, landscaping and lighting, to achieve improved security by deterring, disrupting, or mitigating potential threats. Active measures include the use of proven systems and technologies designed to deter, detect, report and react against threats. CCTV systems are part of such active measures.

Information security is the process of protecting the confidentiality, integrity and availability of data from accidental or intentional misuse by people inside or outside an organisation or facility. Key elements of information security, include technical security measures/controls, such as:

- Encryption/pseudonymisation;
- Limiting information to authorised entities exclusively;
- Preventing unauthorised changes to, or the corruption of proprietary data;
- Guaranteeing authorised individuals the appropriate access to critical information and systems;

- Ensuring that data is transmitted to, received by or shared with only the intended party; and
- Providing security for ownership of information.

Such measures very much influence the modern CCTV systems, in regards to:

- Protection of unauthorised access to the camera itself, especially IP cameras, to VDR systems, and to video storage systems (especially if cloud technology is used);
- Ecryption of video transmission links between camera and storage system, especially in the instance of IP camera case;
- Encryption or pseudonymisation of retained video material, either on local or cloud storages; and
- Antimalware/end-point protection, on both camera and storage systems.

Operational security is the process of creating policies and procedures, and establishing administrative controls to preserve privileged information regarding organisational capabilities and vulnerabilities. Operation security is of paramount importance in order to create effective CCTV security policies and procedures, and that certainly should be an important part of the overall Information Security Management System (ISMS), established on the basis of the ISO/IEC 27001 international security standard.

Applying advanced information security technologies to CCTV

Cloud-based computing has touched just about every industry and it will continue to reshape the security and surveillance sector, as well. Security can now be offered as a service that is managed remotely, freeing up valuable human and capital resources that no longer need to be on-site at every location which requires monitoring.[7]

Secure remote access to security systems will increase in use, including by end-users who want the convenience and real-time benefits of being able to monitor property and events without

having to be physically present. Such systems must be well protected at the end point (camera), as well as protecting video transmission and video retention system components.

Cloud storage is another important aspect of how systems are becoming more efficient in this model. Much larger volumes of data can be stored cost-effectively and securely at dedicated server facilities, allowing users to archive video and associated data for longer periods of time and improve its accessibility as well.

While the vision of IoT is enticing for the convenience, capabilities and flexibility that vast networks of connected devices offer, there is a growing risk for security threats and breaches as the number of entry points of a network dramatically increases. As a general rule of thumb, as you increase availability and access to any network device, it potentially increases exposure to cyber threats.

As security camera systems become increasingly interconnected with the rise of the Internet of Things, offering benefits such as remote access and third party integration – just as with other network connected devices – it is critical to perform an information security risk assessment and implement security polices in the design and implementation of a network video system. The first step is establishing an understanding and use of industry standard security protocols, including:

- Multi-level user authentication and authorisation;
- Password protection;
- SSL/TLS encryption;
- IEEE Standard 802.1X;
- IP-filtering; and
- Public key infrastructure (PKI) electronic certificate management.

As a network device, a camera, or other connected physical security devices, may pose a risk. If devices, services and applications do not need to interact, users should try to limit connectivity between them. Additionally, segmenting the video system from the core network is a good overall protection measure, thereby reducing risks of video resources and business resources adversely effecting each other.

Recently, surveillance CCTV cameras being used as IoT devices are being used by hackers to gain entry into corporate IT networks. The security industry needs to quickly get a grip on keeping hackers out of devices connected through IoT, by using transport encryption and establishing more secure firewalls and monitoring which alert the security administrators of potential hackers.

CCTV privacy concerns

Many civil liberty campaign groups, academics and consultants, have published research papers into CCTV systems. Challengers of CCTV point out the loss of privacy of people under surveillance and the negative impact of surveillance on civil liberties. Furthermore, they argue that CCTV displaces crime, rather than reducing it.[10]

Proponents of CCTV systems argue that cameras are effective at deterring and solving crime, and the appropriate regulation and legal restrictions on surveillance of public spaces can provide sufficient protections so that an individual's right to privacy can reasonably be weighed against the benefits of surveillance. However, anti-surveillance activists have maintained that there is a right to privacy in public areas.

According to the debate of whether surveillance cameras should be put in public areas, such as schools, stores, libraries, airports, bars and clubs, some individuals feel more secure with

cameras, while other citizens and privacy advocates feel nervous about the idea of someone watching them every time they are out in public.

As the volume and quality of cameras and sensors are increased, cities are turning to more advanced face and object recognition software to make sense of the data; civil liberty activists are concerned about how the technology of CCTV systems could be abused.[10] With cameras in remote cities all connecting to the same database, a person's movements can be tracked across states or continents. For instance, it could be used to single out a person attending multiple political protests.

In the workplace, employers have to deal with two competing interests; employers have a legitimate need and right to watch their employees.[11] At the same time, employees maintain some privacy rights while they are at work. Workplace privacy laws vary by country, but it is very common for video surveillance of restrooms, locker rooms and break areas to be illegal, while surveillance of work areas is permitted.

From a legal perspective, there is a significant difference between a video only camera and a camera that records audio along with video. As such, if your camera is set up to record audio, you will fall under even more legal scrutiny. [11]

CCTV and GDPR

The EU GDPR regulation is designed to strengthen the privacy laws governing the data of EU citizens worldwide. Protecting personal information, including image data which may allow individuals to be personally identified, is a central consideration and it brings CCTV data into the scope of GDPR.[12]

The GDPR is a set of laws designed to protect personal data from commercial abuse and to encourage organisations that retain such data to harden their defences and improve their processes for looking after it. This will significantly increase the importance of control over all types of data, not least because companies that breach any of the GDPR's principles run the risk of massive fines – up to €20 million or 4% of turnover, whichever is higher – as soon as the regulation comes into effect.[13,14]

Some of the key facts about the GDPR include:[12]

- The GDPR applies to all companies worldwide that process personal data of EU citizens.
- The GDPR widens the definition of personal data, bringing new kinds of data under regulation. The GDPR considers any data that can be used to identify an individual as personal data. It includes, for the first time, materials such as genetic, mental, cultural, economic, or social information.
- The GDPR tightens the rules for obtaining valid consent to using personal information. The GDPR requires all organisations collecting personal data to be able to evidence clear and affirmative consent in order to process that data.
- The GDPR introduces mandatory privacy impact assessments (PIAs) to identify privacy breach risks and minimise risks to data subjects.
- The GDPR introduces a common data breach notification requirement which harmonises data breach notification laws in Europe. This is intended to ensure that organisations constantly monitor for breaches of personal data. Organisations need to notify the local data protection authority of a data breach within 72 hours.
- The GDPR introduces the right to be forgotten; organisations are not to hold data for any longer than necessary and are not to change the use of the data from the purpose for which it was originally collected. Data must be deleted at the request of the data subject.
- The GDPR requires that privacy is included in the design of systems and processes. Software development processes must factor in compliance with the principles of data protection. Essentially, all software must be capable of completely erasing data.

- The GDPR allows any European data protection authority to act against organisations, regardless of where in the world the company is based. This enforcement is backed by significant fines for non-compliance.

The key security technologies encompassed by GDPR are:

- Data discovery, cataloguing and classifying;
- Data loss protection;
- Data encryption;
- Email encryption;
- Data breach identification and blocking;
- Pseudonymisation;
- Data portability;
- Mobile device management;
- Perimeter security;
- Cloud storage and sharing services;
- Anti-malware and advanced threat protection – endpoint protection;
- Application security testing;
- Evaluating cloud service providers;
- Identity and access management;
- Behaviour analytics;
- Privileged access management; and
- Format-preserving encryption (FPE).

CCTV and GDPR compliance

As for CCTV in regards to GDPR compliance, businesses and organisations operating CCTV and electronic surveillance systems need to consider:[12]

- Conducting a Privacy Impact Assessment (PIA) to ensure that all CCTV cameras serve a legitimate purpose.

- Allowing CCTV systems to power on/off, where appropriate, so recordings of footage are not continuous. Audio and video need to be independent from each other as well. Legitimate reasons for recording either, or both, need to be clearly established.
- Sound recordings should only be obtained where absolutely necessary, in order to support the legitimate reasons. The use of CCTV surveillance systems should not be regularly placed in the working environment in order to record conversations between the public and employees.
- Recordings from CCTV systems need to be stored securely, whilst access is required to be restricted to authorised personnel.
- CCTV recordings need to be of an appropriate quality to meet the purpose intended.
- Regular checks are needed to ensure that the date and time stamps recorded on images is accurate.
- Recording and playback functions need to provide access to recordings made in specified locations and times, in order to comply with subject access requests from individuals in recordings, or in response to police requests.
- Appropriate policies need to be enforced so that employees know how to respond to requests from individuals or police for access to CCTV recordings.
- Ensuring that the appropriate security safeguards are in place to prevent interception and unauthorised access – the copying of recordings or viewing.
- CCTV recordings that no longer serve a purpose need to be deleted. Clear documentation of the information retention policy, which is clearly understood by CCTV system operators, need to be established.
- The need for signage and the availability of other appropriate information; there is a need to notify individuals of surveillance information processing, such as their presence in an area where CCTV is in operation and their rights of access to recordings and/or images of themselves.

What many organisations often do not realise is that personal data is not just written material, but includes video and audio if this allows individuals to be identified. One area of particular concern is CCTV. Nowadays, there is a constant flow of news articles, highlighting the security flaws that have enabled hundreds of thousands of CCTV systems across the world to be hacked and used in Distributed Denial of Service (DDoS) attacks.[13]

When the GDPR comes into force, management will set out operational processes to help their employees demonstrate compliance. Due to the inherent limitations of traditional CCTV, where data is held on DVRs, these will inevitably restrict general access to the equipment, rather than allowing access to specific data by authorised employees.

One of the solutions is to hold CCTV information securely in the Cloud, with access limited to authorised personnel. There is no longer a physical DVR; data is sent directly and securely from the cameras to the Cloud. Such systems can not only provide an overview of all visual data collected by the CCTV cameras connected to it, but also complete control over access to that data, which is encrypted from end-to-end and can be viewed using a standard computer, tablet or smartphone, via secure browser technology. They can also only record CCTV data when needed and can automatically delete it when it is no longer required.

References

1. http://whatis.techtarget.com/definition/CCTV-closed-circuit-television
2. http://www.in-security.eu/index.php/news/archives/advances-in-cctv-can-offer-peace-of-mind
3. https://en.wikipedia.org/wiki/Closed-circuit_television
4. https://www.facilitiesnet.com/security/article/From-cutting-edge-to-off-the-shelf-Facilities-Management-Security-Feature–2643
5. https://www.ifsecglobal.com/role-cctv-cameras-public-privacy-protection/
6. https://www.facilitiesnet.com/security/topic/How-Can-CCTV-Surveillance-Systems-Improve-Security–19062
7. https://www.ifsecglobal.com/smart-cctv-and-the-internet-of-things-2016-trends-and-predications/
8. https://systemsurveyor.com/iot_survellance/
9. https://www.facilitiesnet.com/security/article/Taking-Security-To-the-Next-Level-Facilities-Management-Security-Feature–2566

10. https://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/index.html
11. https://itstillworks.com/legal-issues-concerning-surveillance-cameras-3333.html
12. https://www.ic2cctv.com/news/cctv-regulation-compliance-surveillance-footage-new-gdpr-information-security-standard/
13. https://gdpr.report/news/2017/04/25/gdpr-key-cctv-cyber-security/
14. http://smallbusiness.co.uk/cctv-system-gdpr-compliant-2541510/