Video Surveillance: Privacy Issues and Legal Compliance

Mahmood Rajpoot, Qasim; Jensen, Christian D.

Published in:
Promoting Social Change and Democracy through Information Technology

Publication date:
2015

Video Surveillance:
Privacy Issues and Legal Compliance

Qasim Mahmood Rajpoot, Christian Damsgaard Jensen
Technical University of Denmark, Denmark

ABSTRACT

Pervasive usage of video surveillance is rapidly increasing in developed countries. Continuous security threats to public safety demand use of such systems. Contemporary video surveillance systems offer advanced functionalities which threaten the privacy of those recorded in the video. There is a need to balance the usage of video surveillance against its negative impact on privacy. This chapter aims to highlight the privacy issues in video surveillance and provides a model to help identify the privacy requirements in a video surveillance system. The authors make a step in the direction of investigating the existing legal infrastructure for ensuring privacy in video surveillance and suggest guidelines in order to help those who want to deploy video surveillance while least compromising the privacy of people and complying with legal infrastructure.

Keywords: Video Monitoring, Privacy, Information Security, Legislation, Data Protection, Data Retention, Storage, Encryption

INTRODUCTION

Use of video surveillance, both by public authorities and the private sector, is spreading fast amid the increasing demand to build infrastructure to protect against harm to people or property. This development has been further accelerated by the decreasing cost of the hardware (Cavallaro, 2007) and the ubiquity of relatively cheap communication infrastructure. Video surveillance is considered a valuable tool to protect people and property from harm. Law enforcement agencies worldwide rely on closed circuit TV (CCTV) systems to help prevent, detect and investigate attacks against public safety. It is also used to detect and investigate attacks against property, e.g. vandalism. The private sector also uses CCTV to protect public safety in the private sphere mostly to protect against intrusions, theft and vandalism. Video surveillance is particularly attractive because it allows people in one location to supervise activities in other locations. This means that law enforcement community can extend the reach of the police forces by having police officers in one location survey the activities of several locations and alert rapid mobile police officers when imminent crime is suspected or detected. This increases the presence of the police force in the community or it allows the same quality of policing with a smaller police force. As the costs of hardware and communication infrastructure has come down, whereas the costs of police officers training management and pays have generally increased, so considerable savings can be achieved through a model with video surveillance and a rapid reaction force. Similar arguments hold for the private sector, where cost reduction and the possibility of outsourcing security services to external companies are important factors in the rapid uptake of video surveillance technologies. As a consequence of these trends, in many developed countries, surveillance cameras are now frequently found in office buildings, shopping malls, housing estates, streets, squares, parks, busses, trains, stations, airports and many other public places, as well as in an increasing number of private companies and homes.

The pervasive use of video cameras in public places captures the activities of people and allows officials to see the daily activities of a target individual. Such pervasive surveillance may impact negatively on the democratic rights of people to freely express their thoughts and to associate freely to share those thoughts. People might not feel comfortable to express their views or to take part in protests against the government policies if they know that they might be identified for such activity later on. Moreover, the output of these surveillance systems may also be abused for other nefarious purposes, such as stalking individuals or used by paparazzi to learn the whereabouts of celebrities.

Contemporary video surveillance systems utilize advanced techniques, such as object-identification and object-tracking, which allows tracking of an individual spanning over multiple cameras distributed throughout a larger area, e.g. an entire city (Moncrieff, Venkatesh, & West, 2009). Compared to contemporary video surveillance solutions, traditional CCTV systems are simple recording systems that have to be constantly monitored by human observers without automated technological assistance. Yet there have been reported incidents, in traditional video surveillance, where the operators were involved in unauthorized collection of data on the activities of individuals. For instance, in a report by BBC News (2005), a group of council employees in the UK spied on a woman's apartment using surveillance cameras installed in that area. Possibilities for such misuse are further increased with the advent of contemporary video surveillance systems that facilitate rapid data retrieval enabled by searching and advanced imaging technology. Such advanced technology in pervasive video surveillance may enable linking the activities of a target individual across multiple video streams.

As criminals and terrorists increasingly make use of new technology to mount attacks on public safety and cause incidents like 9/11 and the Madrid and London bombings, the public and law enforcement agencies must continuously increase their technological capabilities to protect innocent individuals. However, the need for increased security does not mean that privacy has any less importance. Privacy advocates and civil libertarians consider video surveillance a serious threat to the privacy of non-criminals who may be captured by cameras in public places several times a day (Kumagai & Cherry, 2004; Solove, 2002). Employment of video surveillance systems in public areas might cause deterrence, not only for criminals and terrorists, but also for individuals who want to raise concerns against government policies or simply meet with friends or beloved ones without being observed. Regardless of these privacy threats, the importance of video surveillance systems in combating the security threats is considered very important (Buttarelli, 2010), so surveillance systems must be designed and used in ways that protect individuals against crime, without compromising their democratic rights to privacy and freedom against technological measures.

In order to increase the public acceptance of video surveillance systems, it is important that they obey the law of the territory where they are installed and that their deployment strikes a balance between security and the need to protect privacy. The aim of this chapter is to identify the privacy issues and the legal requirements associated with video surveillance systems. The chapter is organized as follows: in the next section, we provide an overview of surveillance and its different types focusing particularly on video surveillance. In Section 3, we identify threats to privacy posed by video surveillance systems and classify the legislation that may apply on video surveillance systems. Section 4 presents a model to help identify privacy requirements. We also provide a taxonomy of video surveillance and suggest a list of guidelines provided by several public and private bodies worldwide, to serve as recommendations for organizations planning to install video surveillance systems while protecting privacy of recorded people and avoiding breaking the law.

BACKGROUND

Surveillance

Surveillance is the act of watching the activities of people, with or without the consent of the people being watched, typically for management or security reasons. The technological development has ensured reduced hardware costs and increased levels of automation, so governments and law enforcement agencies worldwide consider surveillance a cost-effective method for fighting serious threats to public safety.

Surveillance is increasingly used in developed countries and the majority of people are unaware of the magnitude of its occurrence in the form of our images recoded by surveillance cameras in public places, interception of our communication over the internet, or our voices recoded during phone conversations (O'Donnell, 2010). There are several forms of surveillance and a significant amount of work in surveillance has been carried out through biometrics (Lyon, 2008) and 'dataveillance' such as communication monitoring (Marx & Muschert, 2007). Several sociologists have discussed the reasons motivating the high level of surveillance experienced in modern societies along-with its implications. Surveillance is viewed as a key tool of social classification, power and disciplinary control in the modern state (Maguire, 1998). The term Panopticon is often used to indicate the ultimate power offered by massive surveillance (Foucault, 1977; Wood, 2003). The term Panopticon is originally coined by the English philosopher and social theorist Jeremy Bentham in the late 18th century to describe a type of building where a single watchman can observe all people from a central location (Drapper, 2002; Semple, 1993). The Panopticon was promoted as the ideal architecture for a prison, because the fact that prisoners cannot know when they are being watched means that they always have to act as if they are currently under surveillance, thus effectively controlling their own behavior at all times (this is called an 'unequal gaze' by Foucault). The concept of a Panopticon is discussed in detail by Foucault, who observes that the discipline imposed by the Panopticon is ideal for creating 'docile bodies' that comply with the rules of a modern industrial society, i.e. bodies that function in factories, military regiments, and school classrooms. The 'unequal gaze' achieved through the Panopticon causes the internalization of disciplinary individuality, and creates the docile body required of the prisoners. This means one is less likely to break rules or laws if they believe they are being watched, even if they are not. The concept of 'discipline' has been further advanced towards 'control' where surveillance systems are used to methodically control what people can or cannot do (Stalder, 2002; Zureik, 2007).

Surveillance systems can be categorized many ways, but we primarily distinguish between two major types of surveillance systems based on the means using which they are conducted: i) Electronic Surveillance and ii) Non-electronic Surveillance. The former includes computer surveillance, telephone tapping, video surveillance, workplace surveillance and mobile phone surveillance. Non-electronic surveillance, on the other hand, does not involve digital technology but makes use of human-beings such as appointing human operatives on a target and intercepting postal messages. The benefit of electronic surveillance is that it facilitates automation, e.g. by computers, so that mass surveillance can be achieved with relatively few human resources. As we have mentioned earlier, the costs of surveillance technology (hardware and network connectivity) are decreasing, so human resources have become the most costly component of a surveillance system. The automation of surveillance systems therefore allows more people to be monitored at equal costs or an overall reduction of costs in the surveillance system. Another important advantage of reducing the number of humans actively involved in a surveillance system is a significant reduction of insider threats, from abuse of power as mentioned earlier. Therefore, the advent of digital technology has significantly reduced the use of non-electronic surveillance.

It should be noted that although the term ‘surveillance’ will be used extensively throughout this chapter, our particular focus is on video surveillance. We do, however, give a brief overview of computer surveillance and workplace surveillance before we focus on video surveillance and its related issues.

Computer Surveillance

Computer surveillance is the act of monitoring the computer activity, data stored in the computer and the data transmitted over the network. Computer surveillance techniques that focus on the activities and data stored on individual computers are typically referred to as *host-based* techniques, while techniques that primarily monitor the data transmissions and traffic flows on the network are known as *network-based* techniques. Regardless of the techniques that are being used, computer surveillance can be either voluntary and participatory, such as the use of cookies by web-browsers, or involuntary and even surreptitious, such as the use of device fingerprinting techniques (Nikiforakis et al., 2013; Yen, Xie, Yu, Yu, & Abadi, 2012) or the extensive amounts of log data that have been stored by European network providers since the introduction of the European Data Retention Directive (The European Parliament and the Council of the European Union, 2006).

Host-based surveillance techniques normally require software to be installed on the individual host. This software typically monitors activities, e.g. running processes and subsystems, and/or data on the system, e.g. important system files, such as the content of configuration files, system and application log-files, or important data files created by the users. As with the network-based techniques, this software may be installed either by the users or system administrators for explicit monitoring purposes, as is the case with anti-virus software, spam-filtering systems, spy-ware detection systems and other systems installed to detect or prevent the presence of malicious software (aka. malware) on the host computer, or by the different forms of malware mentioned above. Monitoring system activities, such as running processes and sub-systems, normally tells the monitor if the system is performing as expected. This has security applications as exemplified by the monitoring systems mentioned above, but monitors are more often installed to ensure that the performance of applications and sub-systems conform to the service level agreement (SLA) or to predict possible future bottlenecks based on observed trends in the system usage patterns. Malware normally monitors system activities to determine what kind of malware detection systems are present and if possible try to disable them. Monitoring system configuration files and the different log-files created by sub-systems and applications provides complete situational awareness aggregated from correlating notable events registered by each sub-system or application. This is often used to detect evidence of hostile reconnaissance, which often precedes an attack as part of an Advanced Persistent Threat (APT) or a malware infection, but it is more commonly used to debug sub-systems or applications that do not perform as intended. Malware monitors system files to detect and remove evidence of their own presence and it monitors user data files to identify valuable assets, such as trade secrets, credit card information, passwords for other systems, etc. and transfers this information back to its operator through the Internet. Some information stored on the computers may be public in nature, but should still be restricted to a limited set of authorized users. This is particularly true for online social media, such as Facebook, Linked-In, Instagram and Snapchat, which can be analyzed to extract information about a person’s interests, associations, beliefs, plans and activities (Albrechtslund, 2008).

Network-based computer surveillance requires access to the communication infrastructure at some point between the two communicating parties. For example the Communication Assistance for Law Enforcement Act in the United States, authorizes the law enforcement agencies to tap phone conversations and to intercept internet traffic including reading of emails. This act requires the Internet Service Providers to install sniffing technology allowing law enforcement agencies to monitor the internet traffic. As the network traffic is passing beyond the control of the two end-points, unencrypted communication can be eavesdropped upon, and possibly altered, without the knowledge of the

communicating parties. Unencrypted communication, such as standard email and web browsing activities, can be screened for interesting content, typically by programs that look for specific words or phrases, but even if the communication is encrypted, the monitor can still learn who is talking to whom, as well as the time, frequency and extent of the communication, so that human examiners can be alerted for further investigations. The use of such surveillance techniques by the intelligence community have recently received much attention after the revelations of Edward Snowden, a former employee of Booz Allen Hamilton contracted to work for the National Security Agency (NSA). Edward Snowden has leaked documents that shows that the NSA is collaborating with a number of U.S. federal agencies and foreign intelligence agencies to filter Internet traffic passing through these countries (BBC News, 2013; The Guardian, 2013). The implications of such mass surveillance of Internet communication is similar to the effects of video surveillance in public places that we mentioned above, i.e. people are likely to apply self-censorship and refrain from expressing opinions and views that may be considered "dangerous" by the intelligence services. As the work of the intelligence services is necessarily secret, self-censoring citizens must leave a wide margin of error, which severely limits the expression of free speech through the Internet. As with contemporary video surveillance, this mass surveillance capability stems from the automation made possible by computers.

The brief discussion of online social media above highlight a problem with the increasing reliance on cloud services, i.e. computing services provided by external organizations. Many of these services are provided free of charge, or at a very low cost, which entitles the service provider to impose their own conditions on the use of their services. The world's leading search engine, Google, stores search phrases along with identifying information including IP address in a database for up to 9 months (Toubiana & Nissenbaum, 2011). Such identifying information is later partially anonymized by removing the last octet of IP address and is retained for at least further 9 months (CNet, 2008). This allows Google to deliver targeted advertisements relevant to the individual in the context of the search. Moreover, Google's privacy policy states that Google scans the contents of emails exchanged over its email service, Gmail, collects information about their users' internet surfing habits and modifies cookies on their users' computers. This information is primarily collected by Google to profile their users and make their online marketing more effective, but U.S. law enforcement agencies publicly admit to using such data collected from such organizations in order to strengthen the profile of an individual under surveillance. It is common to find laws that authorize security agencies to monitor activities of their people over the internet, in other parts of the world such as the European Data Retention Directive (The European Parliament and the Council of the European Union, 2006).

Workplace Surveillance

Frequent usage of internet and email at work and sophisticated computer technology allow the employers to regularly monitor the actions of their employees, e.g. many corporate firewalls block access to social networks or certain websites, so that employees do not waste time on private activities while they are at work. Moreover, activity logs from enterprise resource planning (ERP) systems, customer relationship management (CRM) systems or Bespoke Case Management Systems (BCMS) provide management with an accurate record of what, where and when their employees work. While these activity logs are typically required to comply with corporate governance legislation, they may also be abused to closely monitor the activities of employees in the workplace. Employers are continuously increasing the monitoring spanning from monitoring of email, web surfing to tapping of office phones to enhance the productivity of the organization. This has become so prevalent that the U.S. government has published a brief discussion of what practices are legal (Beesley, 2012). In many companies where employees are often working away from their main office, it is common to install GPS tracking in the company car, so that the employee can easily call for road side assistance in case of a malfunction and the employer can help track deliveries or recover vehicles that have been stolen. While there are obvious benefits to GPS tracking for both employer and employee, it is also possible to abuse the tracking to measure the performance of their

employees, e.g. for a travelling salesman it is possible to correlate the average length of their visit to a potential customer with the size of their sales to that particular customer thus calculating the efficiency of the salesman. Such *secondary use of data*, i.e. use of data for a purpose different from the one for which it was collected, is generally not allowed, but it is difficult to prevent or detect. According to a survey conducted by American Management Association (2007), more than 75% of US organizations monitor email messages, internet usage, phone calls and computer files of their employees. More than 25% of the fired workers were dismissed for misusing of email while around 33% have been fired for misuse of the Internet. Misuses include violation of company policy, inappropriate content and excessive personal use. There are many genuine reasons for organizations to know what is happening within the organization, however, the employer is expected to remain aware of the employee's right to privacy. In most countries , privacy or data protection legislation, at a minimum, requires that employers obtain consent from the employees by stating how the organization is monitoring them, what information is being collected, the purpose of the information collection and who may review the information. Compliance with this legislation generally also prevents the employer from secondary use as mentioned above. Close monitoring by management may either be seen as a welcome interest in the employees' wellbeing, but it is more often interpreted by employees as a sign of distrust by management, which typically has a negative impact on employee morale. Excessive monitoring will typically not reduce the speed of work, which is easily monitored, but the quality of work, which is often more difficult and costly to monitor, may suffer from the lack of motivation among employees.

Video Surveillance

As stated earlier, this chapter focuses particularly on video surveillance systems, also known as CCTV, its impact on privacy and the relevant legislation in a representative selection of developed countries with respect to privacy. These countries have been selected because video surveillance is widely available in these countries. Video surveillance is a system that employs, normally, a network of cameras to monitor a particular area (public or private) for protection against theft, violence, terrorism or other similar issues. A simple system would allow a watchman to observe what is going on in an area under surveillance while a sophisticated one may include thousands of cameras linked together making use of state-of-art technology to automatically identify and track a particular person from one location to another (Moncrieff et al., 2009).

As mentioned in the beginning of this chapter, the potential benefits of CCTV especially with respect to security are seen as a cost effective mechanism to fight severe threats to public safety. People are monitored in public areas like train stations, buses, stores and ATMs sometimes without even being noticed. There exist more than 4 million cameras in UK alone (Norris, McCahill, & Wood, 2004) - thanks to technological advances in manufacturing, communication and storage capabilities. According to a report from BBC News (2002), it is estimated that an average person in London is caught on camera around 300 times a day. The technology that facilitates the collection of information also poses a great risk of misusing or abusing of the surveillance data, for instance in a report by BBC News (2005) few council workers used CCTV cameras to spy on a woman. In another incident reported by The Guardian (2010), an airport worker at Heathrow Airport was given a police warning for harassment after he allegedly took a photo of a female colleague as she went through a full-body scanner at Heathrow airport. For this reason, massive usage of CCTV in public places is of great concern for civil libertarians and is seen as a threat to privacy by critics (Kumagai & Cherry, 2004), not only for the risk of abuse, but also for the risk of self-censorship in expression and behavior as mentioned earlier.

Existing legislations to protect the privacy of citizens in the context of lawful video surveillance vary greatly among different countries with respect to the different aspects of video surveillance that are being regulated. For example, there are different rules for limiting the storage time of recorded images, the need for notification signs in the surveillance area and the possible requirement of a court warrant in

order to perform surveillance on a particular person. In Section 3, we shall categorize the relevant legislations and provide a summary of legislation, in this regard, for selected countries as mentioned above.

Capabilities of Video Surveillance Systems

Contemporary video surveillance systems that cover most of the public areas are often linked through a communication network. The pervasive form of video surveillance systems combined with the technological advances such as high resolution, magnification, identification and tracking have the potential to disrupt the balance between the need for such systems and the privacy of individuals (Beech et al., 2006).

In contrast to the early age and many currently used CCTV cameras, which can only see as far as a human eye, modern cameras can pan and tilt and can provide a lot more detailed image than previously possible. A camera having 60-times optical zoom lens can read what is written on a cigarette pack at 100 yards (Slobogin, 2002). Furthermore, in a report by New York Times (2004), 400-times magnification cameras have been deployed in Chicago. Improved quality of recordings, reduced storage costs and use of digital technology enable traversing and exploitation of recorded data in ways previously impossible with analog recordings. For example metadata information including date, time, location and information about objects in the recordings make it easier to search for a particular person or activity and may lead to profiling of individuals (Solove, 2002).

Although facial recognition and other remote biometric systems are yet in their infancy, there is a significant investment in this area and the reliability of the identification process is improving (Beech et al., 2006). Advancements in this area can be integrated with CCTV systems to track movement in their field of view or across networked cameras allowing an operator to automatically follow a target object in an entire city in real time or in stored data (Moncrieff et al., 2009). This means that people can be tracked in real time and with little effort, which makes cyber stalking extremely easy for anyone with access to the surveillance system, regardless of whether this access is authorized or not. People participating in political rallies can be followed to their home address as the meeting dissolves and any people visiting celebrities or political dissidents can be followed on camera by paparazzi or law enforcement agents in oppressive regimes.

In contrast, there also exist technologies that can minimize the above-mentioned invasive effects of video surveillance systems on privacy. Digital masking can automatically hide the faces, license plates and other identifying areas in the images of non-targeted people while storing the recorded data (e.g., Chinomi, Nitta, Ito, & Babaguchi, 2008; Senior et al., 2005). Another example of such technology is Google Street View which blurs the license plates of cars and the faces of people in the images. In order to protect unauthorized access to the data, the stored data can also be encrypted, so that only to the individuals who have the relevant decryption key can access the video stream (e.g., Carrillo, Kalva, & Magliveras, 2008; Frederic & Ebrahimi, 2008). Encrypting the video streams in the camera with a key that is only known by authorized users means that the video data is protected from interception both in transit between the camera and the video storage system and when it is stored in that system. If the authorized user loses the decryption key, however, the entire database of video data becomes illegible, which is sometimes addressed through some mechanism based on key-escrow or threshold cryptography. Use of watermarking or logging could also be helpful to track when and where data was accessed, although it cannot prevent access to the recorded data. A digital watermarking scheme embeds a visible but imperceptible watermark in the video stream that identifies either the sender, i.e. the camera, or the intended recipient of the video stream. This means that if the video stream is ever leaked, it will be possible to identify the source of that leak. Watermarking has been extensively studied as part of digital rights management (DRM) systems used by the motion picture industry, but few, if any, systems have

proven to be robust against different types of attacks to remove, overwrite or simply embed a lot of extra watermarks into the video stream thus providing plausible deniability to the person who leaks the data.

PRIVACY & LEGISLATION

Social, legal and technological issues surrounding video surveillance are multifaceted. The previous section discussed the capabilities of advanced video surveillance systems that can allow automatic information extraction and exploiting the system for biometric identification and tracking of individuals. In this section, we discuss and try to cover privacy expectations, the democratic values at stake and the legislation relevant to video surveillance systems.

Though there does not exist a universal definition of privacy, it is often described as how far society can intrude into personal affairs of an individual. A well-known definition of privacy given by Alan Westin (1967), author of "Privacy and Freedom", is: "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others" (p. 7). In many privacy theories it is considered an individual right. For example Thomas Emerson (1970) states that privacy is "based upon premises of individualism, that the society exists to promote the worth and the dignity of the individual. . . . The right of privacy . . . is essentially the right not to participate in the collective life—the right to shut out the community" (p. 545). Critique to such privacy definitions also exist which argue that privacy is an individual right that should trump social interests. For instance, Amitai Etzioni (2008) contends that privacy is "a *societal license* that exempts a category of acts (including thoughts and emotions) from communal, public, and governmental scrutiny" (p. 196).

The boundary between what we reveal and what we do not and control over that boundary, are among the most important attributes of civilization (Nagel, 2002). Many people don't feel comfortable in exposing their behaviors to strangers even if they don't fear disapproval or hostility by the society. In a similar context, another point which is frequently debated is, when you are in a public space such as in a mall or a street, every step you take may be watched by someone anyway so what difference does it make whether you are watched by a person or a camera. The fundamental difference is symmetry. When you are being watched by a person you can watch them back however, when you are being watched but cannot watch them back forms an asymmetrical relationship. Consider a one-sided mirror between an employee and employer's room to understand the situation. Thus the heart of the debate is not the fact that whatever you do may be watched by someone rather the opposite that there may be a particular person who is watching everything you do, facilitated by the automated large-scale video surveillance without much effort and cost (Margalit, 2008).

Advent of technology with its capacity to collect and analyze information about individuals increased interest in the right of privacy. Presently, most of the countries in the world recognize the right of privacy in their legislation. The provisions mostly include rights of sacredness of the home and secrecy of communication, at the least. In some countries, for example the United States, where the right of privacy is not explicitly mentioned in the constitution, the courts have ruled inferring this right from other provisions.

Threats to Privacy

The current and potential capabilities of video surveillance systems are quite attractive for law enforcement officials worldwide and they see video surveillance as an effective mechanism to fight against security threats. Critics, however, argue that being pervasive in nature video surveillance poses a threat to many democratic rights of the non-criminals and it might force the law-abiding people to change their daily routines in order to avoid being caught by the camera. Few privacy awareness

initiatives like Isee project in Manhattan (Institute for Applied Autonomy, 2005) and Observing Surveillance Project in Washigton (Observing Surveillance, 2002) identified locations of CCTV cameras to help people avoid being captured by the cameras.

There are certain constitutionally protected values which are at stake because of extensive video surveillance. First such right at stake is the right of anonymity which is closely related to privacy. Many people expect to remain anonymous in public places such as entering an infertility clinic or a psychiatrist's office. The presence of video cameras in public places would capture all such activities and would allow the officials to see daily activities of any individual. Secondly, the democratic right of people to freely express their thoughts and to associate freely to share those thoughts is in danger. People might not feel comfortable to express their views or to take part in protests against the government policies if they knew they might be identified for this activity later on. Another potential problem of video surveillance system is its discriminatory use by the officials against a particular individual or community based on the ethnic, racial, gender or religious grounds. For instance, Norris & Armstrong (1999a) found in their study about CCTV surveillance in the UK that black people are twice as likely to be a target of surveillance as compared to white people and similarly men are three times more likely to be surveilled than women, not because of their involvement in crime or disorder but simply based on categorical suspicion.

Nothing to Hide, Nothing to Worry About

A typical argument that is often presented in discussions about privacy issues is: "If you have got nothing to hide, you have got nothing to worry about" (Margalit, 2008, p. 425). A similar argument was presented as a slogan by the British government in a campaign to support video surveillance (Rosen, 2005). Frequently encountering such an argument in news interviews and discussions, Daniel Solove (2007, pp. 749-750) states that he decided to ask the readers of his blog to provide their opinions in response to this argument. Some interesting comments he received in response include:

- This is not about hiding something, this is about it being none of other people's business
- I am doing nothing wrong and don't need to justify my position. If you need to investigate my activities, get a warrant to do so
- I don't have anything to hide, but I don't have anything I feel like showing you, either

The reasoning of the argument nothing to hide depends on the fact that privacy is violated only if something illegal or embarrassing is revealed about an individual. Hence the majority of people not involved in such activities has nothing to worry. Rephrasing the argument in a generic manner that *"all law-abiding citizens should have nothing to hide"* reveals that nothing to hide argument is misleading and is based on a wrong assumption that privacy is about hiding wrong-doings. Concealment of bad things is just one aspect of privacy among many other aspects like lack of transparency and accountability and usage of collected data for purposes other than the informed ones. The nothing to hide argument attempts to hide the existence of a problem altogether (Solove, 2011).

Incidents

A potential threat in video surveillance systems is voyeurism – exploitation of video surveillance system by the authorized personnel for targeted collection of data on activities or behaviors of an individual (Norris & Armstrong, 1999b). According to a report by BBC News(2005) a few council workers in Liverpool spied on a woman's apartment using a modern pan-tilt-zoom CCTV street camera. Such misuse can be extended to spy on government officials or celebrities. For example, in another incident which

started a whole new debate about use of CCTV, a security guard used a museum's CCTV camera to spy on the German Chancellor Angela Merkel's private apartment (Cavallaro, 2007).

Despite posing a threat to privacy and dangers of its misuse by the officials, the usefulness of CCTV systems cannot be denied. What is mainly needed is that these systems must be designed in ways that not only protect privacy and freedom while protecting the people against security threats but they must also be able to prevent or detect any abusive usages by using techniques such as logging, encryption and authorization control mechanisms.

Classification of Relevant Legislation

The legislation regarding CCTV varies significantly in Europe as well as the rest of the world (Privacy International, 2007). Some countries, e.g., Canada and Italy, have made regulations regarding usage of CCTV by private and public authorities; others such as France and China have regulations but they apply mainly to private systems, while some countries, for example India, have no particular laws in this regard. CCTV is primarily criticized as a threat to privacy and hence it is mainly regulated in the context of privacy and data protection. There could be several provisions related to CCTV including privacy protection, criminal proceedings, federal & state laws and retention period which need to be consulted for employment of CCTV system in a particular country. Below we classify legislation regarding video surveillance into different categories, in order to serve as a reference point to investigate what relevant provisions are to be considered before deploying or for maintaining CCTV systems in a particular region of the world.

Privacy and Data Protection

Most of the countries recognize the right to privacy. In some countries, for example the United States, where right of privacy is not recognized explicitly in the constitution there exist court rulings which recognize this right implicitly linking it with other provisions in the constitution. Regulations regarding privacy are particularly important in cases where specific regulations on video surveillance are missing in legislation of a country.

Communication Interception

Some countries such as Canada and Denmark have made regulations over communication interception, even by public or law enforcement authorities, and require a court order before intercepting the communication of an individual under surveillance. This court order is usually valid for a limited duration, few days to few months, and the court may renew it depending upon the matter, for example in criminal proceedings which could lead to prison of more than two years, for which an individual is being surveilled. This type of legislation is also particularly relevant if no or limited legislation exists regarding video surveillance.

Exemption for Public Authorities

In some cases where the system is to be operated by the public or law enforcement authorities, there might exist exemptions in the legislation. These exemptions may allow the authorities to perform communication interception or operate video surveillance systems to keep an eye over the activities of the general public or a specific target without any restrictions. For example, in France Police is allowed to remotely access and collect information held on IT systems.

Federal & State Laws

In countries such as the United States that consist of autonomous states/provinces, one needs to consult federal as well as state regulations in the context of video surveillance. For example, few Canadian

provinces have strict regulations and guidelines prepared by the provincial privacy commissioners that are to be followed by the private organizations who wish to deploy video surveillance systems in publicly accessible areas such as shopping malls and super markets.

Regulatory Body

Many countries have a regulatory body (also called regulator, privacy commissioner or data protection authority) to keep oversight of data protection practices being followed by the organizations that need to process personal data of any form whether images captured through video surveillance systems or other data such as medical and biometric data. In such countries, legislation might require registering and/or obtaining prior permission from regulator before employing CCTV system operated by public or private authorities. In Spain, for example, the regulator requires an efficacy study of the system against alternative methods to justify a video surveillance system.

Video Surveillance

The legislation of a country may include laws that apply explicitly to video surveillance systems. The laws could be related to overt video surveillance systems or could cover covert systems as well which are normally used by security agencies or detectives in an investigation. Depending upon the video surveillance system to be deployed, one needs to consult the legislation carefully whether the laws apply to public authorities, private bodies or both. Countries such as Canada and the Netherlands which have explicit regulations regarding video surveillance often also include clauses about followings:

Notification: The requirement that the CCTV system controller must notify the public about the surveillance by displaying meaningful symbols.

Workplace Surveillance: There might exist laws that refrain or restrict the usage of video surveillance systems over workplace to monitor employee performance.

Retention Period: The maximum time-limit for which the personal data or images could be stored.

Privacy Safeguards: The requirements regarding masking, logging, access control and auditing mechanism that limit access to the surveillance data.

Public Access to their Data: The law often requires that there must exist mechanism to allow people to access their images in a reasonable timeframe.

Legislation in Selected Countries

In this section, we summarize the legislation of Canada, the United States and other selected countries in Europe (Banisar & Davies, 1999; Privacy International, 2007, 2010) regarding privacy in video surveillance systems in the light of classification of relevant legislation, described in the previous section. We choose these countries because of two reasons. First, video surveillance is widely available in these countries. Secondly, there is sufficient information available regarding their regulations in English language, from reliable sources. This summary is not supposed to be exhaustive and the law of a country may include further requirements that are to be followed by the organizations who perform video surveillance. But it serves to provide a general idea.

Canada

1	No explicit right of privacy in Charter of Rights and Freedoms, although it

	outlines protection from unreasonable search and seizure which is often considered to be applicable on informational privacy too
2	Communication interception requires court order
3	The federal Personal Information Protection and Electronic Documentation Act (PIPEDA) also applies to video surveillance
4	Regulatory body does exist and has provided certain guidelines both for covert and overt video surveillance performed by public and private sector
5	It is obligatory to inform public about video surveillance via signs
6	The signage should include the purpose of collection of video surveillance and the organization's privacy contact person
7	Video data should be kept only as long as necessary and must be destroyed when no more required

Denmark

1	The right of privacy is recognized in the constitution
2	Communication interception requires court order and the frequency of requests and approval is quite high
3	It is obligatory to inform public about video surveillance via signs
4	In 2007, act on TV surveillance was amended enabling private sector to perform video surveillance on their property which was previously not allowed
5	There exists a regulatory body, however, informing the regulator or taking approval is not required before installing video surveillance systems
6	It is obligatory to inform public about video surveillance via signs
7	Retention period for video data is not clearly stated, however, retention period for other personal information is 12 months

France

1	Privacy right is not explicitly mentioned in the constitution but has been ruled to be implicit
2	Police is allowed to remotely access, record, collect and transfer information held on IT systems
3	Anti-terror act of 2006 authorizes private parties to install CCTV on places open to public and likely to be exposed to risks of aggression or theft
4	Regulatory body exists and authorization from regulatory body is required before installing CCTV systems . However, it has limited powers over activities of government

5	It is obligatory to inform public about video surveillance via signs
6	Retention period for video data is not clearly stated, however, retention period for other personal information is 12 months

Italy

1	No explicit protection of privacy in the constitution, though protections for communication and home are there
2	Pre-emptive communication interception may occur at the discretion of Attorney General
3	Strong regulatory authority exists
4	Video surveillance in public places is permitted only if it is proportionate to the pursuing objectives and should only be activated when other measures are inadequate
5	It is obligatory to inform public about video surveillance via signage
6	Storage of images should be limited in time

Netherlands

1	The right of privacy is recognized in the constitution
2	Communication interception requires court order
3	Video surveillance in public places requires informing the regulator in advance
4	It is obligatory to inform public about video surveillance via signs
5	Video data could be retained for upto four weeks

Norway

1	Constitution does not include a specific privacy clause
2	Communication interception requires judicial warrant, however, bugging conversations of criminals by police is relaxed
3	Regulator operates under ministry of Government Administration but is generally considered independent
4	There is no requirement to inform regulatory body in case of non-recorded video surveillance. However, for recorded video surveillance, the regulatory body has to be informed which has the power to prohibit video surveillance
5	It is obligatory to inform public about video surveillance via signs
6	No data retention law exists

Spain

1	The right of privacy is recognized in the constitution
2	Communication interception does not required court order
3	Video surveillance can only be used when other proportionate methods are not available
4	Video surveillance has to be reported to regulator who will assess its justification
5	It is obligatory to inform public about video surveillance via signs
6	Video data has to be removed after one month

United Kingdom

1	No constitutional right of privacy
2	Communication interception does not require court order rather ministerial approval is enough
3	Surveillance can be done by Police, local authorities or private sector.
4	Regulator has been granted greater powers and fining capacities
5	It is obligatory to inform public about video surveillance via signs
6	Video data could be retained for two years
7	Although CCTV code of practices exist but they have no legal binding

United States

1	No right to privacy in constitution, though court has ruled linking it with other provisions
2	Data Privacy Act protects records held by public authorities, but no comprehensive data protection law for private sector exists
3	Federal Trade Commission issued self-regulating privacy guidelines, however, it has no authority to enforce privacy rights
4	No federal law regarding video surveillance exists. Video surveillance laws in different states vary, for example, in New York video surveillance can only be conducted by the police while in Arizona one can use video surveillance at a public place without posting a notice to inform public
5	No data retention law exists

MODEL & TAXONOMY OF VIDEO SURVEILLANCE

In this section, we attempt to formulate a model from our study of cases, issues and legal requirements. We present a model and taxonomy of video surveillance as a method to facilitate identifying the privacy

requirements and problem areas in a video surveillance system. We start with a discussion of model and discuss taxonomy later in this section.

The model in Figure 1 presents an abstract model of video surveillance as a method to identify the privacy requirements in a video surveillance system. Fundamentally, a video surveillance system must include elements to capture video, to store/record video and to display video to the users, as well as a mechanism to transport video data between these elements. Figure 1(a) shows the main elements of our model, which includes four components, namely: video capture, -transport, -monitoring, and -storage. The video capture component includes the cameras, their local infrastructure, and the area which can be captured by the cameras. Once the data is captured, it needs to be securely transported; this is typically done over the internet, so we have included this as a component in our model. The monitoring component includes the different elements that are necessary to allow somebody to watch the video. The monitoring component must consider all security and privacy concerns that arise when the captured data (live or stored) is watched by the observers. Finally, the storage component is responsible for securely storing the data and restricting the access of stored data to the authorized individuals only.

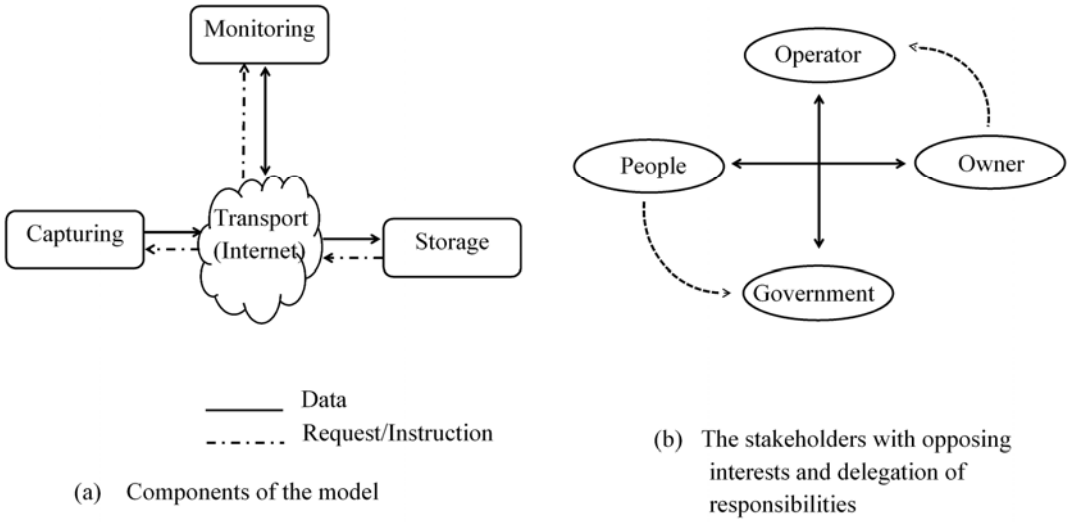

Figure 1: Video Surveillance Model

The four components identified in Figure 1(a), allow us to identify the scope for the privacy requirements that may arise in video surveillance systems. We do, however, also need to consider the different stakeholders and interests in order to identify such requirements. There are two principal stakeholders in a video surveillance systems, the owner, who commissions and is responsible for the system, and the people who are being watched by the system; these are shown as principal opposing forces in Figure 1(b). In practice, however, normally owners do not operate the video surveillance systems themselves, but instead delegate this task to another organization, e.g. a guard company; this organization is referred as operator. Similarly, most people are unable to determine whether video surveillance is fair and warranted or excessive, so it is typically an elected government which regulates video surveillance through legislation and guidelines. This means that, in practice, the video surveillance operator and the government become the real opposing forces in a video surveillance system.

People are the core of our model, because they may have certain expectations from each component of the video surveillance system, whereas the other entities strive to live up to the expectations of the people. It is the combined responsibility of the owner and the operator to ensure the privacy of the people. Privacy

of people should be protected both from outside attackers and the personnel within the owner and operator organizations. The operator is responsible for performing his duties while being least intrusive as far as the privacy of people is concerned.

Based on our model that considers the different components of the video surveillance system, the perspective of the stakeholders involved and the conventional privacy requirements, we describe below the identified privacy requirements in a video surveillance system.

Consent and Signage: Consent of the people who can potentially be recorded by the video surveillance system needs to be taken in advance, either explicitly or implicitly. One way to take consent is by informing the people about video surveillance through *signage* i.e. displaying clear and visible symbols in the area where video surveillance takes place

Anonymity, Data Hiding and Privacy Safeguards: While the system is supposed to monitor the behavior of the people, it should strive to maintain the *anonymity* of the people by hiding their identity using certain *privacy safeguarding mechanisms*. Therefore the system must implement *data hiding* techniques which obfuscate the identity-revealing regions in the images when the operators monitor video streams in a normal situation. In order to hide the identity of observed people, identity revealing sensitive areas are first determined and then removed or de-identified depending upon the approach used. Several types of techniques to hide privacy-sensitive areas have been proposed. A simple technique is to fully remove the sensitive regions but this not only hides the identity but in some cases also the behavior (e.g., Criminisi, Perez, & Toyama, 2003, 2004; Tang, Ying, Wang, & Ping, 2004). Another type of approach is to reduce the level of detail of privacy-sensitive areas, with the help of blurring or pixilation, leaving the subject unidentifiable yet the behavior remains recognizable (e.g., Schiff, Meingast, Mulligan, Sastry, & Goldberg, 2009; Saini, Atrey, Mehrotra, & Kankanhalli, 2013; Yu et al. 2008). The third approach, called abstraction, is to remove the sensitive regions and replace them with dummy objects such as silhouettes or skeletons. Some of the key works in this area are proposed by (Haritaoglu, Harwood, & Davis, 2000; Koshimizu, Toriyama, & Babaguchi, 2006; Senior, Pankanti, Hampapur, Brown, Tian, & Ekin, 2003). Yet another technique proposed in literature, called scrambling, is to encrypt the sensitive regions with a key allowing the area to be decrypted only by authorized personnel possessing the key, see for instance (Boult, 2005; Carrillo et al., 2008; Dufaux & Ebrahimi, 2006). As compared to other techniques, this approach offers the benefit of perfectly reconstructing the original image.

Video properties: The owner needs to determine whether cameras with advanced functionalities such as pan-tilt-zoom, night-vision and high-resolution are really required to be used, with respect to the purpose of the surveillance conducted.

Deletion after retention period: Depending upon the regulations of the region where video surveillance takes place, the captured data must be automatically deleted as soon as the retention period expires.

Voyeurism protection: In order to restrict voyeurism, advanced functionalities such as searching, identifying and tracking an individual are only to be made available when an operator explicitly places such a request to the system. While granting these privileges the system logs the request along with the information about the circumstances in which such a request is granted.

Public access to their data: People should be able to get access to the images containing them, through a pre-define procedure. Certain countries, for example Canada and France, legally bind the surveillance operator to allow individuals to watch their own images captured by the surveillance system.

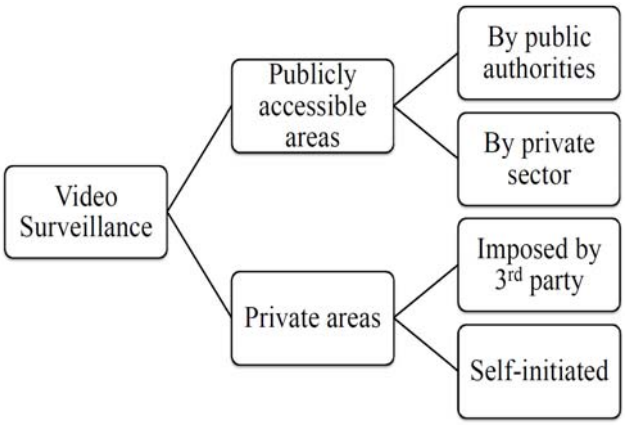

Figure 2: Taxonomy of Video Surveillance System

The points indicated in the model may not be applicable altogether in all areas where video surveillance takes place (Margalit, 2008). Consider example of an educational institute which typically has several areas such as classrooms, offices, research labs, cafeteria, lawns, dormitories, etc. Without question, in different areas people have different expectations of privacy, which must be taken into consideration while deploying video surveillance, hence the requirements would vary in these areas. In this context, we offer a taxonomy of video surveillance as a hierarchical structure in Figure 2. We classify video surveillance into two major types: i) Video surveillance in publicly accessible areas, and ii) Video surveillance in private areas. Publicly accessible areas such as streets, transport, shopping malls, supermarkets, restaurants, etc. are accessible to anyone. On the other hand, private areas are accessible to a limited number of people whose identity may already be known. Video surveillance in publicly accessible areas can be performed either by public authorities (e.g. law enforcement authority) or by private sector (e.g. owner of a supermarket) and each has to follow the relevant laws. Video surveillance in private areas can also be categorized into two subcategories: i) imposed by third party, and ii) initiated themselves. In the former, the video surveillance is initiated by a third party with/without consent of the people under surveillance, example includes workplace surveillance; while in the latter category, it is initiated by the people under surveillance themselves and example includes use of video surveillance in one's own home.

RECOMMENDATIONS

Many public and private organizations have provided certain guidelines regarding deployment and maintenance of the video surveillance systems. Some focus only on public sector and law enforcement agencies, e.g, guidelines given by Beech et al. (2006), while others target both public and private organizations which are using video surveillance systems, e.g., (Buttarelli, 2010). Whether these guidelines are legally binding or not depends on the fact whether they have been provided by a private organization or a public authority, for example, there exist certain guidelines in Canada regarding video surveillance which are provided by the Privacy Commissioner of Canada and hence are legally binding. Here we combine the guidelines for employing video surveillance, provided by European Data Protection Supervisor (Buttarelli, 2010), Privacy Commissioner of Canada (2008), and Constitution Project (Beech et al., 2006) – a non-government organization in USA. These recommendations, albeit not guarantee to avoid breach of law, ensure that the impact of video surveillance on privacy is minimized and therefore may help achieving the compliance with the privacy legislation in a particular country.

1. Establish a lawful reason for conducting video surveillance and use video surveillance only for that purpose

2. Determine whether a less privacy-invasive alternative to video surveillance would meet the requirements
3. Perform the cost-benefit analysis, comparing the alternative means of addressing the stated purpose of the system
4. Build privacy into the system design and address data protection issues on early stage
5. Assess the impact of system on privacy and freedom of individuals
6. Consult the regulatory authority – if any – and other stakeholders of the system, for example employee representative in case of workplace monitoring
7. Determine whether live monitoring without recording is enough, otherwise, store the recorded images securely and destroy them after a specified time (one week in most of the cases)
8. Provide public notices about the surveillance
9. Devise a mechanism to give individuals access to data about them
10. Create technological and administrative safeguards to reduce the possibility of misuse and abuse of the system
11. Provide training to the system operators and educate them on obligation to protect the privacy of individuals
12. Maintain a secure log in order to keep track of the activities performed by the system operators

CONCLUSION

Video surveillance system is generally considered a powerful tool for fighting crime and protect people and property from harm. The combined use of video surveillance with a rapid reaction police force, extends the reach of the police and allows better policing at a reduced cost. The benefits to security, however come at a cost of intrusion of privacy of the citizens that the video surveillance systems are installed to protect. Many civil activists consider the installation of video surveillance systems in public places in conflict with Article 12 of the United Nation's Universal Declaration of Human Rights, which states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Moreover, the constant surveillance often results in changed behavior and self-censorship by the people being monitored, which touches on important freedom rights, such as free speech and the right to assemble. It is therefore important that the deployment of video surveillance systems strikes a balance between security and privacy.

The legal and social implications of video surveillance system are quite extensive and it is important that the use of video surveillance is both lawful and acceptable in the community where it is deployed. Some countries have specific laws and regulations that govern the use of video surveillance, but in many cases such laws have to be weighed against fundamental right and there has to be proportionality between the loss of privacy and the threats that the system is installed to prevent. In order to avoid breaking the law of the territory where the video surveillance system is installed, a thorough study must be carried out to identify all the legal requirements for video surveillance and seeking advice from legal experts is generally recommended. When deploying a video surveillance system, the system must be built in a way that considers the legal requirements identified in this study and mechanisms to detect misuse or abuse of the system should be built right into the system design. Moreover, the people operating the system must be provided adequate training and they should be educated

about privacy issues. This training and education should be accompanied by some form of *non-disclosure agreement* which must prohibit the propagation of anything learned from the video surveillance system to unauthorized outsiders, similar to the secrecy of correspondence. Finally, an independent regulatory authority could play a vital role in making these systems trustworthy by the people and minimizing the big brother feelings in a society where video surveillance is used.

REFERENCES

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, 13(3). Retrieved 14th October, 2014, from http://www.uic.edu/htbin/cgiwrap/bin/ojs/ index.php/fm/article/view/2142/1949.

American Management Association (2007). *Electronic Monitoring & Surveillance Survey.* Retrieved 14th October, 2014, from http://www.plattgroupllc.com /jun08/ 2007ElectronicMonitoringSurveillanceSurvey.pdf.

Banisar, D. & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *Journal of Computer & Information Law,* 18(1), 3–111.

BBC News (2005), *CCTV staff 'spied on naked woman'*. Retrieved 14th October, 2014, from http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/4503244.stm.

BBC News. (2002). *CCTV: Does it work?*. Retrieved 14th October, 2014, from http://news.bbc.co.uk/1/hi/uk/2071496.stm.

BBC News. (2013). *Edward Snowden: Timeline*. Retrieved 14th October, 2014, from http://www.bbc.com/news/world-us-canada-23768248.

Beech, T., Dyer, K., Franklin, S., Messinger, I., Onek, J., & Sloan, V. (2006). *Guidelines for public video surveillance: A guide to protecting communities and preserving civil liberties.* Retrieved 14th October, 2014, from http://www.constitutionproject.org/pdf/video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf.

Beesley, C. (2012). Email, Phone and Social Media Monitoring in the Workplace – Know Your Rights as an Employer. *The US Small Business Administration*. Retrieved 14th October, 2014, from https://www.sba.gov/blogs/email-phone-and-social-media-monitoring-workplace-know-your-rights-employer.

Boult, T. E. (2005). Pico: Privacy through Invertible Cryptographic Obscuration. In Jaynes, C. & Collins, R. (Eds.) *IEEE Computer Vision for Interactive and Intelligent Environment* (pp. 27–38). IEEE.

Buttarelli, G. (2010). *The EDPS video surveillance guidelines*. Retrieved 14th October, 2014, from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

Carrillo, P., Kalva, H., & Magliveras, S. (2008). Compression Independent Object Encryption for Ensuring Privacy in Video Surveillance. In Ostermann, J. (Ed.) *IEEE International Conference on Multimedia and Expo*. (pp. 273–276) IEEE.

Cavallaro, A. (2007). Privacy in video surveillance. *IEEE Signal Processing Magazine*, 24(2), 166–168.

Chinomi, K., Nitta, N., Ito Y., & Babaguchi N. (2008) PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstraction. In Satoh, S., Nack, F., & Etoh, M. (Eds.) *International Multimedia Modeling Conference* (pp. 144–154). Springer.

CNet. (2008). *Debunking Google's log anonymization propaganda*. Retrieved 14th October, 2014, from http://www.cnet.com/news/debunking-googles-log-anonymization-propaganda/.

Criminisi, A., Perez, P., & Toyama, K. (2003). Object Removal by Exemplar-Based Inpainting. In Dyer ,C. & Perona, P. (Eds.). *IEEE Computer Visioin and Pattern Recognition*. (pp. 721−728). IEEE.

Criminisi, A., Pérez, P., & Toyama, K. (2004). Region Filling and Object Removal by Exemplar-Based Image Inpainting. *IEEE Transactions on Image Processing*, 13(9), 1200–1212.

Drapper, T. (2002). An Introduction to Jeremy Bentham's Theory of Punishment. *Journal of Bentham*

Studies, 5(1), 1–17.

Dufaux, F., & Ebrahimi, T.: Scrambling for Video Surveillance with Privacy. (2006). In Jaynes, C. & Welch, G. (Eds.). *IEEE Conference on Computer Vision and Pattern Recognition Workshop* (pp. 160–166). IEEE.

Emerson, T.I. (1970) *The system of freedom of expression*. New York: Random House.

Etzioni, A., (2008) *The limits of privacy*. New York: Basic Books.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. London: Random House LLC.

Frederic, D. & Ebrahimi, T. (2008). Scrambling for Privacy Protection in Video Surveillance Systems. *IEEE Transactions on Circuits and Systems for Video Technology,* 18(8), 1168–1174.

Haritaoglu, I., Harwood, D., & Davis, L. S. (2000). Real-Time Surveillance of People and their Activities. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 22(8), 809–830.

Institute of Applied Autonomy (2005). *i-SEE 'Now more than ever'*. Retrieved 14th October, 2014, from http://www.appliedautonomy.com/isee.html.

Koshimizu, T., Toriyama T., & Babaguchi N. (2006). Factors on the Sense of Privacy in Video Surveillance. In Mase, K. (Ed.) *ACM Workshop on Continuous Archival and Retrieval of Personal Experiences* (pp. 35–44). ACM.

Kumagai, J., & Cherry, S. (2004). Sensors and sensibility. *IEEE Spectrum,* 41(7), 22–26.

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, 22(9), 499−508.

Maguire, M. (1998). Restraining big brother? The regulation of surveillance in England and Wales. In C. Norris, J. Moran & G. Armstrong (Eds.), *Surveillance, Closed Circuit Television and Social Control* (pp. 229-240). Aldershot: Ashgate Publishing Ltd.

Margalit, E. (2008) The case of the camera in the kitchen: Surveillance, privacy, sanctions, and governance. *Regulation & Governance*, 2(4), 425–444.

Marx, G., & Muschert, G., (2007) Personal information, borders, and the new surveillance studies. *Annual Review of Law and Social Science,* 3(1), 375–395.

Moncrieff, S., Venkatesh, S., & West, G. A. (2009). Dynamic privacy in public surveillance. *Computer*, 42(9), 22–28.

Nagel, T. (2002). *Concealment and exposure: and other essays*. Cambridge, MA: Oxford University Press.

New York Times (2004). *Chicago moving to 'smart' surveillance cameras*. Retrieved 14th October, 2014, from http://www.nytimes.com/2004/09/21/national/21cameras.html.

Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. (2013). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In Sommer, R. (Ed.). *IEEE Symposium on Security and Privacy* (pp. 541–555). IEEE.

Norris, C., & Armstrong, G. (1999a). CCTV and the social structuring of surveillance. In Painter, K. & Tilley, N. (Eds.). *Surveillance of public space: CCTV, street lighting and crime prevention*. New York: Criminal Justice Press.

Norris, C., & Armstrong, G. (1999b). *The maximum surveillance society: The rise of CCTV*. Oxford: Berg Publishers.

Norris, C., McCahill, M., & Wood, D. (2004). The growth of CCTV: A global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance and Society*, 2(2), 110–135.

O'Donnell, A. (2010). *Who is watching you, and why?*. PhD dissertation, University of Exeter, UK.

Observing Surveillance (2002). *Observing surveillance project in Washington.* Retrieved 14th October, 2014, from http://observingsurveillance.org/.

Privacy Commissioner of Canada (2008). *Guidelines for Overt Video Surveillance in Private Sector*. Retrieved 14th October, 2014, from https://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp.

Privacy International. (2007). *Surveillance Monitor 2007 – International Country*

Rankings. Retrieved 14th October, 2014, from https://www.privacyinternational.org/reports/ surveillance-monitor-2007-international-country-rankings.

Privacy International. (2010). *European Privacy and Human Rights.* Retrieved 14th October, 2014, from https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf.

Rosen, J. (2005). *The naked crowd: Reclaiming security and freedom in an anxious age.* New York: Random House.

Saini, M. K., Atrey, P. K., Mehrotra, S., & Kankanhalli, M. S. (2013). Privacy Aware Publication of Surveillance Video. *International Journal of Trust Management in Computing and Communications*, 1(1), 23–51.

Schiff, J., Meingast, M., Mulligan, D. K., Sastry, S., & Goldberg, K. (2009). Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In: Senior, A. (Ed.) *Protecting Privacy in Video Surveillance*. (pp. 65–89). Springer.

Semple, J. (1993). *Bentham's Prison: A Study of the Panopticon Penitentiary*. New York: Oxford University Press.

Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., & Ekin, A. (2003). Blinkering Surveillance: Enabling Video Privacy through Computer Vision. *IBM Technical Paper, RC22886 (W0308-109)* Retrieved 14th October, 2014, from http://www-ee.ccny.cuny.edu/wwwn/yltian/Publications/rc22886.pdf

Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., Ekin, A., … Lu, M. (2005). Enabling Video Privacy Through Computer Vision. *IEEE Security & Privacy*, 3(3), 50–57.

Slobogin, C. (2002). Public privacy: camera surveillance of public places and the right to anonymity. *Mississippi Law Journal*, 72(1), 213−233.

Solove, D. J. (2002) Digital dossiers and the dissipation of fourth amendment privacy, *Southern California Law Review*, 75(1), 1083−1169.

Solove, D. J. (2007) I have got nothing to hide, and other misunderstandings of privacy. *San Diego Law Review*, 44(1), 745−772.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press.

Stalder, F. (2002). Privacy is not the antidote to surveillance. *Surveillance and Society*, 1(1), 120–124.

Tang, F., Ying, Y., Wang, J., & Ping, Q. (2004). A novel texture synthesis based algorithm for object removal in photographs. In: Maher, M. J. (Ed.), *Asian Computing Science Conference* (pp. 248–258). Springer.

The European Parliament and the Council of the European Union (2006). *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006*. Retrieved 14th October, 2014, from http://www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/national-security/directive-2006-24-ec.

The Guardian. (2010). *Airport worker given police warning for 'misusing' body scanner*. Retrieved 14th October, 2014, from http://www.theguardian.com/uk/2010/mar/24/airport-worker-warned-body-scanner.

The Guardian. (2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* Retrieved 14th October, 2014, from http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Toubiana, V., & Nissenbaum, H. (2011). An Analysis of Google Logs Retention Policies. *Journal of Privacy and Confidentiality*, 3(1), 3−26.

Westin, A. (1967) *Privacy and freedom*. New York: Athenum.

Wood, D. (2003). Editorial: Foucault and Panopticism revisited. *Surveillance and Society,* 1(3), 234–239.

Yen, T. F., Xie, Y., Yu, F., Yu, R. P., & Abadi, M. (2012). *Host Fingerprinting and Tracking on the Web: Privacy and Security Implications*. Paper presented at Network and Distributed System Security Symposium, San Diego, CA.

Yu, X., Chinomi, K., Koshimizu, T., Nitta, N., Ito, Y., & Babaguchi, N. (2008). Privacy Protecting Visual Processing for Secure Video Surveillance. In Chellappa, R. & Girod, B. (Eds.). *IEEE International Conference on Image Processing* (pp. 1672–1675). IEEE.

Zureik, E. (2007). Surveillance studies: From metaphors to regulation to subjectivity. *Contemporary Sociology: A Journal of Reviews,* 36(2), 112–115.

KEY TERMS AND DEFINITIONS

Video Monitoring: The act of visually observing a place or the activities of people

Information Security: Protection of information against unauthorized access

Regulation: An order, rule or law prescribed by an authority

Data Retention: A collection of stored data

Data Protection: Safeguarding mechanism to protect the stored data

Encryption: The act of scrambling data which can be unscrambled only if a required piece of information is available

Communication Interception: Stealthily monitoring the data when it is in transit from one point to another

Regulatory Body: Authority that supervises data protection practices