International Journal of Information Technology and Language Studies (IJITLS)

Public Views: How to Make CCTV Surveillance Systems Satisfy Security and Privacy Concerns?

Lubna Mahmoud Abu Zohair
Lubna.abuzohair@gmail.com

The British University in Dubai, Dubai, UAE

Abstract. The significant need for the existence of camera surveillance systems has emerged these days. Despite the existence of privacy concerns, the aim was to address them and have these systems satisfying security and privacy concerns. Qualitative research was conducted and interviews approach were followed to gather public visions for the needed CCTV systems' characteristics that achieve the aim of this research and different ideas were proposed. None of the previous researches tackled this area of study by listening to public concerns or extract the needed CCTV systems features from their visions, and that what made this research distinct from others. The implication of this study will open the gate for researchers to work on the proposed ideas toward achieving video surveillance systems that are more friendly and acceptable by the public.

Keywords: Security, Privacy, CCTV, Surveillance, Closed Circuit Television, Video Surveillance, Features, Concerns, Qualitative Research, Interviews.

1. Introduction

With the light speed emergent of security and safety needs, the prevalence of Closed Circuit Television (CCTV) surveillance systems become a crucial need for any country worldwide. Closed Circuit Television system is defined as the use of cameras to capture photos or video signal and transmit it to a certain system or systems (Dempsey, 2007). People's everyday life behavior or acts, locations, relations, modes, belongings and more are being captured to achieve, as apparent reasons, their reassurance and peaceful city. However, the way that its handled or used, processed, stored, or exchanged made the protection of personal privacy rights more complex and difficult to be maintained. Privacy right has been defined earlier in 1967, by Westin, who provided two widely cited definitions, which are: " the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others", and "the voluntary and temporary withdrawal of a person from general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups in a condition of anonymity or reserve" (Boguslaw & Westin, 1968).

1.1. Problem Statement

There are still great debates regarding which one should be taken part at the expense of the other, the citizens' right of privacy or their safety (O'Mahony, 2014)(Friedewald & Pohoryles, 2016), rather, rare contributions in how to make such CCTV systems act as privacy protection and security assurance tools altogether and at the same time. However, that balance and requirements is not achieved yet, as what was noted in UAE security and planning manual for the vision of 2030 in (Abu Dhabi Urban Planning Council, n.d.). Furthermore, their 2030s visions is to find that balance between the need for the surveillance with the need for privacy. So, the main aim of this qualitative research will be to explore or develop ideas and visionary thoughts about the required surveillance systems features that can narrow the privacy concerns of the public and help them coexist with such systems existence. That will never be better expressed and studied with anything rather than the elements who are in daily exposure to it, i.e. the public. This research study will target the public of United Arab Emirates (UAE). The main contribution of the outcome of this research is to help public coexist with the existence of CCTV system, and that will be achieved by hearing what public wants and applying their suggested ways in narrowing their security

concerns and implementing the needed privacy protection solutions required in order to accept and live with the fact of its existence.

1.2. Research Question

On the ground or basis of the research dilemma, this study sought to answer the following question: How to make CCTV surveillance systems satisfies security and privacy concerns? To address that main question, this research should endeavor to answer the bellow sub-questions:

1.2.1. How serious is the pervasiveness of the surveillance system? (To reflect how important is the need for a solution to coexist with its existence)

1.2.2. What are the security vital and important roles provided by CCTV systems? (To understand the importance of the presence of such systems)

1.2.3. What are the privacy concerns caused by the existence of such systems? (To point out to the concerns that make people refuse to be surveilled)

1.2.4. What are the CCTV systems' characteristics or features that can satisfy security and privacy concerns simultaneously? (The assessment of the aforementioned question will facilitate finding answers to this question)

The structure of this paper is outlined in the following manner: Section two illustrates narrative literature review related to the research main theoretical frameworks, i.e. Security roles, ways for privacy protection, and visionary needed features to allow CCTV support and provide security and privacy protection at the same time. Section three will define and detail the followed research methodology. Then the results, limitations, and future work will be presented in section four. Last, the conclusion section will conclude the research.

2. Narrative Literature Review

A systematic literature review was applied by gathering related research topic information from different databases using the following main key terms: Privacy, CCTV, Security, Video Surveillance, Closed Circuit Television. Different Simulations, Interviews, Case Studies, or Literature were screened and the inclusion and exclusion criteria were mainly based on how that literature far or near from the research main question. Selected ones were used as a source to feed this literature. Literature was combined and presented using a thematic approach. The main themes included in this study were: the pervasiveness of CCTV systems, its need for security, and last, pointing to an available solution for privacy protection. The chosen papers were illustrating practices and research studies international-wise, mainly: UK, US, Australia, and China. Rare studies tackled the dilemma on how to make CCTV systems accepted from security and privacy point of views, and none researches were targeting the public, who are the most exposed item to such systems, to know what they want and their visionary or imaginary thoughts on how to make such systems clear the security and privacy concerns at the same time to help civic coexist with their presence.

2.1. CCTV Cameras Locations

Recently, the presence of surveillance cameras has become significant in most part of our daily lives. It is observable everywhere, in private homes, residential and commercial buildings, metros and buses, streets and districts, companies and offices, government sectors, industrial zones, airports & planes, shops and malls, hotels, nurseries, schools and universities, and many other places (Graham, Brooks, & Heery, 1996) (Mahmood Rajpoot & Jensen, 2015). This spread called for researchers to study more about the positive and negative consequences of such solutions, most importantly the importance of its existence, its privacy threats and penetrations, and workarounds in making surveillance cameras do its role in security while maintaining human rights of privacy at the same time.

2.2. CCTV Security Roles

Different kinds of literature illustrated successful use of case scenarios and studies for the use of CCTV systems as a major security and safety tool. Starting with its usage in traffic and roads safety, in (Conche & Tight, 2006) cameras were utilized in determining the reasons for car accidents. Whereas, UK related studies, (Wilson & Sutton, 2003) explained how CCTV systems used by governments to prevent crime in public places, (Welsh & Farrington, 2002) added to that its importance in hindering cars and motorbikes theft and property crimes, and (Park, Oh, & Paek, 2012) tot in that property crimes deterrence. Additionally, researchers in (Pointing, Hayes-Jonkers, Bohanna, & Clough, 2012) shed the light on how a monitoring tool was used efficiently to restrain assaults violations caused by alcoholics' drinkers,

especially late nights, in Australia. Moreover, Taylor explained the need for CCTV adoption for crime controls at schools for crime control purposes and how it's been tolerated for massive monitoring of attitudes and activities such as students' absence, bullying, and smoking, or for evaluating teacher performance (Taylor, 2013). Last but not least, in western countries, and in the middle east, surveillance cameras were useful in aiding the cases related to terrorisms attacks that were created by extremist groups or personals and enabled successful prosecutions (Maghal, 2016).

2.3. CCTV Privacy Concerns

Many researchers demonstrated privacy violations and threats caused by the CCTV systems. BBC reported ways of abusing CCTV collected information by council workers who used street CCTV pan-till-zoom camera to snoop in a woman in her flat (Cavailaro, 2007), and another incident noted there about security guards who used museum's cameras to spy in a woman in her apartment. (Kalva, Carrillo, & Magliveras, 2009) and (Babaguchi, Koshimizu, Umata, & Toriyama, 2009) stated that disclosing or conducting recorded video analytics in order to identify personals or groups to solve certain issues or cases put human privacy in jeopardies. In (Piatrik, Fernandez, & Izquierdo, 2012), Tomas et al. explained that decision errors in CCTV data analytics could lead to addressing the wrong person and, besides, identity theft and continuance tracking of people behaviors could disclose private personal features and thus posing individuals' privacy and data protection risks. Yupeng et al. in (Zhang, Lu, Nagahara, & Taniguchi, 2014) mentioned that the fact that anyone within the cameras viewing angle could be captured or recorded by CCTV systems caused personal privacy vulnerability and threat, where such data could be used and shared in unauthorized manners and scenarios.

2.4. CCTV Privacy Protection Workarounds

Maintaining privacy while surveilling for safety and security is a big challenge. However, and since the face is the important human features that can be used to identify their identities and be used to threaten privacy, techniques to blur, pixelization, encryption, and masking were proposed in (Boult, 2005) to hide individuals' that feature. Also, distorting the corresponding pixels of the face or replacing it with other shapes, like what is presented in (Korshunov & Ebrahimi, 2013)of replacing faces with colored eclipse to prevent face recognition. Another easy, reversible (undoing the facial hiding) and secure approach were introduced in (Korshunov & Ebrahimi, 2013) that works on warping human's facial geometrical characteristics in order to preserve their privacy. Access control frameworks is implemented and illustrated by (Kerr & Van Schyndel, 2014) to allow law enforcement to control access to surveillance data to enhance its protection. Regulations guidelines that have been suggested in (Piatrik et al., 2012) also could participate in privacy protections while using CCTV systems, among them, to limit the scope and viewing angle of public surveillance systems, rules related to lower the storage period of recorded data, make the individual facial characteristics obscure in a way that it can be identified only when needed, and last to avoid linking personal identities documents with recognized individuals.

3. Research Methodology

To extract a variety of themes related to the research question concepts, the interview was adopted as a methodology for this research study. The usefulness of such an approach, as explained in (McNamara, 2009), is its ability to widen the exploration of participants' experience-based information.

3.1. Participants

This study aimed to target public visions and forecasts in how they can foresee the features of CCTV systems that can make them an efficient solution for combating security and privacy threats. Five public participants were selected randomly from the United Arab Emirates (UAE), among them were expats and local Emiratis. Additionally, an expert in information security and data privacy in one of the largest institutions in UAE was interviewed as well to see or judge how common, or how far or near, his thoughts and forecasts from publics' ones, and also to assess the validity or reliability of civic thoughts from being achieved by comparing them with expert's ones. Public participants were selected randomly from different areas in Dubai, and they were mainly students at the British University in Dubai (BUiD). However, the expert was one of the known UAE conferences' panelists in the domain of Information Security and Data Privacy, and he was working in one of the biggest institutions in UAE as Chief Information Officer.

3.2. Interview Protocol

The main purpose of the interviews was to know the needed CCTV systems' characteristics or features that could be envisioned or recommended by the public to trust and coexist with the existence of such surveillance systems. Semi-structured interviews were chosen and used because it helps people to express their opinions freely without limits and also help interviewers to branch out main questions to different sub-questions until they'll get saturated and profound answers (Kvale, 1996).

To achieve the aim of this research, i.e. to identify characteristics or features that public recommends or envisions for CCTV surveillance systems to trust and coexist with its existence, different factors were studied, among them: cameras locations and way of installations (how and what to view), security concerns tackled by cameras and its importance, privacy threats that are posed by CCTV systems and how to narrow it, last participants' demographic details (as an independent variables), such as: gender, nationality and qualification, to examine how responses and requirements may vary from one participant to another. So, the main theoretical framework areas or concepts (as a dependent variable) and the corresponding interview questions are displayed in Table 1 below.

Research main concepts	Interview Questions (Question Code)
Camera Locations (Pervasiveness)	During your everyday life, where did you experience seeing surveillance cameras? (Q1)
CCTV Security Roles	Do you think why people may feel secure for the existence of cameras? (Q2)
CCTV Privacy Concerns	What will be your reactions or behaviors if you'll see the cameras? (Q3)
	Why do you think why people may concern about privacy if they'll know cameras are watching them? (Q4)
CCTV Forecasted Features needed to provide security while maintaining privacy at the same time	How do you envision the recommended camera features that make you more comfort about your privacy in that places? i.e. How it should function? (Q5)
	What about cameras current locations, and camera orientation, if you'll suggest a change on them what it could be? (Q6)
	Do you want to add any other suggestions to make camera surveillance system provide security and protect privacy at the same time? (Q7)

Table 1. Research Main Concepts and Corresponding Interview Questions

In Appendix section, Table 6 illustrates most parts of one of the conducted interview protocol and shows how it was flowing, and also it presents one real answer for one of the interview's questions, its sub-question, and also its related descriptive and reflective notes that were taken during the conversation. The interview questions were chosen after running a pilot test for them, to confirm from their clarity. Once the interviews were done, and since all participants accept the audio recording for the conversation, that dialog was transcripted into text. In Appendix one complete transcript for a dialog of one of the participants is illustrated.

3.3. Data Analysis

To examine and explore all data documents, qualitative content analysis conducted according to the line by line open coding illustrated in (Khandkar, 2009). The beauty of this method lies in breaking the data documents or transcripts into small manageable chunks of ideas for easy analysis and classifications. First, before starting with the main content analysis, demographic details were extracted for all participants and illustrated in Table 2. None of the Participants accepted to share other details rather than nationality and qualification, except PT1. As the first step in the content analysis, the interview questions with their related participants' answers were filled in a table, i.e. Table 3-A and Table 3-B, female responses were gathered in one table, i.e. Table 3-A, and males' ones in another, i.e. Table 3-B, including in the last expert replies. That distinguish have been made to compare answers between different genders and compare all public ones with the expert response, taking into consideration their qualifications and nationality. Then, the main themes, answered by participants, for each research concept were extracted.

PT. Codes	PT. Name	PT. Gender	PT. Nationality	PT. Qualification	Interview Time and Date	Public /Expert
PT1	Thomas	Male	India	Student/Worker	7/Mar/2018 11:00 am	Public
PT2	N/A	Male	Emirates	Worker	8/Mar/2018 07:00 pm	Public
PT3	N/A	Female	India	Student	7/Mar/2018 12:00 pm	Public
PT4	N/A	Female	Sweden	housewife	8/Mar/2018 09:00 pm	Public
PT5	N/A	Female	Emiratis	Student	8/Mar/2018 08:00 pm	Public
PT6	N/A	Male	India	worker	9/Mar/2018 09:00 pm	Expert

Table 2. Participant Demographic Details

After that, the extracted themes have been moved to another table that shows the main concepts with the corresponding common primary themes, participant codes who answered that, and secondary themes that were emerged from primary ones, assuring the removal of any duplicated answers. See the illustration of the aforesaid in Table 4.

4. Results and Discussions

The pervasiveness of the video surveillance became a reality that no one can change. Therefore, gathering ideas to allow public coexistence with these systems were the main objective of this research. The first phase to achieve that was the idea of this project since it's important to know at first the visions from the main consumers or exposed elements to such systems, i.e. the public, in how to accept and live with the fact of their existence. As an overall significant notice about the outcome of this study, there were answers' commonalities in the public responses, despite the difference in genders, nationality, or qualifications, and also, they were in harmony with the expert's opinion. To answer the main question in details, below illustrates the detailed results for the research's sub-questions:

4.1. How serious is the pervasiveness of the surveillance system?

This question was asked to reflect on how important is the need for ways to coexist with CCTV existence. Most public answers from both genders (two males and Females) were equally agreeing that cameras exist in: roads, residential building or private homes, commercial buildings and offices, Shopping Malls, and car parking or metro or bus stations. Also, more than one participants were agreeing that they were noticeable as well in Airports, Universities or schools, and banks. And Car showrooms, embassy, parks, elevators, and corridors are the rest of the mentioned locations. This reflects how big is the spread of cameras and how they are really existing in most areas related to our lives, as given in the literature.

4.2. What are the security vital and important roles provided by CCTV systems?

To understand the viability of the need of such systems and the importance of their presence, this question was raised, and around 80% of the respondents answer that they assure that the unlawful activities are easy to be caught, also, 66% of the responses pointing to the necessity of cameras in providing the feeling of being secure as someone is monitoring. Moreover, the rest of the reasons of being secured were their trusts of its ability to deter people from committing crimes, they found it effective tool for Identify weaknesses or problems to be rectified, people became more likely to follow the rules and regulations, and they caused improvements in public safety and reduced the criminal rates. These answers were not contradicting with what been given in (Conche & Tight, 2006), (Wilson & Sutton, 2003), (Pointing et al., 2012), and (Welsh & Farrington, 2002) studies.

Questions	PT3 Response	PT4 Response	PT5 Response
Q1	On roads (to monitor traffic or people), buildings (residential & commercial)	Airport, ATM, banks, embassy, consulate, highway, traffic, parking lots, shops, police, jail, court, monitoring traffic on a highway, some people have them in their cars. At various businesses (such as shopping centers, schools, various institutions), at people's residences (homes)	In elevators, apartment buildings, bank branches, airports, shopping centres, car showrooms
Q2	Any fraud activity can be easily caught, We feel secure when we have a feeling that someone is monitoring.	They feel that the camera may catch people involved in unlawful activity. For example, cameras may catch someone speeding on a highway, therefore putting other people's lives in danger. A traffic light may catch someone crossing on a red light. If there is a motor vehicle accident, the camera can show whose	If something happens, there's a record that makes it easier for the perpetrator to be apprehended. Given then the increased likelihood of getting

		fault was it. Cameras installed on business or private property can catch a thief trying to break in. Cameras may deter bad people from doing bad things. They could also offer a sense of security to those protected by them.	caught, cameras deter people from committing crimes. The general behaviors observed can be used to design security procedures (e.g. times for security personnel to walk by). It can help identify weaknesses to then be rectified (e.g. seeing holes in a fence where thieves are getting through, so this can be fixed)
Q3	Will be more conscious as if someone is monitoring us (Mainly to protect my privacy, M) (For example. Private behavior: I went to a place and my daughter was crying I want to breastfeed her. there were no people there but there were cameras. So, I couldn't feed her.	Surveillance can generate a good reaction because people are afraid to be punished and more aware of what is morally wrong and right. People are more likely to follow the rules and regulations and avoid cheating. Normal people and those with healthy morals would probably be on their best behavior. They usually care about their image and their reputation and would be embarrassed to be caught in an unflattering situation. Others may see security cameras as their "15 minutes of fame" and they can make funny faces or behave in a funny way for those monitoring the camera. Then you also have those immoral individuals who will engage in unlawful activity with total disregard to the fact that there are cameras around them. Surveillance cameras may affect the way we behave in public. People may change the way they dress for fear of drawing attention to themselves.	I'm more cautious in my behavior, make sure I don't do anything that could be deemed inappropriate. Otherwise normal.
Q4	These data can be misused, Sharing through the internet	First of all, to be watched people may experience negatively as they are "spied", Even if you are not doing something wrong to be monitored it will give you a sense of no privacy and a sense of loss of your anonymity. The fact that you are filmed and became a part of a database that you can't control and have no idea how it will be used it's a scary thing to think. Although surveillance cameras improve public safety and reduce criminal rates, they also are severely affecting our private lives. We all have private lives that we want to protect from the prying eyes of the government and other entities. Surveillance information is easily abused; therefore, this information can fall into the wrong hands. Surveillance may catch the criminals but may not be able to prevent the crimes. Security cameras could be used to spy on people.	They may be concerned that behavior that's not necessarily illegal may still be used against them to get them in trouble. They may not like the idea of being watched, even if their behavior is ok. They don't know who is seeing the recordings. Very often, they are not given any notice that they are being recorded.
Q5	It can blur faces and made it visible only in suspicious cases	To protect people's privacy, the user of the surveillance information should not be allowed to zoom on people's faces unless there is a reason to believe that the benefit of that action would outweigh the risk of invading someone's privacy.	Motion activated (i.e. only switch on if someone near to access the secured area) High-quality, high-pixel images
Q6	I don't mind it keeping in any public places. it should not be peeping into	Privacy cameras should not be installed in public restrooms, hospital rooms or any other places where the public has an expectation of privacy. They should not be pointed towards people's windows. Cameras should be installed	Signage notifying people that cameras are present

	private spaces	only in those locations where the necessity of filming is much more than a necessity to be private. The cameras will be oriented to the object that is an aspect to protect and surveil.	
Q7	Nothing more to add	To protect people's privacy, strict laws should be in place to regulate the use of surveillance cameras (what is recorded, how long the recording is stored, who will have access to that information, how can compliance with those rules be verified and enforced, what punishment would be applied to violators). There should be a strong system protecting the information gathered from falling into the wrong hands. Obligatory to inform the public that there's a camera. Cameras can't be placed into the area where you aspect to be private or oriented in such a way that it will be a violation of privacy	Policies on how long the recordings are kept, who is seeing them, and where/how they are being stored.

Table 3-A. Line by Line Coding for All Female Participant Responses

Questions	PT1 Response	PT2 Response	PT6 Response
Q1	Malls, parking lot, government offices, Public parks, private homes	Cameras can be seen on the streets (eyn Al Saqer), entrance gates, Basement car Parking, Offices, shopping malls, and corridors.	Shopping Malls, Airports, Universities, Bus Stations, Metro Stations, Traffic Junctions
Q2	I think it creates a feeling of being watched and hence acts a deterrent, for example, a security camera in an ATM machine lets users know that the area is under surveillance and gives the feeling of security.	Yes, surveillance cameras have and will prevent many crimes some people disagree and claim that will violate their privacy but it's not correct because why be out in public if they want privacy.	Often there is news that criminals have been caught based on camera videos, Legally it might be easier to prove your version, You feel that others might not dare do something wrong for fear of getting caught, You feel help is at hand because someone is watching the video feed.
Q3	I got used to it by now and don't mind them, usually security cameras are positioned in way that it's not very prominent like a videographer pointing the camera continuous at you, so you know the camera is there but at the same time it's not focused on you specifically	Always I will behave good in front of cameras especially to prevent my belongings and privacy to avoid illegal recording or monitoring. Also, if you have nothing to hide then have nothing to worry about.	You might become self-conscious when you sense that you are watched. But mostly you go about your business without problems
Q4	Recording people without their permission, and moreover sharing this information with others.	People need to be clear why their information is collected. How cameras images or records being used. how long camera images or records being kept and are they safe and only authorized people can see. Rights of access to the information by the individual concerned	There is always a chance that the video can be viewed by an unauthorized person, there are chances that the camera and the system have not be configured securely, there are open Camera feeds that can be accessed over the internet), the videos can be edited and misused for malicious purposes, your movements can be tracked.
Q5	It probably could delete records after some time (Timeframe might depend	Cloud-managed surveillance systems, to centralized the control. SSL encryption between webcam and	The video should be secured and should be watched only by authorized

	on the area if surveillance), Ensure that information is not shared with others (Others could be anyone else not owning the surveillance system, we could provide they are regulated by agencies, at some point there has to be a trust factor, but needs to be monitors and regulated for violation) by signing NDS agreements with regulatory bodies	systems Firewall for system access protection The web-based graphical user interface, to view the content	personnel, Copying should be done only with legal permissions, there should be warning signs about the presence of cameras.
Q6	I think all public places should be monitored by camera	Movable, night view, design, minuteness and infrared.	Cameras should be limited to entrances, exits Zooming in should be done only in case of suspicion of security risks and should be logged. There should be a routine audit of the system.
Q7	The people handling security tapes or storage need to be trained, for privacy preservation, they would need to sign NDS and again be listed in the database of regulators, They cannot be bringing in any recording devices in the surveillance room, Face masking etc. should be at level 2, Level 1 is raw data video capture, Depending on access clearance The system could unlock the features and reveal the identity (Level 1 data should be encrypted. Data custodian can be the surveillance owner since he takes the responsibility), A good idea would be to have a centralized storage with multiple point s of camera surveillance, this could be managed by a government body	Switch on when any movement detected only and Privacy rights by default.	AI can make surveillance better. Suspicious objects can be identified automatically. Suspicious movements can be detected too. All disks removed from any surveillance system should be completely wiped before recycling. Security personnel who are in charge of surveillance should be screened. USB and other external storage should be used only with legal permissions Internet Access should be prohibited in systems connected to surveillance systems

Table 3-B. Line by Line Coding for All Male Participants' Responses, Including the Expert's One.

Concepts	Participant Codes	Primary themes	Secondary themes
Camera Locations	PT3, PT5, PT2, PT6 PT3, PT4, PT5, PT1 PT3, PT1, PT2, PT4 PT4, PT5, PT6, PT2 PT4, PT1, PT2, PT6 PT4, PT5, PT6 PT4, PT6 PT4, PT5 PT4 PT5 PT1 PT2	On roads (streets, highways, or traffic junctions), buildings (or Private Homes), Offices (or commercial buildings) Malls (or shops) Car Parking (or other bus or metro stations) Airports Universities (or institutions, or schools) Banks (and ATMs) Embassy, consulate, police, jail, court, in their cars. In elevators, car showrooms Public parks Entrance gates and corridors.	Monitor traffic and people
CCTV Security Roles	PT3, PT4, PT5, PT2, PT6 PT3, PT4, PT1, PT6 PT5, PT6 PT5 PT5 PT6 PT4 PT4	Unlawful activities can be easily caught, Feel secure when we have a feeling that someone is monitoring. cameras deter people from committing crimes. Observed behavior to design security procedures Identify weaknesses to then be rectified Easier to prove your version People more likely to follow the rules and regulations Improve public safety and reduce criminal rates	Fraud, High-speed driving, crossing traffic lights.
CCTV Privacy Concerns	PT3, PT4, PT5, PT2, PT6 PT3, PT4, PT2, PT6 PT1, PT2, PT6 PT3, PT1, PT2 PT4, PT5, PT6 PT4, PT2 PT1 PT6 PT6 PT3 PT4 PT5	More conscious about moralities. Data can be misused. Nothing since they have nothing to hide or fear of. Fear of content sharing without informing. Feeling of being spied with no reason. Right to access or control databases that aren't provisioned Recording people without their permission camera and the system have not been configured securely, Open Camera feeds that can be accessed over the internet), No Private Behaviors, like Breastfeed babies. Loss of your anonymity. Behavior that's not necessarily illegal may still be used against them to get them in trouble.	Embarrassed to be caught in an unflattering situation. Prevent my belongings and privacy to avoid illegal recording or monitoring.
CCTV Forecasted Features needed to provide security while maintaining privacy at the same time	PT3, PT2 PT4, PT6 PT5, PT2 PT1, PT6 PT6, PT4 PT3, PT4 PT5, PT4 PT6, PT4 PT4, PT5 PT1, PT6 PT2 PT2 PT2 PT6 PY6 PT4 PT4 PT6 PT1	Blur faces and made it visible only in suspicious cases. Guards should not be allowed to zoom on people's faces unless there is a reason. Motion activated (i.e. only switch on if someone near to access the secured area). CCTV needs to be monitored and regulated for violation. CCTV systems should be secured. IT should not be peeping into private spaces. Signage notifying people that cameras are present. There should be a routine audit of the system. Strict privacy violations laws, policies, and regulation. Prohibit the entrance of any recording or storage devices in CCTV room, but only legally. Cloud-managed surveillance systems, to centralized the control. SSL encryption between webcam, CCTV systems, or GUIs.	Regulation related to what to record, how long to save, who should access, how to audit, and what is the punishments.

	PT1 PT6 PT6 PT6 PT2 PT1 PT1	Firewall for system access protection Copying should be done only with legal permissions, There should be warning signs about the presence of cameras. Should not be installed in public restrooms, hospital rooms or anywhere the public has an expectation of privacy. The cameras will be oriented to the object that is an aspect to protect and surveil. Cameras should be limited to entrances. Train Guards and system owners for privacy preservation. Have a centralized storage with multiple point s of camera surveillance that could be managed by a government body. AI can make surveillance better to identify suspicious objects or movements. All unwanted disks should be completely wiped before recycling. Internet Access should be prohibited in systems connected to surveillance systems. People needs to be cleared why information being collected. Delete records after minimal time frames. Ensure that information is not shared with others.	

Table 4. Concepts with Related Main Themes and Secondary Themes

4.3. What are the privacy concerns caused by the existence of such systems?

In the previous questions we saw how participants were agreeing about CCTV existence benefits, however, it's important to know from them what they don't like about having them, and what makes them hesitant to coexist with them. All participants except one said that they feel that they should be conscious whenever they know that there is a surveillance camera, however, most of the males noted that they start to get use of it and act normal. Unlike women, this can be due to the fact that women may be forced to do some private behavior acts (as Brest feeding) in addition to their overall shying nature they will keep consciousness toward the existence of cameras. Moreover, four of the participants were concerned about the misuse of recorded items. And the rest of the common reasons were their fear of content sharing over the internet and the unwanted feeling of being spied for no reasons. Other interesting answers were that they still feel that they've been recorded without any permissions and at the same time they cannot access the information. (Kalva et al., 2009) and (Babaguchi et al., 2009) in the literature gave the example of how the data can be misused and (Piatrik et al., 2012) and (Cavailaro, 2007) mentioned in the literature illustrate the consequences of being spied without legal reason. That results show that still privacy threats exist and until today same fears or concerns are presented, that's why until today and as per participants' responses still the concern is not eliminated to be able to coexist.

4.4. What are the CCTV systems' characteristics or features that can satisfy security and privacy concerns simultaneously?

After assuring from CCTV pervasiveness and its necessity for security, and when we asked the public for the ways to remove their privacy concerns in a way that can make them accept the presence of CCTV, they showed their excitement in producing ideas to eliminate these concerns. The interesting thing in the answers of this question was the variety of their visions for the wanted or prospected CCTV systems. The visions that were in common are: the need for face hiding mechanisms and make real identities visible to authoritative entities, as what was proposed in (Korshunov & Ebrahimi, 2013) study, systems guards shall be monitored for unlawful acts like zooming on people's faces without reasons, CCTV systems rooms have to be secured and not easy accessible by unauthorized people, notifying people about the presence of cameras, and last the need for strict policy, laws, and regulation against any violations. So as a result of these responses we notice that in some of them like (the request for being notified about its existence) is implemented, but since they're still recommended that mean the current notification techniques are not known or pervasive enough. Also, it's clearly shown that the public is not awarded about the existence of laws that protect their privacy from being violated. Besides the aforementioned recommendations, there are other pointed by the expert which seems interesting, like: the usage of artificial intelligence solutions

to make the surveillance more efficient and directed only toward the suspicious objects and the prohibition of the internet access for the surveillance systems. Also, another last feasible suggestion is to employ motion or zooming auto activated features, such that only if suspicious faces or movement is detected the camera can switch on to record. Overall, some of the requested features may be existed, like what is aforementioned about (Piatrik et al., 2012), but the lack of completed system and corresponding regulations are missing, and the awareness are not conducted properly. However, some others are not yet implemented, and the benefit of this research was to shed the light on such kind of prospected features to be the next research proposal for any researchers interested in this domain.

The main limitation and challenge faced in this study were the time limit. More number of public participants supposed to be interviewed to have more variety of responses and more views and visions for the future wanted CCTV systems. However, that can be one dimension of the future work of this study. Other interesting dimensions might be to target privacy professionals who can give feasible predictions for the needed features of CCTV systems, based on given public responses. Additionally, the aforementioned public responses can be compared and evaluated against existing privacy practices to evaluate and locate the gaps in the existing practices and narrow them by designing strategies and regulations for surveillance systems that have privacy as an integral part of it.

5. Conclusion

CCTV surveillance systems become essential tool needed for safe and secure living. However, and until today, privacy concerns related to its existence still exist. Due to that fact, civics have difficulties in accepting the existence of such systems. Hence, this research lists these issues which were gathered from those who were exposed to them. Besides, their forecasts for the features of such systems were huddled, such that it can be moved to a next step where it can be applied to achieve the main objective of this study, i.e. to have a camera surveillance system that satisfies security and privacy concerns and acceptable for the public to coexist with.

References

Abu Dhabi Urban Planning Council. (n.d.). *Abu Dhabi Safety and Security Planning Manual*.

Babaguchi, N., Koshimizu, T., Umata, I., & Toriyama, T. (2009). Psychological study for designing privacy protected video surveillance system: PriSurv. In *Protecting Privacy in Video Surveillance* (pp. 147–164). https://doi.org/10.1007/978-1-84882-301-3_9

Boguslaw, R., & Westin, A. F. (1968). Privacy and Freedom. *American Sociological Review*, *33*(1), 173. https://doi.org/10.2307/2092293

Boult, T. E. (2005). PICO: Privacy through invertible cryptographic obscuration. In *Computer Vision for Interactive and Intelligent Environments 2005* (Vol. 2005, pp. 27–38). https://doi.org/10.1109/CVIIE.2005.16

Cavailaro, A. (2007). Privacy in video surveillance {in the Spotlight}. *IEEE Signal Processing Magazine*, *24*(2), 168–169. https://doi.org/10.1109/MSP.2007.323270

Conche, F., & Tight, M. (2006). Use of CCTV to determine road accident factors in urban areas. *Accident Analysis and Prevention*, *38*(6), 1197–1207. https://doi.org/10.1016/j.aap.2006.05.008

Dempsey, J. (2007). *Introduction to Private Security*.

Friedewald, M., & Pohoryles, R. (2016). *Privacy and Security in the Digital Age*.

Graham, S., Brooks, J., & Heery, D. (1996). Towns on the television: Closed circuit TV in British towns and cities. *Local Government Studies*, *22*(3), 1–27. https://doi.org/10.1080/03003939608433827

Kalva, H., Carrillo, P., & Magliveras, S. (2009). Compression independent reversible encryption for privacy in video surveillance. *Eurasip Journal on Information Security*, *2009*. https://doi.org/10.1155/2009/429581

Khandkar, S. H. (2009). Open Coding. *Cpsc*, 1–9. https://doi.org/10.4135/9781412963909.n299

Korshunov, P., & Ebrahimi, T. (2013). Using warping for privacy protection in video surveillance. In *2013 18th International Conference on Digital Signal Processing, DSP 2013*. https://doi.org/10.1109/ICDSP.2013.6622791

Kvale, S. (1996). An introduction to qualitative research interviewing. *Sage Publications*. https://doi.org/10.1016/S0149-7189(97)89858-8

Maghal, J. (2016). National Security vs. Privacy in the modern age.

Mahmood Rajpoot, Q., & Jensen, C. D. (2015). Video Surveillance: Privacy Issues and Legal Compliance.

Promoting Social Change and Democracy through Information Technology.

McNamara, C. (2009). General Guidelines for Conducting Research Interviews. *General Guidelines for Conducting Interviews*, 2–4. https://doi.org/10.1017/CBO9781107415324.004

O'Mahony, C. (2014). The Modern Law Review, 524–527.

Park, H. H., Oh, G. S., & Paek, S. Y. (2012). Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea. *International Journal of Law, Crime and Justice*, *40*(3), 179–191. https://doi.org/10.1016/j.ijlcj.2012.03.003

Piatrik, T., Fernandez, V., & Izquierdo, E. (2012). The privacy challenges of in-depth video analytics. In *2012 IEEE 14th International Workshop on Multimedia Signal Processing, MMSP 2012 - Proceedings* (pp. 383–386). https://doi.org/10.1109/MMSP.2012.6343473

Pointing, S., Hayes-Jonkers, C., Bohanna, I., & Clough, A. (2012). The role of an open-space CCTV system in limiting alcohol-related assault injuries in a late-night entertainment precinct in a tropical Queensland city, Australia. *Injury Prevention*, *18*(1), 58–61. https://doi.org/10.1136/injuryprev-2011-040080

Taylor, E. (2013). Vision of Control: A Case Study on School CCTV, 40–60.

Wilson, D., & Sutton, A. (2003). Open-Street CCTV in Australia. *Trends and Issues in Crime and Criminal Justice*, (271).

Zhang, Y., Lu, Y., Nagahara, H., & Taniguchi, R. I. (2014). Anonymous camera for privacy protection. In *Proceedings - International Conference on Pattern Recognition* (pp. 4170–4175). https://doi.org/10.1109/ICPR.2014.715

Appendix

Title - Public Views: How to make surveillance systems satisfies security and privacy concerns	
Introductory Background Information	
Date & Time:	March 7th, 2018 at 11:00 am
Location:	British University in Dubai
Interviewer:	Lubna
Interviewee Details	
Name (optional):	Thomas
Gender (Male / Female):	Male
Nationality:	N/A
Qualification (Student, Worker, N/A):	Student and Lecturer
Contact Details (optional):	N/A

Research Brief Description

Please let me brief you about my research topic. My research study seeks to know public views in how to make CCTV systems achieving security while maintaining public privacy at the same time. I planned to know that by studying what are your privacy concerns and how can you envision mitigating it by stating your visionary thoughts about the characteristics of such a surveillance system that can do so. So the aim of this research is to gather all needed aspects that make CCTV system provide security and privacy for publics.

Request for Recording Consent

Can I have your consent to record this conversation? ☐ (YES) ☐ (NO)

[If yes] Thank you for allowing me to record, please let me know if I should stop recording at certain point or if you require to delete certain part of recorded things.

[If no] Its fine, and appreciated for letting me know. Instead I'll take a notes of our conversation.

Before the beginning of the Interview:

Our interview will last approximately less than 20 minutes during which I will be asking you regarding that study.

Please note that there is no wrong or write answers and all your views will be important for the success of this research.

Kindly, stop me whenever you want, either if you'll have any questions, or you'll request any clarifications.

Main Question

- What are the features or characteristics of cameras that it should be exist to make it provide security and maintaining Human rights of privacy? Any imaginary thoughts or visionary forecasts?
  - ✓ Descriptive notes*:*
    To not keep the video recorded items for long time, to regulate the access and the misuse of recorded items, apply video editing features to hide features used to identify people (faces) in the level that is accessed by those who monitoring or owning the CCTV system and make such features unlocked only by authoritative agencies and for legal purpose.
  - ✓ Reflective notes:
    He was talking as if he's seeing the efficiency of his methods, as if the main reason for the misuse is the availability of recorded data, thus it should not be available for long. He sees that owners of such systems must be accountable and held responsible for any misuse occurred as a result of not securing or monitoring the access and the use of their system.

Sub Question

- What about the camera Location, orientation, zooming features, new legislations?
  - ✓ Descriptive notes:
    He believes that camera's current locations in public area with its current positions is still required and needed to monitor and combat crimes in those vital areas.
  - ✓ Reflective notes:
    Privacy concerns for him will raise if such cameras is meant to point toward him, and that's not the case for him in the most situations where he experienced seeing cameras. Hence, he agrees on its current features in public areas.

Table 4. Interview Protocol (First Page / First Question)

Thomas Interview Transcript

Lubna: I'd like to thank you once again for being willing to participate in the interview aspect of my research study.

Lubna: Please let me brief you about my research topic.

Thomas: No hassles, you are welcome

Lubna: My research study seeks to know public views in how to make CCTV systems achieving security while maintaining public privacy at the same time. I planned to know that by studying what are your privacy concerns and how can you envision mitigating it by stating your visionary thoughts about the characteristics of such a surveillance system that can do so. So the aim of this research is to gather all needed aspects that make CCTV system provide security and privacy for publics.

Thomas: Ok

Lubna: Our interview will last approximately less than 20 minutes during which I will be asking you regarding that study.

Thomas: Ok, go ahead

Lubna: But before that, can I have your consent to record this conversation, so I'll be able transcript it and add it as a row data for my research?

Thomas: Yes

Thomas: Ok

Lubna: Thank you for allowing me to record, please let me know if I should stop recording at certain point or if you require to delete certain part of recorded things.

Lubna: Before the beginning of the Interview:

our interview will last approximately less than 20 minutes during which I will be asking you regarding that study. Please note that there is no wrong or write answers and all your views will be important for the success of this research. Kindly, stop me whenever you want, either if you'll have any questions, or you'll request any clarifications.

Thomas: Ok

Thomas: No questions currently, thank you

Thomas: Please go ahead with your questions

Lubna: My first question is, during your everyday life, where did you experience seeing surveillance cameras?

Thomas: I have experienced seeing security cameras in malls, parking lot, government offices

Lubna: Any other places to add?

Thomas: Public parks, private homes

Lubna: for the private homes, were they external or internal cameras?

Thomas: External cameras usually near the entrance or porch

Lubna: Do you think why people may feel secure for the existence of cameras?

Thomas: I think it creates a a feeling of being watched and hence acts a deterrent

Thomas: In such a sense you could say that yes people do feel secure

Lubna: can you give one or two example?

Thomas: For example, a security camera in an ATM machine let's uses know that the area is under surveillance

Thomas: And gives the feeling of security

Thomas: Yes

Lubna: Ok I got it now. S, generally, what will be your reactions or behaviors if you'll see the cameras?

Thomas: I got used to it by now and don't mind them

Thomas: I go along doing my tasks

Lubna: So you'll not act consciously?

Thomas: Usually security cameras are positioned in way that it's not very prominent like a videographer pointing the camera continuous at you

Thomas: So you know the camera is there but at the same time it's not focused on you specifically

Thomas: Yes

Lubna: But that viewing angle could make it view what it supposes not to view, especially in private residential area, don't you agree on this?

Thomas: It's possible

Thomas: Hence privacy is important

Lubna: Great, this brought me to this question, why you do you think why people may concern about privacy if they'll know cameras are watching them?

Thomas: It's a thin line between privacy and security

Thomas: There are usually laws that govern these

Lubna: But to rephrase, what may threat the privacy of people when it comes to surveillance cameras?

Thomas: Recording people without their permission

Thomas: And moreover sharing this information with others

Lubna: You are rights, i agree with you.

Lubna: any more concerns to add?

Thomas: Nothing for the moment

Lubna: So, from your point of view, how do you envision the recommended camera features that make you more comfort about your privacy in that places? i.e. How it should function?

Thomas: It probably could delete records after some time

Lubna: I believe that the current lifetime for the recording to be saved is 6 months?

[3:36 PM, 3/29/2018] Lubna: how much less would you suggest to make it?

Thomas: Ensure that information is not shared with others by signing NDS agreements with regulatory bodies

Thomas: Time frame might depend on the area if surveillance

Lubna: do you mean by others: Security guards, shops owners, ...?

Lubna: providing that cameras are installed nowadays in offices, shops, residential and commercial buildings as well.

Lubna: So from whom you'd like to restrict access from?

Thomas: Others could be anyone else not owning the surveillance system

Lubna: Is that mean that you are trusting all surveillance systems owners?

Thomas: We could provide they are regulated by agencies

Thomas: At some point there has to be a trust factor

Thomas: But needs to be monitors and regulated for violation

Lubna: I see. I got your point.

Lubna: What about cameras current locations, and camera orientation, if you'll suggest a change on them what it could be?

Thomas: I think all public places should be monitored by camera

Lubna: Do you want to add any other suggestions to make camera surveillance system provide security and protect privacy at the same time?

Thomas: The people handling security tapes or storage need to be trained

Thomas: For privacy preservation

Thomas: They would need to sign NDS and again be listed in the database of regulators

Thomas: They cannot be bringing in any recording devices in the surveillance room

Lubna: There are current features like face masking or hiding or blurring and others that hides the identity of public and only authoritative entity can disclose it

Thomas: Yes, that's a very good thing

Lubna: so would you agree to add it among the needed features

Lubna: great, any concerns if such features will be implemented?

Thomas: Face masking etc. should be at level 2

Thomas: Level 1 is raw data video capture

Thomas: Level 2 is masking etc.

Thomas: Depending on access clearance

Thomas: The system could unlock the features and reveal the identity

Thomas: But again, there has to norms for all these

Thomas: Currently different surveillance temas have different ways of handling privacy

Lubna: Great ideas, but do you think who should be the data custodian of level 1?

Thomas: Level 1 data should be encrypted. Data custodian can be the surveillance owner since he takes the responsibility

Thomas: Mandatory log file should be enabled for each access

Lubna: Currently offices, shop, different kind of business is required by governments to install such systems, so in that case why the owners of such a system should have access to the raw data?

Lubna: I am talking about the use case scenarios applied in UAE

Thomas: Depends on who owns the system

Thomas: If shopkeeper own the system

[Thomas: And recording facilities he may as well be responsible for it

Thomas: If government owns the recording systems

Thomas: They should be responsible

Lubna: Thank you for bearing with me until now, I got very interesting answers and to the point replies. The last three main questions will be raised to judge the quality of my research study,

Lubna: would you like to add anything regarding the aforementioned questions?

Thomas: A good idea would be to have a centralized storage with multiple point s of camera surveillance

Thomas: This could be managed by a government body

Thomas: With participation from camera owners

Thomas: No nothing

Lubna: Thank you, I think I agree with you and I can foresee that as an ideal solution to be implemented in the future since most of the shop owners or companies were installing such systems to comply with the country's regulations related to that matter.

Lubna: Great, I would like to thank you again for your time, and last, I just need from you the following background details if possible. (Your Qualification and Nationality)

Thomas: Ok now that's privacy

Thomas: 😄

Thomas: Thomas

Thomas: From India

Lubna: I respect your privacy, answer whatever you can answer as it’s not a must

Thomas: Masters in computer science

Lubna: Good person, Good people, I enjoyed interviewing you. I had a very interesting notes about your thoughts. And btw. Thank you for providing your name 😄, so please tell me what I should exclude from the aforementioned

Thomas: I feel the nationality could be excluded

Thomas: But if you feel it's required for your research ... go ahead

Lubna: Done, Thank you again for your participation, informative response and valuable time.

Thomas: Thanks