Privacy in Pervasive Video Surveillance
Trust through Technology and Users Cooperation

Antoni Martínez-Ballesté, Agusti Solanas, Marc Vives and Hatem A. Rashwan
Departament d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili, Tarragona, Catalonia, Spain.

Keywords: Video Surveillance, Privacy, Trust, Mobile Applications.

Abstract: During the last decades, video surveillance systems (VSS) have become popular and, nowadays, they can be found almost everywhere. When those systems were initially deployed, they were mainly used by authorities only and, people tend to accept to be surveilled for the sake of security. Currently, VSS are located in public places and controlled by governmental agencies, but some others are placed in private spaces and controlled by corporations, banks, and so on. In addition, VSS have gained computational capabilities and, nowadays, off-the-shelf cameras are able to record high quality digital video that can be easily shared by means of private networks or even the Internet. Trust is strictly related to the operators of those VSS and their behaviour. Hence, it is necessary to define a comprehensive model for trustworthy video surveillance, aiming at preserving the right to privacy of citizens. In this article we present a platform for trustworthy video surveillance. Our model is based on the use of real-time and accurate techniques, and the active cooperation of people using mobile applications.

1 INTRODUCTION

The existence of pervasive video surveillance systems (VSS) and their inherent ubiquitous nature endanger the privacy of people since they are recorded while performing their daily activities and, a lot of private information can be obtained from these recordings. The main goal of video surveillance is to improve security. Clearly, authorities must be able to access those cameras and their recordings whenever necessary, but the massive and growing use of VSS requires to reconsider their associated privacy problems.

Current legislation in most countries states that any image that allows the identification of a person must be considered as *personal data*. By doing so, the law is protecting people against deliberate attacks to their privacy rights. However, in most cases, legislation only specifies that the responsible for the management of the recordings is the *owner* or *operator* (*i.e.* the administrator of the systems). That means that people have to trust that the owner behaves according to the law. Also, laws require the owners of VSS to publicly announce the presence of surveillance cameras. New proposals for legislations (European-Parliament, 2012) propose the adoption of privacy by design methodologies, so as to tackle the concept of privacy in a comprehensive manner.

Notwithstanding, citizens lack a certain way to know how many cameras have recorded them whilst performing their daily activities. This is specially important in the context of a smart city, where video surveillance plays a key role (Martínez-Ballesté et al., 2013a).

Moreover, scientific literature (Senior, 2009) addresses the privacy-preserving video surveillance problem by paying attention to the algorithms used to protect the so-called regions of interest (the sensitive information such as faces, car plates or other identification information): first, computer vision techniques are used to detect the regions of interest; afterwards, information security procedures are applied to those regions so as to preserve the privacy of individuals (*e.g.* preventing the re-identification of people). However, the privacy issues raising in our globally video-surveilled society must be tackled from a much wider perspective.

Having this holistic view in mind, **trustworthy video surveillance** can be defined as the combination not only of technologies, but also other elements, to ensure the right to privacy of citizens comprehensively.

In this article we present a model for achieving trust in pervasive video surveillance. Essentially, we

Martínez-Ballesté A., Solanas A., Vives M. and A. Rashwan H..
Privacy in Pervasive Video Surveillance - Trust through Technology and Users Cooperation.
DOI: 10.5220/0004724200490054
In *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems* (PECCS-2014), pages 49-54
ISBN: 978-989-758-000-0
Copyright © 2014 SCITEPRESS (Science and Technology Publications, Lda.)

describe a software platform that allows the reliable protection of people's privacy and a mobile application that allows citizens to be aware of the video surveillance prevasive challenge.

2 TRUSTWORTHY VIDEO SURVEILLANCE

Trustworthy video surveillance can be described as a complex problem comprising three main concepts: *Law Enforcement*, *Trust in the VSS Technology* and *Social Cooperation*. These three elements must work together to achieve comprehensive and feasible trustworthy video surveillance systems. They are addressed in the following paragraphs:

- *Law Enforcement* is the first and most apparent component and, it refers to the legal aspects of VSS. Users clearly feel more comfortable with a legislation that protects them from dishonest VSS owners. In a comprehensive trustworthy video surveillance scenario, legislation should go further than the current one. For instance, law could require the use of privacy-preserving techniques over the recordings of the cameras. However, as we will see later, current legislations are mainly focussed on trusting the owners of the VSS.

- Trusting that owners and operators behave properly is not so easy (*e.g.* how could we be sure that they will not send the recordings to unauthorised people?). In this sense, the idea of *Trust in the VSS Technology* consists in handing over trust from the owners to the very VSS. Thus, for a VSS to be trusted, it must guarantee the detection of sensitive information within the recordings, and their protection. That means that everyone should have access to the protected recordings (*i.e.* the *public version* of the video) so as to be able to verify that their privacy is properly protected (*e.g.* their faces have been properly obfuscated). Moreover, authorities (the so-called *trusted managers*) might be able to obtain the original recordings from the protected ones by applying some secure disclosure functions if necessary (*e.g.* in case of criminal investigation or the like). However, ensuring trust in a VSS is not straightforward. First the system must be able to detect all sensitive areas of the images and protect them without the supervision of humans that could misbehave. Also, the obfuscation procedure should be performed in real time to avoid the storage of unprotected information. Note that those are challenges that are currently being studied by the research community (Martínez-Ballesté et al., 2012).

- Finally, the last piece of the puzzle refers to *Social Cooperation*, which is based on the social relations amongst citizens and how they could help in improving their privacy. Users generate most of the information stored in Internet-based information systems. In addition, most of these systems have collaborative filtering applications in which users can rate the site information and add their opinions. Thus, for the people to realise about the privacy problems related to VSS, it is necessary that they might know the cameras that have recorded them during their daily activities. To address this problem, a collaborative approach seems to be very promising, since every user could contribute by informing about VSS and by rating their privacy protection quality (*e.g.* according to some of the properties stated above).

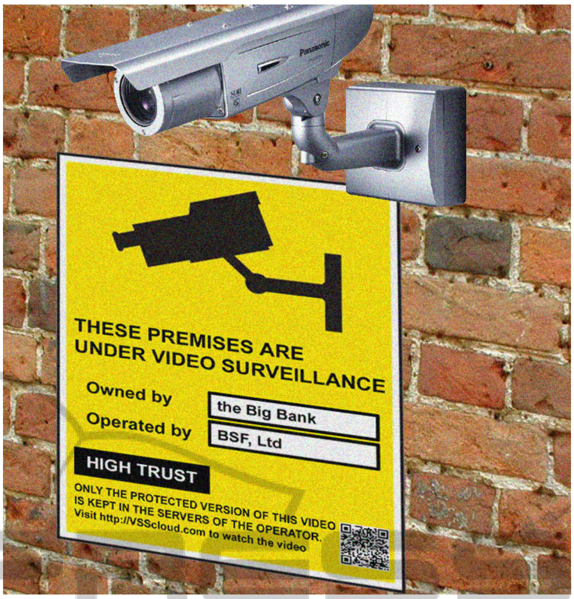

THESE PREMISES ARE UNDER VIDEO SURVEILLANCE
Owned by
the Big Bank
Operated by
BSF, Ltd
HIGH TRUST
ONLY THE PROTECTED VERSION OF THIS VIDEO IS KEPT IN THE SERVERS OF THE OPERATOR.
Visit http://VSScloud.com to watch the video

Figure 1: Example of a VSS camera with an appropriate warning sign.

Our approach to trustworthy video surveillance fulfills the aforementioned concepts.

3 CAMERAS: THE LAW'S PERVASIVE CHALLENGE

The number of surveillance cameras is growing at an unprecedented pace. According to (Lewis, 2011), in 2001 the number of cameras in the United Kingdom was about two million. Moreover, any citizen can be recorded by an average of 300 cameras a day while

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

staying in London. As a matter of fact, most of them are operated by public authorities, but the rest are scattered throughout shops, corporate buildings, private blocks, etc. The key issue is that those cameras are privately controlled and, consequently, the trust lies on the appropriate behaviour of the owners that, in principle, may not inspire as much confidence as public authorities. Besides, the ease access to this technology and the aforementioned growing computational capabilities of VSS pave the way for a massive collection and analysis of information that leads to a Big Brother Effect (*i.e.* a lot of private information can be obtained from the recordings, namely consumer habits, routines, contacts, social status, etc). As an example, video surveillance technology allows the surveillance and tracking of citizens while they drive (Cherry, 2012).

Indeed, security is (or should be) the only purpose of VSS. Thus, legislation plays a central role when privacy issues are involved and specially when there is a need for finding a proper balance between conflicting interests: on the one hand, the right to privacy; and on the other hand, the right to security.

In this line, governments have enacted laws regarding the use of video surveillance systems. For instance, European legislation (European-Parliament, 1995) considers citizens' data obtained by VSS as personal data. Additionally, some countries have also enacted laws explicitly concerning video surveillance. In the case of Spain (Bosch, 2011) it takes into account, among others, the following principles:

> I) VSS must be advertised, both indoors and outdoors;
>
> II) The owner of the system must take the right precautions to ensure the safety of the images and prevent modification, loss or unauthorized access or treatment;
>
> III) Data cannot be released to third parties, except for criminal investigations;
>
> IV) The use of cameras will always be respectful with the rights of individuals.

Legislation should evolve and *make the adoption of privacy-preserving VSS mandatory*. Moreover, we propose that besides informing about who is the owner of the VSS, mandatory information signs should contain other useful information such as e.g. whether the video is accessible through the Internet. In addition, each camera in a VSS should be labelled with a *level of trust*: i.e. from a *low/no trust level* if no privacy-protection is offered, to a *high trust level* if the camera belongs to a trustworthy VSS (Martínez-Ballesté et al., 2012).

To illustrate this concept, Figure 1 shows a drawing of camera with a proper warning sign. This sign clearly states the owner and operator of the VSS, as well as the level of privacy protection. Moreover, people are informed about the website that they can visit to check that their privacy has been correctly preserved. Last but not least and, specially in indoor locations, a display might be placed next to the camera to show the obfuscated video so as to allow people to verify that their privacy is being protected.

4 ALGORITHMS FOR TRUSTWORTHY PRIVACY

As we stated in Section 1, privacy-aware video surveillance is usually achieved by means of computer vision techniques applied to the surveillance video and its transformation using a variety of procedures (blurring, scrambling, etc).

In order to achive trustworthy video surveillance, and to materialize the concept of *Trust in the VSS Technology*, the following properties must be achieved (Martínez-Ballesté et al., 2013b):

1. The sensitive information must be detected accurately by the computer vision techniques.
2. The sensitive information must be protected using a reversible procedure.
3. The computational procedures applied to the video must perform in real time.

Note that if the first requirement is fulfilled, no human interaction will be necessary (and hence no "operator" will be monitoring the unprotected video). The fulfillment of the 2nd requirement avoids the storage of the original unprotected video in case of crime investigations. Finally, if the video is processed in real time no temporary storage of the unprotected video will be needed.

Hence, if legislation regulates on the use of trustworthy VSS, owners must ensure that sensitive information is protected in real-time and accurately. They will have to choose from a plethora of products and technologies to accomplish the mandatory utilization of privacy- preserving technologies.

There are some techniques in the literature devoted to the accurate detection of regions of interest in real time. Specifically, when the regions to be detected are faces, the *Haar-Features* technique (Viola and Jones, 2001) is accurate and works in real time. For a more general kind of regions of interest (*e.g.* bodies, cars, etc.) and, in the case of cameras focusing on a fixed background, robust techniques based on background subtraction such as *Codebook Construction* (Kim et al., 2004) can be used. Finally, techniques based on optical flow estimation (Horn and Schunck, 1993) overcome the shortcomings of a fixed background.

Furthermore, in order to protect the sensitive information and, at the same time, allow its disclosure under certain conditions (*e.g.* for criminal investigation), invertible operations/functions must be used. The so-called *coefficient alteration techniques* (DuFaux and Ebrahimi, 2006) are invertible operations in which the process of protection (and disclosure) depends on a key. The key is used to generate a "protection stream" – a set of bits that will be used to specify how the information in the regions of interest is changed. Since this technique alters the sign of the coefficients of the compressed video streams, its use does not affect the efficiency of the compressor (which is essential in any video storage network). Authorities could cryptographically generate the "protection stream" whenever it is necessary to use it to disclose a portion of the protected video.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

5 CAMNOTIFY: MAKING VSS VISIBLE

The right of people to privacy in VSS can be complemented with the ability to easily know the cameras of VSS that have recorded a given person. Hence we propose a website database of VSS and a complementing mobile application (*CamNotify*) that might help people realise about the privacy concerns related to pervasive video surveillance. The VSS using our software packages (allowing accurate and real-time video protection) should be listed in the database so citizens, equipped with a mobile phone running our app, could be notified of the nearby VSS.

Note that by means of this application, users could collaborate with the web service in different ways, for instance, by adding comments about the VSS, by voting, and by providing information about possible abuse or misuse. In that sense, collaborative filtering techniques could be also applied over the data stored in the census database of the service to obtain a holistic view of the privacy of users with regard to VSS. Finally, users could notify the existence of cameras belonging to VSS that are not using the privacy protection techniques. Consequently, the VSS database could be updated collaboratively by the users of the application.

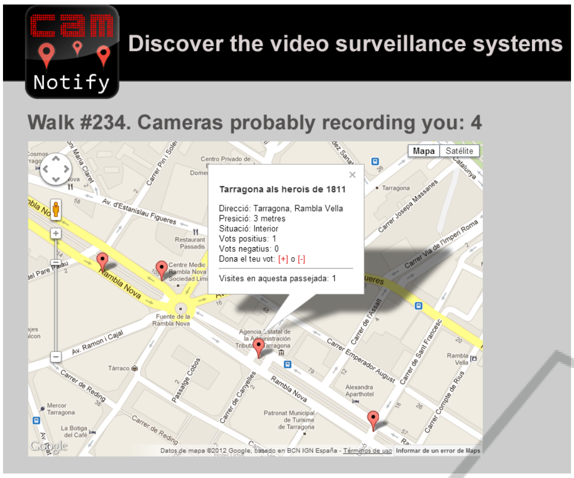
We have designed and implemented a prototype of this mobile application that is described in the following lines. With the aim to illustrate the scenario, let us consider the following example: Peter Smith enrols in the web service to be aware of the VSS that might have recorded him during his everyday activities. After downloading the *CamNotify* application to his smartphone, he registers to the service and turns on the application. The mobile app uses the self-location and communication capabilities of the device to request the web service a list of nearby cameras, according to its current position (longitude and latitude). In fact, this action occurs each time the smartphone detects a significant change in Peter's location.

Now, the app is able to measure distances between the current location of the device and the location of the cameras in the list. The cameras located close to the smartphone (*i.e.* that might have been recording Peter) will be listed in the display (on a map). Also, the list of cameras is shown 4. In addition, this list of cameras will be sent to the web service, which will be also aware of the time in which Peter passed nearby each camera.

After some time, Peter enters a shop willing to buy some coffee. He realises that the shop owners have installed several cameras in the shop premises. However, there is no visible sign advertising them nor any display in which the recorded video is shown. Peter takes a look at his smartphone and realises that this VSS is not in the list. Hence, he makes use of *CamNotify* to request the addition of a new camera in that location 3. Certainly, he will specify a *low trust level* for the VSS.

When he arrives home, Peter opens his laptop and connects to the web service website (cf. Figure 2) and he can access the list of cameras that might have recorded him, which are grouped by *walks*. He can read the comments of other users, manage some information and, naturally, he can make comments on the cameras he saw during the day (for instance, by warning that a camera that is currently labelled with a high level of trust, actually does not have a visible display).

Two hours later, Mary Martin, who is also a CamNofity user, enters the shop previously visited by Peter. She receives an alarm in the application: *CamNotify* warns her that there is a new camera being detected nearby and the web service needs to confirm that there is a real camera there (note that the camera was included in the system a few hours ago and it could be a fake). Mary confirms with a positive vote that the camera is actually there. Naturally, after a certain number of positive votes, the web service will stop requesting CamNotify users for confirmations. However, CamNofity can randomly request users to approve cameras from time to time, aiming at being notified of VSS not operating any more.



Discover the video surveillance systems

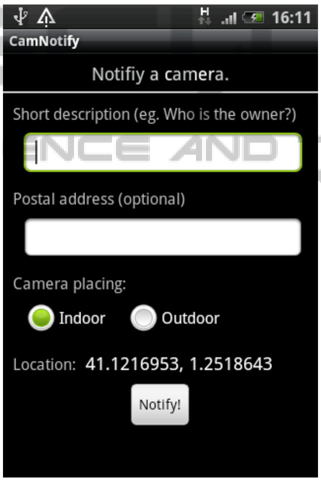
Walk #234. Cameras probably recording you: 4

Tarragona als herois de 1811

Direcció: Tarragona, Rambla Vella
Presició: 3 metres
Situació: Interior
Vots positius: 1
Vots negatius: 0
Dona el teu vot: [+] o [-]

Visites en aquesta passejada: 1

Figure 2: Website for the CamNofity application.



Notifiy a camera.

Short description (eg. Who is the owner?)

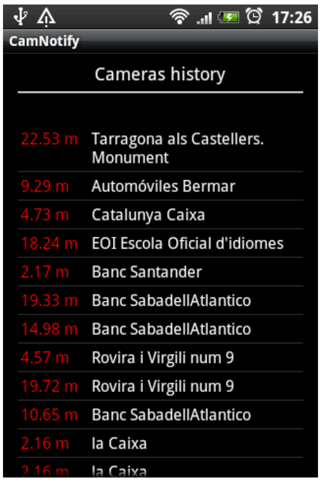
Postal address (optional)

Camera placing:

● Indoor ○ Outdoor

Location: 41.1216953, 1.2518643

Figure 3: The application allows the user to introduce a new VSS camera that is not in the system.



Cameras history

22.53 m	Tarragona als Castellers. Monument
9.29 m	Automóviles Bermar
4.73 m	Catalunya Caixa
18.24 m	EOI Escola Oficial d'idiomes
2.17 m	Banc Santander
19.33 m	Banc SabadellAtlantico
14.98 m	Banc SabadellAtlantico
4.57 m	Rovira i Virgili num 9
19.72 m	Rovira i Virgili num 9
10.65 m	Banc SabadellAtlantico
2.16 m	la Caixa
2.16 m	la Caixa

Figure 4: The list of cameras that might have recorded the user.

As a result, using such an application will contribute to cooperatively build a complete database of VSS. The web service will have a census composed by the cameras using its platform for detection and protection tools and the cameras that have been notified by users.

6 CONCLUSIONS

In this article we have presented a model for trust in pervasive video surveillance systems. Our model consists of Law Enforcement, Trust in Technology and Social Cooperation. To make our model a reality, first, legislation must evolve so as to make the adoption of privacy-preserving technologies in VSS mandatory. Second, instead of trusting the owners and operators of the VSS, the underlying technology for privacy protection must be trustworthy. Finally, citizens have to play a key role in assessing the different level of trust in the pervasive VSS.

We have discussed the role of legislators with respect to the achievement of comprehensive privacy in video surveillance. We have stated that the use of reliable protection techniques should be mandatory. We have shown that there are some feasible techniques that are worth to be trusted, since they allow the operation in real time thus avoiding the need of temporarily storing the original video. Finally, we have focused on the function of users when making visible the pervasive video surveillance systems. Thanks to a mobile application, users can be notified of the cameras around them. Moreover, they can contribute to collaboratively build a "map" of video surveillance systems.

We believe that following the proposals and recommendations of this paper, a scenario with trustworthy video surveillance is completely feasible. Legislators and engineers must pave the way for a social acceptance of this important family of pervasive technology.

ACKNOWLEDGEMENTS

This work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007- 0004 ARES, project TIN2011-27076-C03-01 CO-PRIVACY, and by the Rovira i Virgili University through project 2012R2B-01 VIPP.

SCIENCE AND TECHNOLOGY PUBLICATIONS

REFERENCES

Bosch, R. B. (2011). Análisis de la doctrina administrativa de la agencia española de protección de datos en relación con el tratamiento de imágenes a través de videovigilancia. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, (25):61.

Cherry, S. (2012). License plates, cameras, and our vanishing privacy (Spectrum). http://spectrum.ieee.org/podcast/geek-life/tools-toys/license-plates-cameras-and-our-vanishing-privacy.

DuFaux, F. and Ebrahimi, T. (2006). Scrambling for video surveillance with privacy. In *Privacy Research in Vision*, page 160.

European-Parliament (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://europa.eu/legislation_summaries/information_ society/data_protect% ion/l14012_en.htm.

European-Parliament (2012). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free moovement of such data. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Horn, B. K. P. and Schunck, B. G. (1993). Determining optical flow: A retrospective. *Artif. Intell*, 59(1-2):81–87.

Kim, K., Chalidabhongse, T. H., Harwood, D., and Davis, L. S. (2004). Background modeling and subtraction by codebook construction. In *ICIP*, pages V: 3061–3064.

Lewis, P. (2011). You're being watched: there's one CCTV camera for every 32 people in UK (The Guardian). http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance.

Martínez-Ballesté, A., Pérez-Martínez, P. A., and Agusti, S. (2013a). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, 51(6):136–141.

Martínez-Ballesté, A., Rashwan, H. A., Castellà-Roca, J., and Puig, D. (2013b). A trustworthy database for privacy-preserving video surveillance. In Guerrini, G., editor, *Joint 2013 EDBT/ICDT Conferences, EDBT/ICDT '13, Genoa, Italy, March 22, 2013, Workshop Proceedings*, pages 179–183. ACM.

Martínez-Ballesté, A., Rashwan, H. A., Puig, D., and Fullana, A. P. (2012). Towards a trustworthy privacy in pervasive video surveillance systems. In *PerCom Workshops*, pages 914–919. IEEE.

Senior, A. W. (2009). *Protecting privacy in video surveillance*. Springer.

Viola, P. and Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *Proc. CVPR*, 1:511–518.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS