Building a Privacy Accountable Surveillance System

Francisco Jaime[1], Antonio Maña[1], Zhendong Ma[2], Christian Wagner[2], Daniel Hovie[2] and Mathias Bossuet[3]
[1]*University of Málaga, Málaga, Spain*
[2]*Austrian Institute of Technology, Vienna, Austria*
[3]*Thales Communications & Security, Paris, France*

Keywords: Surveillance, Privacy, Accountability, Methodology, SALT, Process, Scenario.

Abstract: This paper presents a sample surveillance use-case based on a video archive search scenario. Privacy and accountability concerns related to video surveillance systems are identified and described here, thus assessing the impact on privacy of this type of systems. Then, after a description of the scenario, we produce the design for this particular context using the SALT methodology developed by the PARIS project. This methodology follows the privacy-by-design approach and ensures that privacy and accountability concerns are properly taken into account for the system under development. This kind of development entails a series of advantages, not only from the point of view of the subject under surveillance, but also for the other system stakeholders.

1 INTRODUCTION

Video surveillance systems are spreading nowadays nearly everywhere, they are present not only in private properties, but also in many public places, such as banks, airports, markets, etc. However, on many occasions the citizens (the objects under surveillance) are not fully aware of the surveillance system, i.e. they do not know what type of that the system is retrieving from them and the purpose it will be used for. Even more, they may not even know about the existence of the surveillance system at all. These circumstances entail a series of privacy lacks regarding the object under surveillance in current surveillance systems.

The PARIS project (PrivAcy pReserving Infrastructure for Surveillance) tries to provide a solution to this problem. In this way, taking into account privacy concerns in the development of surveillance systems becomes the main goal of the project, but not only that, accountability is another important feature to have in mind. It would be desirable to have the possibility of tracking who is accountable of the actions performed by the system at a given time or situation, especially when a privacy violation takes place.

We have developed a methodology that follows a privacy-by-design approach, which will help system stakeholders to identify the privacy and accountability requirements for the given surveillance system they intend to deploy. Besides, it will also guide surveillance system designers in order to make them aware of the privacy and accountability concerns, as well as provide them with relevant information to facilitate the task of taking into account these concerns by the implementation of proper measures.

To achieve this goal, the PARIS project lies in the SALT (Social, ethicAl, Legal, Technological) framework. This framework contains the information regarding the privacy and accountability concerns from the social, ethical, legal and technological points of view for current surveillance systems within a variety of environments and contexts. Such information will be provided by experts and it is the core that supports the methodology. Questionnaires destined to system stakeholders are also provided, which will provide criteria to assess the impact on privacy of the surveillance system to be.

Together with the SALT framework there is also a process, which makes use of a set of tools and the SALT framework. Surveillance systems designers can follow this process during the development of the system design.

In this paper, we show a sample use case based

Jaime F., Maña A., Ma Z., Wagner C., Hovie D. and Bossuet M..
Building a Privacy Accountable Surveillance System.
DOI: 10.5220/0005401606460654
In *Proceedings of the 3rd International Conference on Model-Driven Engineering and Software Development* (SPIE-2015), pages 646-654
ISBN: 978-989-758-083-3

on a video archive search system within a given scenario. Based on it, we identify the privacy and accountability requirements of this particular surveillance system and provide a privacy friendly design following the SALT methodology elaborated by the PARIS project, and hence experimentally showing the advantages achieved by its application.

Next, the paper is structured as follows: in section 2 we provide background information regarding privacy and accountability in current video-surveillance systems; in section 3 we describe the use-case taken as a sample for the application of the SALT methodology; section 4 details how the system is designed following the SALT process; in section 5 we describe the advantages and goals achieved thanks to the SALT approach in this particular use-case; finally, section 6 concludes the paper.

2 PRIVACY AND ACCOUNTABILITY IN VIDEO-SURVEILLANCE SYSTEMS

This section identifies the most typical privacy and accountability concerns for nowadays video-surveillance systems, how they currently are taken into account (in case they are) and how the SALT approach could contribute for improvements.

2.1 From the Research Side

Privacy and accountability must be considered throughout the lifetime of a video-surveillance system, typically consisting of the requirements identification, design, installation, operation, and decommission phase. At design time, the main focus of privacy and accountability concerns is on how to apply design principles, paradigms, practices, and technologies to achieve privacy by design, i.e. to ensure privacy and increase personal control over one's information (Surden, 2007). Existing work on this topic targets software, hardware, and system. Smart cameras, i.e. surveillance cameras with advanced digital signal processors, can be programmed to mask a person's face or scramble a certain area in the captured video (Solove, 2006). The video data from smart cameras is split into two streams. The metadata stream describes the objects, events, behaviour, and other context information of the video, which is shown to the operator to fulfil surveillance purpose. The image stream containing the raw data can only be accessed by authorized personnel. Video analytics capabilities are developed to generate metadata that has the potential to eliminate the need to show raw video data to surveillance operators. To enforce privacy, video surveillance system is accompanied by multilevel access control architecture (Slobogin, 2002). Layered access model can be defined to ensure minimum-disclosure of information and the access to video data is on a need-to-know basis. Since video surveillance systems are comprised of computing and communication devices, standard and specific-purpose software, log management can be used to establish audit trail for accountability. Hence context-aware log generation, temper resistant storage, and intelligent log analysis are all topics related to the implementation of log management for accountability.

2.2 From the Industrial Side

From an industrial perspective, the building of video-surveillance systems is most of time based on the fulfilment of expressed customer technical requirements. It merely means that the degree of privacy and accountability provided by the system results from the applicable statements of law (and of any applicable authorization process) and from the prescriber requirements.

The status on this point about privacy and accountability enabling features for video-surveillance systems is to be found in three directions mainly: the security of data (that contributes to better privacy), the limitation of the collection of the data (very important contributor also to the privacy protection level of the whole system), and the features dedicated to evidence management.

A very important contributor to privacy clearly lies within the usage procedures that are enforced by the organization and operators who perform the routine surveillance tasks based on the video system (often using some other capabilities or features, such as those from Access Control Systems, Intrusion Detection Systems). One may notice that the three aforementioned categories are related to privacy rather than accountability. Very often in nowadays systems, accountability really arises mostly from organizational processes, whereas some technical capabilities might really help to increase accountability of surveillance systems.

The security of data is the most important and most focused point within video-surveillance real-life systems. First thing is to avoid unexpected and

unauthorized disclosure of video data, and second thing is to control and limit the possible actions of the operators strictly to the "need to know" attached to their missions. Avoid unauthorized disclosure often results from ISS (Information Security System) measures application: encryption of exchanges at network level, authentication of the cameras, high-grade authentication of the operator. It also results from physical access controls to the IT servers and operating stations of the system. In the most advanced video-surveillance systems, intrusion detection at the network level can be performed to avoid the stealing of any information. The limitation of the operators actions is performed using standard administration means to ensure differentiation of access to cameras, and access to live and/or replay video.

The limitation of the collection of the data results from two important (and different) video-surveillance features: the position of the CCTV cameras and the dynamic masking of privacy zones. The very first collection limitation factor clearly results from the position of the cameras itself: if no camera is positioned in my home, I'm sure I will not be filmed, otherwise… Some devices can also allow limitation of angular freedom of the sensor. In addition to this, the very nice dynamic masking is mostly provided in IP cameras (meaning within the most recent systems) and allows for protecting several zones in the image (they are blanked directly in the raw stream).

Also, when prosecution is at stake, protection and authentication of data is required. Modern video-surveillance systems propose technical features that allow for building a powerful and efficient electronic safe-box to embed video-surveillance gathered data.

Privacy is really taken into account in systems in operations. Nevertheless, it is most of the time within a non-global approach that results from disparate initiatives. A by-design approach would allow a more deterministic result, and also a better co-management of technical-related privacy and accountability enablers and of usage processes. At the end, some very simple to very innovative technical capabilities could be used to dramatically increase the privacy and accountability of the video-surveillance systems. A very common logging tool applied to operators' actions would, as an example, be the basis for a very powerful accountability system. Incoming homomorphic processing could also be used to realize video-content analysis (potentially realized everywhere, in the Cloud) without accessing the data.

3 SALT METHODOLOGY

The SALT methodology includes a system design process, which if followed, allows for the integration of privacy an accountability concerns within the surveillance system at early design stages, without diminishing the original functionality pursued by the given surveillance system. The diagram shown in Figure 1 depicts this general process.

As it can be seen, different actors are involved within the process depending on their role and the task they have to perform, ranging from the system proposer to the final system operator.

The system proposer is the actor who initially has the intention to deploy a surveillance system within a given context/environment. Therefore, the first thing to be done according to the SALT methodology is to apply a questionnaire (available at the SALT repository). The answers to this questionnaire help to assess the impact on privacy of the current SUD (System Under Development), providing information about the legitimacy of the system according to the current laws applicable to the context where the system is expected to be deployed.

If system is legitimate, we can go on with the process and collect the system requirements from the system proposer. These will mainly be functional requirements, although some privacy and/or accountability related requirements may also be included (they could be a counterpart of another requirement).

With this information and the context of the surveillance system, the SALT repository is accessed and the corresponding SALT references are retrieved. These SALT references provide relevant information regarding privacy and/or accountability requirements applicable to the SUD, and also a set of recommendations about how to address those requirements. By merging these recommendations with the previous system requirements, we get what we call the SALTed system requirements.

This is the initial input for system designers, who will also access the SALT repository searching for SALT references. In this case, the look for possible recommendations for the integration of solutions for the system requirements, as well as possible system restrictions, which may com from the legal, social, ethical or technological points of view. And not only this, a set of validation rules may also be available, allowing for checking whether the proposed SALT recommendations are met by the system design or not. As a consequence, thanks to all this information system designers create a system design.

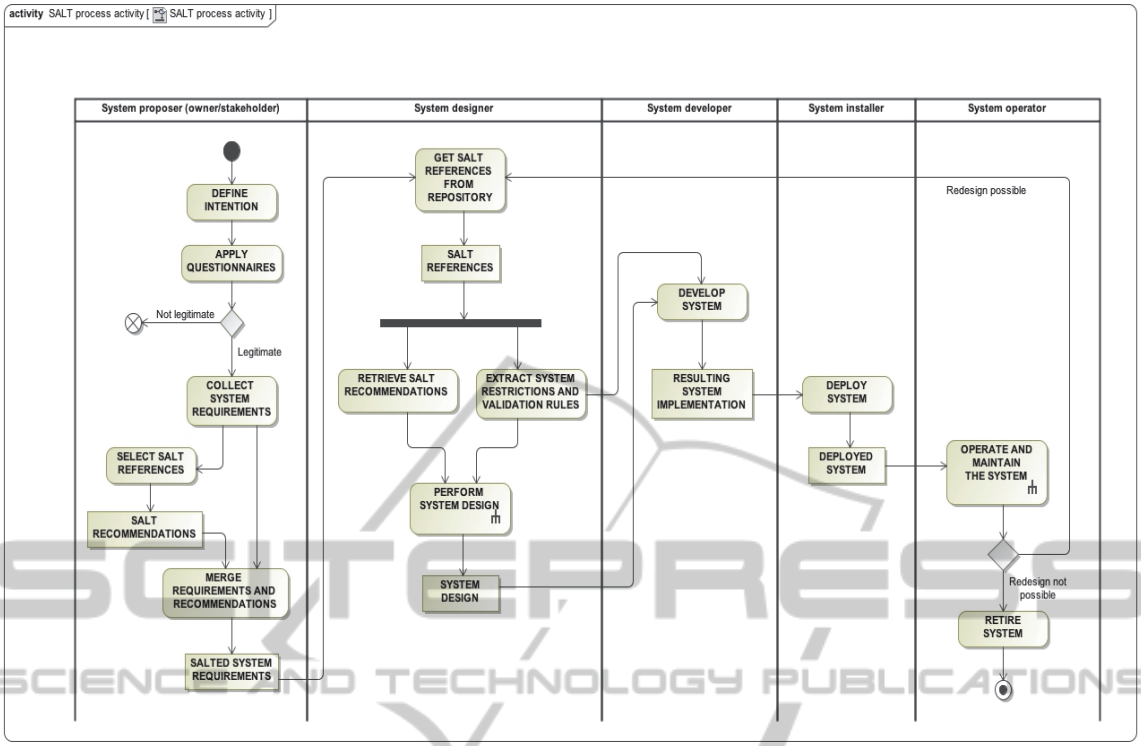

Figure 1: SALT methodology process diagram.

Next, system developers develop the system itself and provide an actual implementation. Then a system installer physically deploys the system and the system operator is able to work with it.

There is a feedback flow that considers the system maintenance and a possible system redesign in case some requirements have changed, e. g. an update of the applied laws.

4 SAMPLE USE-CASE

To demonstrate the application of the SALT framework, let us consider a use case of designing a distributed video archive search (VAS) system. The VAS system is supposed to search and analyse video surveillance data involved in suspected crime scenes. The video data are captured and stored in surveillance systems deployed at various geographic locations and operated by different organizations, e.g. banks, airport, public transport. Network Video Recorder (NVR) is used in these systems to store video image from multiple cameras. Video management system (VMS) is used to manage the access of operator stations to the video data in NVR. To be more efficient in protecting public security and combating crime, the law enforcement agency (LEA) wishes to use video search technologies to facilitate crime investigation. The LEA discusses its need and requirements with the technology provider and the surveillance system operators, in which it proposes to establish a project team for the design and development of an advanced VAS system that can access and search video data in various NVRs over the network. A high-level system overview is illustrated in Fig. 2.

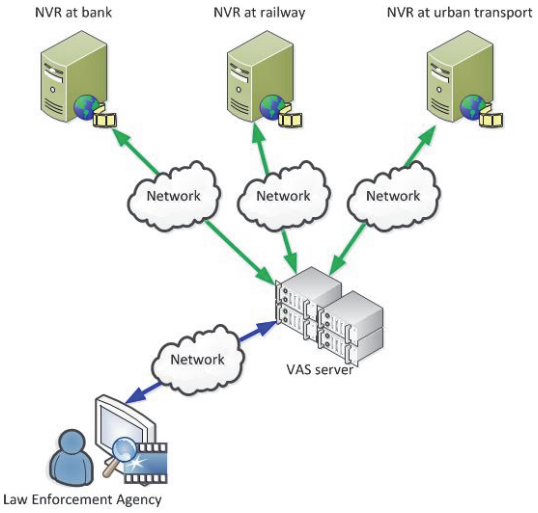

Figure 2: High-level view for VAS system use case.

The top priorities beside the surveillance need are to enforce privacy and accountability at all levels of the system design. The project team faces several challenges. First, beside technology, the project team must ensure that the VAS system complies with local privacy regulations and social norms. Second, the VAS system design must ensure that all privacy risks during the system runtime are identified in the design phase and properly addressed by technical and non-technical measures. Third, the system must address privacy and accountability issues while ensuring that the system is usable and the project stays within the time and budget constraints. Finally, the project must cover a broad range of interests, concerns, and requirements across multiple dimensions and find a win-win solution in the end, i.e. a system that increases security of the public while preserving privacy of the very same people.

5 SYSTEM DESIGN USING THE SALT APPROACH

If we follow a common design process, all functional (and some not functional) requirements of the SUD described in Section 3 are taken into account, which produces a system design that fully matches the desired way of operation of the resulting system. However, this approach does not take into account privacy and accountability requirements, at least from a dedicated perspective. This means that even though some privacy and/or accountability requirements may be met by the initial system design, some other can be (and will surely be) omitted.

This said, we need to clarify how is the system design going to be materialized. In general (and not only for this particular use case), the SALT methodology uses UML (Universal Modelling Language) as the way to produce one (or several) diagram for representing the system design. Figure 3 shows the initial system design (created through a common design process) for this particular use case.

Following we describe the elements depicted in Fig. 2:

- **Surveillance System:** represents the whole system. General attributes or methods applied to the system should appear in this element.
- **VMS:** represents the video management system. Access and processing of video data is performed through this element. It is composed of NVRs and cameras.
- **NVR:** represents network video recorders, which store the video data and are mostly located at the site of the surveillance cameras, which are used by. They have a name and hold arbitrary contact information.
- **Camera:** the camera object is used to identify surveillance camera tracks within a provider. It has a name as an ID, which is used as a reference to identify the correct track when the Video Archive Search
- accesses the provider to fetch the surveillance videos. Additionally, they hold the (physical) camera address as well as its coordinates. These shall make selecting cameras more convenient.
- **Algorithm:** algorithms used by the video archive search. It is very simple, it only consists of a human readable name and its ID. The ID is used by the VAS to identify the algorithm in its own system.
- **Database:** here is where information is stored.
- **Warrant:** the warrant is the central object of the access control system. It can be seen as a policy or authorization entry. This element represents the search warrant received from the judge or the direct authorization by the Data Protection Officer, depending on de applied legal framework. It consists of a name, the users, who re allowed to use this entry, and a time frame in which the warrant is valid.
- **Sensitive Data:** information used by the system susceptible of being attached to privacy and accountability concerns.
- **Permission:** a permission holds a combination of cameras with a shared time frame and algorithms, Within the system, it is seamlessly integrated into the warrant object, making it easier and more intuitive for the Data Protection Officer to use the administration interface.
- **User:** person who uses the system.
- **LEA:** law enforcement agency, such as police or alike.
- **Video Standard API:** system access API adapted to standard users.
- **Video Privileged API:** system access API for users with special privileges.

However, if we apply the SALT methodology instead, we end up using a set of questionnaires during a first stage of the process prior to the system design phase. The answers to these questionnaires help to identify privacy and accountability concerns that are applicable to the SUD. Besides, during the design time, the system designer can also access the SALT framework in order to search for new

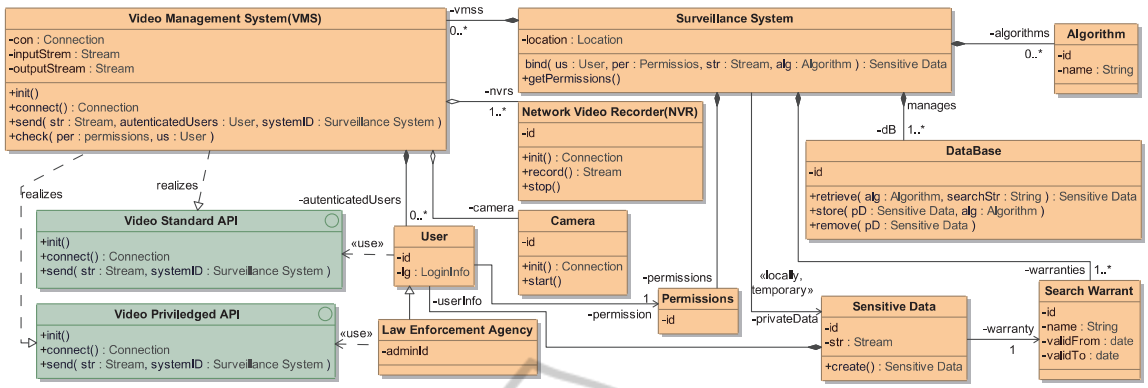

Figure 3: Initial design for VAS system use case.

requirements according to the SUD and the context where is going to be deployed. All this ensures having information related to privacy and accountability concerns at design time, which leads to a privacy-by-design and accountability-by-design approach. For the current use case described in Section 3, the following requirements have been identified:

- Clearly define the purpose of processing sensitive data, for which the evaluation of the stakeholder's problem is required.
- Indicate and justify the legal ground on which the implementation of the system relies (legitimacy).
- Justify the necessity and suitability of the system and the selected technologies for the defined purpose (proportionality).
- Data protection risk assessment, identifying the potential impacts on individual's rights.
- Transparency of the surveillance process.
- Description of the collected data, including the purposes of its collection and the target groups affected (nature of the collected data).
- Impact on privacy of the expected system accuracy and the errors that may occur (expected system accuracy).
- Description of the different users hat can have access to the data stored in the system, and justification of that access (limitation of access to data).
- Description of the circumstances in which the data can be transferred to third parties (disclosure of data).
- Whenever it is permitted to process data, it is preferred to avoid a centralized storage of the information (storage of data).
- Data collected and stored by the system should be properly protected (security of stored data).
- The retention duration of data should be carefully assessed. Data shall not be kept for longer than necessary to achieve the stated purpose(s). This implies that once data is not necessary anymore, it should be immediately deleted. Also, each retention' duration should be adapted to each category of data (retention and deletion of data).
- Data transmissions should be adequately protected in order to avoid unwanted disclosure of personal information (protection of data communications).
- The impact on privacy of a failure in the system components must be evaluated (privacy impact of system failures).
- It is important to identify the operations performed without any user interaction, and to implement the adequate mechanisms to control them in order to verify that they are working as expected (control of unattended operations).
- Inform data subjects about the process of data collection.
- Only the necessary data for the surveillance service should be collected.
- Trace all data collection processes.
- Implementation of compliance procedures and policies that respect the choice of the authorized persons, and the review and update of these policies at least every two years.
- The collected data is only used for the purposes for which they were initially recorded.
- Trace all data deletion processes.
- Deletion or rectification of inaccurate data.

Apart from the identification of the requirements above, the SALT framework also provides a possible way to deal with such requirements within

the design under development whenever it is possible. At this point, it is important to remark that there may be several different ways of dealing with each privacy/accountability concern, although a given SALT reference (the information unit within the SALT framework) provides just one possible implementation for each concern. Besides, there are some concerns whose definition is too vague and/or wide, thus making impossible to provide a 100% reliable solution for them. But even for these cases the SALT framework shows partial solutions that will help a human user (by providing extra information, limiting the number of elements to check, etc.) to verify whether a given concern is properly addressed within the system design or not.

Consequently, according to the information obtained from the SALT framework, the system design shown in Fig. 2 can be improved by specifically taking into account privacy and accountability concerns for this particular use case. This leads to a new system design, which can be seen in Figure 4.

These are the additions done in order to improve the VAS system design:

- **Purpose:** to describe and justify the purpose of the processing of sensitive data we extend de *Sensitive data* element with and attribute called "purpose" as a plain text string to include the evaluation of the stakeholders' problems.
- **Legitimacy:** the VAS system relies in a clear explanation and justification of the legal ground. To express that information we expand the *Surveillance system* element with the "legitimacy" attribute.
- **Proportionality:** for this aspect we use a new attribute called "proportionality" within the *Surveillance system* element.
- **Interference with Privacy Rights:** individuals' rights claim for a high level evaluation in order to verify and identify the potential impact. Therefore, we require a sensitive data risk assessment and we have to include specific operations to provide this functional requirement. This functionality is included in the *Surveillance system* element, in the method "identifyInterference()".
- **Nature of the Collected Data:** all processed sensitive data needs to be characterized, describing the purposes, goals and target groups affected by this data analysis. To contain this information we extend the *Sensitive data* element with the attribute "nature".
- **Expected System Accuracy:** the surveillance system has a specific degree of accuracy that has to be defined to indicate the impact on privacy. We include this information in a new attribute called "expected accuracy" in the *Surveillance system* element.
- **Access Limitation to Sensitive Data:** different users can have access to the sensitive data with several limitations, privileges and authorization levels. We manage these properties with the "authorization level" attribute within the *Permissions* element.
- **Disclosure of Personal Data:** sensitive data could be transmitted and shared among other users under specific circumstances. We have to strictly define them in the attribute "disclosure" in the *Sensitive data* element.
- **Sensitive Data Storage:** the method "protectionMethod()" included in *DataBase* element will take care of protecting sensitive data.
- **Retention and Deletion of Data:** the method "automaticDeletion()" within the *DataBase* element will handle the deletion of those sensitive elements whose retention period has expired.
- **Protection of Data Communications:** the "communicationsProtection()" method in the *Surveillance system* element should implement proper mechanisms intended to protect data communications.
- **Privacy Impact of System Failures:** the documentation of the privacy impact when the system fails is registered by the attribute "sf_privacy_impact" located within the *Surveillance system* element.
- **Control of Unattended Operations:** this issue is handled by two artefacts, both of them in the *Surveillance system* element. First, we have the "unattended_operations" attribute, which lists the operations carried out without a human interaction. Besides, the method "operationControl()" should define the control mechanisms for the operations identified in the previous attribute.
- **Inform Data Subjects:** there are no specific elements to address this requirement. System stakeholders should somehow make aware data subjects about the data collection process.
- **Minimization:** there is no way to guarantee that the system only collects the minimum and necessary sensitive data for the system purpose. However, the *Surveillance system* element is extended with the method

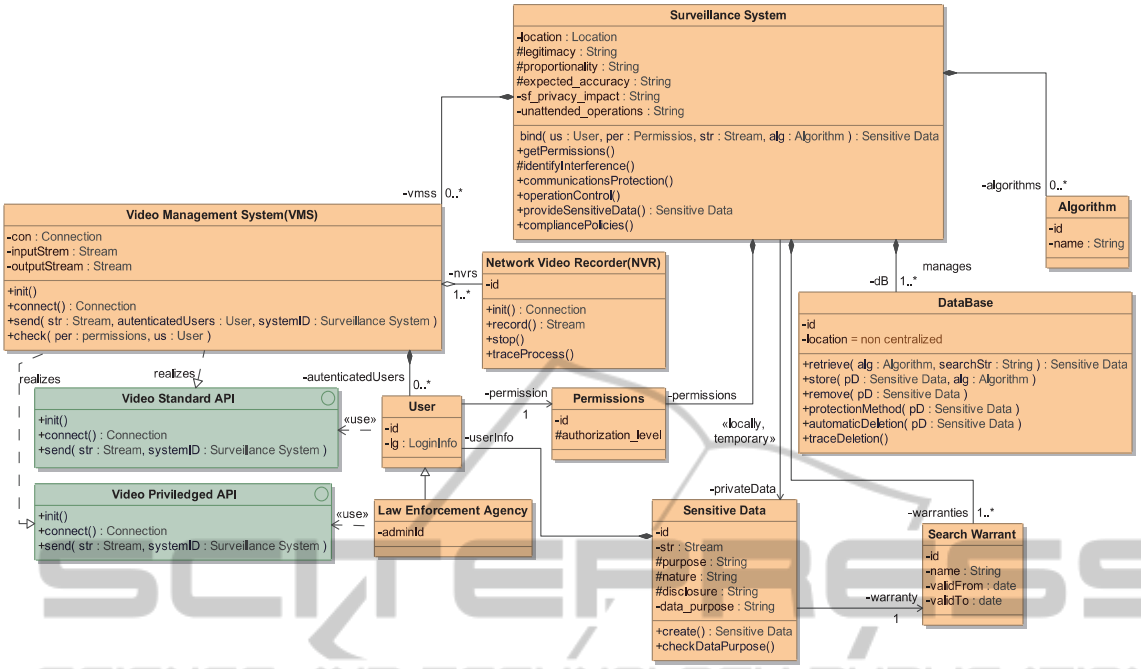

Figure 4: Final design for VAS system use case.

"provideSensitiveData()", which can help an external auditor to locate the data collected by the system and then check whether this data is really necessary or not.

- **Trace Data Collection Processes:** the *NVR* element includes another method called "traceProcess()" for this matter.
- **Compliance Procedures and Policies:** a method called "compliance_policies()" in the *Surveillance system* element will return those policies and procedures implemented, thus an external auditor will be able to access this information.
- **Use of Data according to its Initial Purpose:** the element *Sensitive Data* has an attribute called "data_purpose" for the system to know the purpose of each sensitive data recorded. Apart from that, the method "checkDataPurpose()", also within *Sensitive data*, is in charge of checking that the value of the "data_purpose" attribute matches the purpose of the surveillance system.
- **Trace Data Deletion:** inside *Data base*, the method "traceDeletion()" traces every time some data is deleted from the data base.
- **Deletion or Rectification of Inaccurate Data:** there is no way for the system to know whether the collected data is sufficiently accurate or not.

6 ADVANTAGES AND ACHIEVED GOALS

Even though current design and development processes for video-surveillance systems do not specifically address privacy and accountability requirements, some of them are covered thanks to the inherent characteristics and performance of the technology components or the design process itself. That is the case of smart cameras, which are able to apply blurring technologies to people faces, for example; or access control mechanisms, which only allow authorized personnel to operate privacy sensitive parts of the system.

However, surveillance systems designers are not usually supposed to know all privacy and accountability concerns that are applicable to the system under development (SUD). And even in the case they know about them, it may be difficult to devise how to apply these concerns to the SUD.

Here is where the SALT methodology (including the SALT framework, SALT process and the resulting toolset) comes in. It provides a way to help systems designers to develop privacy and accountability –aware systems. To achieve this goal, the SALT methodology counts on the SALT framework, which we can define as a set containing the privacy and accountability –related knowledge, obtained from experts in four main areas: social,

ethical, legal and technological. All this data are physically stored within a repository, which could be distributed over different locations.

The experts' knowledge within the repository is structured within smaller units called SALT references. Thanks to these references, systems designers will be able to identify and locate other privacy and accountability concerns concerning to their SUDs that are not addressed by current design processes. And not only that, together with the definitions of concerns, the references include possible ways of applying such concerns to a SUD (there may be several possible solutions, thus just one is provided in each reference for each concern). This is greatly convenient for systems designers: they will be able to know about the privacy concerns and also about a possible way to implement them.

Besides the repository, the SALT approach also includes a toolset that allows for different functionalities, such as managing the information within the repository (addition, retrieval), assistance to system design creation and automated validation of the privacy and accountability concerns applied to the system design (whenever it is possible).

How to use the SALT methodology, what tools are necessary and when, and for what purposes, are clarified by the SALT process. The SALT process is a guide for systems developers, which they can follow in order to provide a privacy and accountability –aware surveillance system. And even more, this process will also guide systems stakeholders and privacy experts in their relation with the SALT methodology and the surveillance system: how to add or update information into the repository, identification of new privacy and accountability requirements for the SUD, etc. However, these functionalities are out of the scope of this paper, which is mainly focused on the development of a particular use case and the advantages obtained thanks to the use of the SALT methodology.

7 CONCLUSIONS

The presentation and description of a particular use case based on a video archive search system is used to show how current design processes for surveillance systems do not properly take into account privacy and accountability related concerns, even though some of them may be accomplished as a collateral effect.

To alleviate this situation, the PARIS project proposes the SALT methodology. Thanks to a base of knowledge called the SALT framework and an application process, privacy and accountability requirements are identified at an early stage by system stakeholders. And not only that, system designers are also aware of such requirements at design time, thus achieving a privacy-by-design and an accountability-by-design approach.

The SALT methodology has been generally described, showing the process to follow in order to provide a privacy-aware system design, which will then be developed and physically deployed. Together with the identification of requirements for the SUD, the SALT framework also proposes possible (complete or partial) solutions to address such requirements. As a result, when following the SALT methodology, an improved system design is obtained, where privacy and accountability concerns are properly taken into account at design time.

ACKNOWLEDGEMENTS

Work partially supported by E.U. through the project PARIS (FP7-SEC 312504).

REFERENCES

Cavoukian, A., 2007. *Guidelines for the USE of Video Surveillance Cameras in Public Places.* Information and Privacy Commissioner of Ontario.

Rajpoot, Q. M., Jensen, C. D., 2014. Security and Privacy in Video Surveillance: Requirements and Challenges. In 29th IFIP TC 11 International Conference.

Castiglione, A., Cepparulo, M., De Santis, A., Palmieri, F., 2010. Towards a Lawfully Secure and Privacy Preserving Video Surveillance System. In *EC-Web 2010. LNBIP, vol. 61, pp. 73-84.* Springer, Heidelberg.

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, 23-51.*

Cavallaro, A., 2007. Privacy in video surveillance. *IEEE Signal Processing Magazine 24, 168-169.*

Surden, H., 2007. Structural Rights in Privacy. *SMU Law Review, Vol. 60, Issue 4, pp. 1605-1632.*

Solove, D. J., 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review. Vol. 154, Issue 3, pp. 477-564.*

Slobogin, C., 2002. *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity.* 72 MISS. L. J. 213-233.