

Privacy Enforcement in Surveillance Systems

H. Vagts^{1,2}, A. Bauer¹, T. Emter^{1,2}, J. Beyerer^{1,2}

¹Fraunhofer Institut für Informations- und Datenverarbeitung IITB,
Fraunhofer Str. 1,
76131 Karlsruhe, Germany

²Institut für Technische Anthropomatik (IFA),
Lehrstuhl für Interaktive Echtzeitsysteme,
Adenauerring 4,
76131 Karlsruhe, Germany

Surveillance Systems have become increasingly powerful. Conventional camera based Systems are extended with all kind of sensors (RFID, GPS, etc.), the number of data sources increases, hardware and algorithms improve, and data can potentially be shared between interlinked networks. The technological progress does not threaten solely the protection of privacy; it also provides an opportunity to achieve data and privacy protection on a new level.

In this work we propose privacy and security mechanisms to achieve data protection in surveillance systems while providing the best possible functionality. The suggested methods are included in an Object-Oriented World Model (OOWM) that serves as central information hub. It has been developed as a part of the semi-autonomous surveillance system NEST.

All member states of the European Union must obey the directive on the protection on personal data. Hence the suggested approach enforces mechanisms to be compliant with the directive that cannot be bypassed.

To allow flexible handling of data, the privacy concept for personal data is task-oriented and granular access controls are enforced according to the principle of least privilege. To ensure personal rights, an observed individual can request and access data collected about him. All data related to him can then be corrected or deleted on request with minimal influence to the surveillance tasks. To achieve non-repudiation all

changes in the world model are logged. This also helps to ensure data freshness.

The approach also aims at data minimization. A minimal amount of information is collected and irrelevant data are deleted as quickly as possible. Processed data are also minimized; i.e. only relevant objects, attributes, and prior knowledge are processed. Concluding, only relevant data is stored outside the world model. The persistent information is linked to the world model and appropriate access controls are enforced to realize multiple access levels.

Introduction

Privacy in smart surveillance systems is a recent area of research. Research efforts in smart surveillance have aimed at enhancement of efficiency and political efforts have pushed the deployment of sensors, basically video cameras. In the area of video surveillance some research concerning privacy has been done, for instance by Senior et. al. [4]. They propose a privacy enhancing console that processes the raw video stream and rerenders it. Regions of interest that contain privacy sensitive data (e. g. faces) can be blurred, or entire objects can be removed during the rendering process. Such abstraction is a promising approach, but is not adequate for modern surveillance systems that contain all kind of sensors. Hence privacy must be enforced on a higher level of abstraction. One part of the NEST architecture [1], is the Object-Oriented World Model (OOWM). Information about observed objects, delivered by all kind of sensors is merged at a high level, and all surveillance objects are stored in the OOWM.

The task-based approach of the NEST architecture and the OOWM can be used to achieve privacy on an unrivalled level. It is following shown in the following, how the *Fair Information Principles* can be adhered by smart surveillance systems.

The Fair Information Principles (FIP)

The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* serve as a rule for the EU directives on data protection (95/46/EC, 2002/58/EC), which must be enforced by the member states. The guidelines have been published by the OECD in 1980. Even if the legal situation concerning privacy and data protection should be the same throughout the EU, surveillance and data protection is handled differently in any state. The legal status in the US is also different [3]. The Guidelines contain eight principles for privacy, which should be considered by any legislation. Due to the inhomogeneous law, these principles can be considered as minimum

requirements. Scott McNealy, former CIO of SUN has said in 1999 - "You have zero privacy anyway. Get over It." This quotation is definitively not true, but points out that technology has advanced, modern achievements do not concern about privacy and collect a lot of data. To make things worse, many users do not care about privacy anymore and release personal data without hesitation (social networks, loyal shopping cards, etc.). There has been a shift in the sense of privacy, which is still ongoing. Hence some of the principles (P1, P4) should be called into question. Especially surveillance technology can bring anyone's privacy at risk, without getting noticed. The principles are shown in the following and it is noted, whether a principle should be challenged. Solutions that enforce privacy must deal with all principles, but must be flexible enough to adapt privacy according to future requirements.

- *Data Collection Limitation Principle* - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. (P1)

As mentioned above, it is questionable whether this principle can be kept in future. Data is going to be collected anyway; rather new methods for the protection of usage and lifetime are required.

- *Data Quality Principle* - Personal data should be relevant to the purposes for which they are to be used, should be accurate, complete and kept up-to-date. (P2)
- *Purpose Specification Principle* - The purposes for which personal data are collected should be specified not later than at the time of data collection. (P3)
- *Use Limitation Principle* - Personal data should not be disclosed made available or otherwise used for purposes other than those specified in accordance P3. Except, it is in consent of the data subject, or by the authority of law. (P4)

The purpose restriction is essential to guarantee privacy of a data subject, but similar to P1, it is difficult to control, and usage in another context might often be wanted by data operators. Hence, privacy enforcing methods are required to restrict the usage.

- *Security Safeguard Principle* - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. (P5)

- *Openness Principle (P6)* - There should be a general policy of openness about developments, practices and policies with respect to personal data.
- *Individual Participation Principle (P7)* - An individual should have the right to obtain confirmation of whether or not data relating to him has been collected. To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- *Accountability Principle (P8)* - A data controller should be accountable for complying with measures which give effect to the principles stated above.

In the following sections it is shown, how the eight principals (P1-P8) are handled in the NEST architecture. Security and Privacy are closely related (see P5) and besides these privacy requirements, security challenges exist that must be addressed by smart surveillance systems. A list of all identified key challenges can be found in [3].

A task-based Approach for Privacy Enforcement

Most surveillance systems still perform a *sensor-oriented* approach. In contrast the NEST architecture follows a *task-oriented* approach. Any usage of a resource and each processing step are assigned to a concrete surveillance task. The approach has two great advantages. On the one hand resources can be used more efficiently, e. g. if one specific person should be tracked in a central station. A task-oriented approach examines the entire scene including the requested person. A task-oriented approach monitors only the relevant person and ignores the others. On the other hand, the approach offers great possibilities for enhancement of privacy. It is required by law and the FIP (P3) that the purpose of a surveillance task is specified before the task is executed. If a task is specified strictly according to the purpose, a task-oriented System as NEST can ensure best possible privacy and data protection for the user subjects. As processing is task-related, person related data can be isolated in case of multiple surveillance tasks and privacy protection mechanism can be established very granularly according to the requirements of the task. Hence a task-oriented system is efficient and privacy-aware. One part of the NEST Architecture is the OOWM that acts as central data hub. To enforce privacy the OOWM is connected to a *Privacy Manager* (PM). Following an overview about the NEST Architecture is given and the interaction of the Privacy Manger and the OOWM is described. A detailed description of the OOWM can be found in [2].

Architecture for Privacy Enforcement

NEST is a service-oriented smart surveillance Systems [1] that allows the operator to specify surveillance tasks at semantic level. Fig. 1 shows all relevant parts for privacy enforcement. In the next section is shown how the components realize the eight principles named above. The OOWM acts as central data hub, hence privacy is enforced here. Any information that leaves the OOWM (dotted outer red line) is compliant to the applied privacy policies.

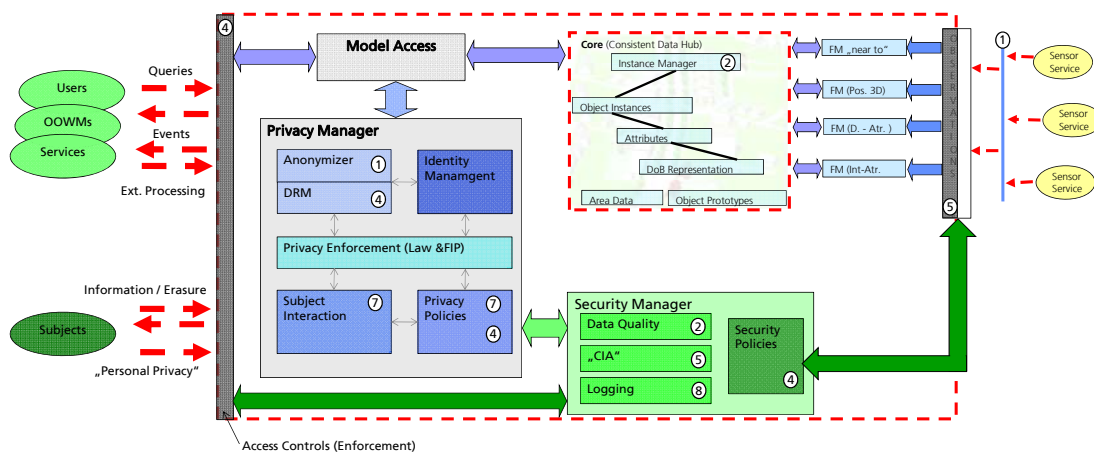


Fig. 1: The Privacy Manager and the Object-Oriented World Model

One of the core ideas of the NEST architecture is to alarm the system operator only in case of specific events. Contrary to obsolete deployments, the operator must not control the system continuously, and as the case may be, watch hundreds of monitors. Hence surveillance relevant data is extracted and decoupled from the raw sensor data and fused into the OOWM. Due to the service-oriented approach, sensors services can be integrated effortlessly, and sensor services can consist of multiple sensors.

Information is not only brought into the OOWM, it is also accessed by Users (authorized system operators), surveillance services, and other OOWMs (other surveillance systems). A user can either send a data query to the system to request specific information about a surveillance object, or can specify concrete events (e. g. abandoned baggage detection). Such events can be subscribed by all three actor groups. Services can also send queries to the OOWM, as well as other OOWMs. Services are required to fulfill surveillance tasks and can potentially perform actions on the objects in the OOWM. To extend the surveillance area multiple OOWMs can be connected and exchange data. In most cases only little information is exchanged with other OOWMs. OOWMs should be connected with caution, as it can result in extensive surveillance, which is forbidden by most legislations.

Besides, sensor services and the three actor groups, data subjects can also interact with the system to request personal data related to them (P7, see below).

The main component for Privacy Enforcement is the Privacy Manager. In fig. 1 each part of the NEST architecture is labeled with the number of the principle, it is relevant for. The functionality and interconnection of the modules inside the PM and *Security Manager* (SM) are highlighted in the next section. The PM intercepts the communication requests and responses, between the OOWM and the actor groups. Access is only granted to an actor; if it is required for fulfillment of a surveillance task (the actor is authorized). Furthermore only as few as possible information is released (see P1 and P4 below). All modules inside the PM are controlled by the *Privacy Enforcement Module*. Another central component is the *Identity Management Module* that manages all objects and their identities.

In addition, the *Task Manager* is also relevant to enforce privacy, it is not shown in fig. 1, but is also connected to OOWM, hence information about existing and planned tasks are present.

Achievement of the Fair Information Principles

Principle P3 and P6, can by definition not be achieved by the Privacy Manager. The purpose for which personal data is collected must be specified before the surveillance task is started. Most legislations require that the entire surveillance task (purpose) is specified before it is started. P6 cannot be achieved by the PM and SM as well. However, openness is important for trust in the surveillance systems. Information about the architecture, policies and operators must be easily accessible for data subjects.

Data Collection Limitation Principle (P1) - The collection of data is firstly minimized at sensor level, i. e. the sensor services (e. g. a multi camera tracker) only select the potentially required sensors for a surveillance task. As a result only potential relevant information is fused in the OOWM and the relation to a specific task exists right from the start. However, sensors can still deliver too much information (attributes of an object) for a specific surveillance task that is not required. Hence the *Anonymizer* removes irrelevant information before the response or event is sent back. The *Anonymizer* also uses *k-Anonymity* to enhance privacy for location based requests. Other methods can also be integrated focusing on other surveillance tasks. Hence the *Anonymizer* can be customized to achieve best possible privacy.

Data Quality Principle (P2) – Relevance of data is already achieved by the task-oriented approach used in P1. Data Quality is achieved by the *Data Quality*

Module (DQM) in the Security Manager, i. e. the DQM performs integrity checks of the existing data, especially if data has been altered by an external services. The OOWM core, more exactly, the Instance Manager is responsible for freshness and correctness of the instantiated objects (for details see [2]).

Use Limitation Principle (P4) – Use of data is restricted according to the surveillance task. Therefore accesses controls are enforced by the SM, access is granted to all involved services during the duration of the task, and such general *Security Policies* are stored in the Security Manager. To enhance privacy, more specific *Privacy Policies* can be specified that describe which attributes are accessible by particular services. A possible enhancement would be to deploy and remove these privacy policies according to the surveillance workflow, i. e. a service is only allowed to access data at a specific point in time. However, this may lead to complications in case of exceptions or other unforeseen activities, and hence requires more research.

Data should only be used in a specific context and only during execution of the corresponding task. Hence any information that leaves the World Model is coupled with digital rights. This is done by the *Digital Rights Management Module*. This is especially important, if data is exchanged between OOWMs. A service or OOWM must have the valid credential to process the requested data, e. g. if a credential has expired, the service or OOWM cannot process information of a subject and the credential must be requested again.

Security Safeguard Principle (P5) – a lot of video-specific approaches exist that try to achieve the standard security objectives: Confidentiality, Integrity and Availability (CIA). The OOWM deals with more abstract data, hence these approaches are useless, and established security mechanisms and protocols are used to achieve »basic security« in the NEST architecture. for instance, Certificates (PKI) or IPSec. Although, these methods are sufficient, but more specific security mechanisms would enhance efficiency. In [3] a *web of trust for surveillance sensors* is proposed to enhance trust in the authenticity of surveillance sensors. Hence only sensor services that are assumed to be trusted are allowed to deliver information into the OOWM.

Individual Participation Principle (P7) – Besides the general privacy policies mentioned above (P4), data subjects can also specify personal privacy policies, i. e. a data subject can find his personal trade-off between efficiency and privacy. For instance, information about a vehicle can be released voluntarily, to enable its monitoring in a parking garage. Naturally not all surveillance tasks (e.g. thievery protection) allow personalisation.

These personal policies must be brought into the system, hence the *Subject Interaction Module*, handles interaction between the data subject and the

surveillance system. This can be realized by personal assistants, which communicate with the OOWM, but other methods, as for instance terminals or pen and paper can be used as well. The interaction module also empowers user subjects to request the personal data related to them. They can induce erasure (if it is compliant with the surveillance task) or correction of their personal data.

Accounting principle (P8) – Any services performed by a module inside the OOWM, any external access by an actor and any data integration by a sensor is logged by the *Logging Module* inside the PM. If, for some reason, a violation of access rules occurs, the operator is notified about it. These logs are also stored and cannot be altered by the operator. Hence they can be used to proof proper processing of personal data.

Conclusion and Outlook

Data protection and privacy enforcement is one of the key challenges in modern surveillance. Systems become more and more powerful and usage of personal data or even any data must be restricted. The task-based approach of the NEST architecture allows privacy enforcement at an unrivaled level. Privacy mechanisms are located inside the OOWM and cannot be bypassed. It has been shown that the Privacy Manager and the Security Manager achieve adherence of the FIP. The abstract data representation in the OOWM allows efficient and privacy-aware processing of data.

Privacy in smart surveillance systems is a recent area of research and a lot of research must be done, for instance in the area of privacy policies and their deployment. Established security mechanisms can be used to achieve basic security but reach their limits in case of huge deployments or spontaneous interconnection for surveillance tasks. Hence further research in this area is also required.

- [1] A. Bauer, S. Eckel, T. Emter, A. Laubenheimer, E. Monari, J. Moßgraber and F. Reinert; NEST – Network Enabled Surveillance and Tracking ; Future Security 3rd Security Research Conference Karlsruhe; September 10th-11th; 2008
- [2] A. Bauer, T. Emter, H. Vagts, J. Beyerer. Object-Oriented World Model for Surveillance Systems, Future Security 4th Security Research Conference Karlsruhe; 2009
- [3] H. Vagts and J. Beyerer, Security and Privacy Challenges in modern Surveillance Systems, Future Security 4th Security Research Conference Karlsruhe; 2009

- [4] Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., Ekin, A.,Connell, J., Shu, C.F., Lu, M.: Enabling video privacy through computervision. *Security & Privacy, IEEE* 3(3) (May-June 2005) 50–57