

# Security and Privacy Challenges in modern Surveillance Systems

Hauke Vagts and Jürgen Beyerer

Fraunhofer Institute for Information and Data Processing IITB

Fraunhofer Str. 1, 76131 Karlsruhe

Karlsruhe Institute of Technology - Institute for Anthropomatics

Adenauerring 4, 76131 Karlsruhe

{vagts,beyerer}@iitb.fraunhofer.de

**Abstract**—This work identifies the security and privacy challenges for modern surveillance systems, which are closely related to existing and arising technology trends, and to the legal background. Important differences and similarities between the legal situation in continental Europe, the UK and the USA are therefore pointed out and changes to legislation that can enhance data protection in future surveillance systems are purposed. Modern installations are complex systems and existing mechanisms, methods from related research areas and new solutions must be combined to ensure security and privacy. Promising approaches are presented and it is shown why they are still insufficient. Finally solutions for privacy enforcement and secure sensor integration in the semi-autonomous surveillance system NEST, developed at the Fraunhofer IITB, are presented.

## I. INTRODUCTION

Many factors such as sinking prices, increased capabilities and 'the war on terror' lead to a growing number of surveillance installations. The major cause for deployment is crime prevention and most systems are still video based. Old installations are typically closed-circuit, have few (analog) cameras, poor viewing quality and do not assist the user. Modern installations are IP-based, can integrate a high number of cameras and assist the operator. Due to the trend for *interconnection* [1], *digitalization* [2] and *ubiquitous data acquisition* (RFID, Ubiquitous Computing, etc.), systems become not only more powerful and concurrently frightening, but also more vulnerable. To assure success of surveillance solutions security and privacy objectives must be achieved.

Video-based sensors are still the dominating data source in surveillance systems and many surveillance systems (cameras) have been deployed during the last years. Due to massive improvements in hardware, situation analysis and image recognition even old installations can become relatively "smart" and provide intelligent surveillance. Modern deployments provide even more potential for successful, i. e. task fulfilling, surveillance. The trends and factors mentioned above, have led to alarming surveillance possibilities. Major research efforts have been invested in enhancement of functionality and political efforts have increased the number of cameras. Similar to progress in other domains, security and privacy have been neglected and the abuse/misuse of modern surveillance systems has become issue. Analog installations can be secured by physical isolation and access controls.

Furthermore manipulation of the collected data is difficult, costly and hence not worthwhile in the most cases. To reduce deployment costs modern installations are integrated into an existing IT-infrastructure, which allows easy usage and data exchange. On the contrary, a surveillance system is opened for attacks on security and privacy. Malicious operators can relate personal data to other data sources with less effort.

### A. Surveillance in the UK

The United Kingdom is the best observed country, current estimations about installed cameras differ between one million and 4.2 millions [3] [4] [5], the real number is unknown. The guesstimated number of cameras in London is 500,000 [5], which equates a 14:1 ratio of inhabitants to cameras. In debates about surveillance, it is heavily cited that a citizen is watched by 300 cameras per day, the number may be true, but is a fiction as its creators G. Armstrong and C. Norris [6] say. Nevertheless it has become an 'urban legend' [7]. Even if these impressive numbers are estimated, an extreme tendency towards surveillance is undeniable.

Disregarding the political discussion about surveillance, it is a fact that old-fashioned surveillance systems are not practical to reduce or even prevent crime, or to fulfill other tasks, as it is shown by the following examples.

New York and London have populations of 8 and 7 million, respectively, and comparable police budgets, but the total crime rate of London has estimated about seven times those of New York [8]. New York has about 40% more police on the beat and spends less money on surveillance. Another example for inefficiency of video surveillance took place in 2005. To seek out a terrorist that has placed a bomb, more than 2,500 video tapes [9] have been watched.

By way of comparison, Germany has about 30,000 cameras in public places (estimated) [4] [10] and 400,000 in industrial spaces [4]. The "Deutsche Bahn AG" (operator of the public rail system) runs more than 2,800 cameras that are accessible from a security central in Berlin [11], thereof 150 cameras at the central station in Frankfurt and another 120 in Leipzig. Though the number of cameras in central stations as in Frankfurt is comparable to the UK, the overall numbers of cameras is still lower, but they are growing as in the rest of the world.

Huge deployments and inefficient analysis of data have augmented efforts for creation of smart (modern) surveillance systems and it is save to say that surveillance systems will become much smarter.

### B. Towards Smart Surveillance

The mentioned trends directly affect surveillance systems, affected technologies evolve at a high rate and smart systems provide an enormous potential for abuse. Modern systems can integrate, beside cameras, all kind of sensors and data sources, e.g. acoustic sensors [12], smell sensors, Biometrics, RFID, or GPS. The meshed application of such sensors facilitates ubiquitous data generation, and wireless techniques allow easy and cheap integration of mobile data sources. The increasing interconnection of anything simplifies the integration of external data sources (e.g. public or private data bases) and linkage with other surveillance deployment. In addition, overall quantity of available data has increased, all kind of information is digitalized and people give away personal information without considering the consequences (e.g. by using social networks, loyal shopping cards, etc.). Once information is released, it cannot be withdrawn. Methods for data mining and crawling also increase and storage is already cheap.

Besides ubiquitous data generation and interconnection, cameras and video processing also enhance. Hence, smart surveillance systems (e.g. [13][14][15]) evolve with the advancement of smart cameras (e.g. [16][17]), pattern recognition, multi-camera tracking, situation and video analytics and other related areas of research. (Meta-)Data must not merely be extracted, but rather be organized and accessed. This is especially relevant in smart surveillance systems that may generate a 'tangled data mess' that can not be handled [18]. In [19] Hampapur et. al. present a framework for searching surveillance video. Inhomogeneous sensors (different modalities), an increasing amount of information and data fusion at different levels of abstractions, require a more abstract representation. Hence, an *Object Oriented World Model* (OOWM) [20][21] is part of the NEST architectures, it handles data representation, organization and is easy to access. A review about other distributed surveillance systems can be found in [22].

### C. Arising Issues and Concerns

Smart surveillance deployments cannot be planed as isolated systems, hence security and privacy problems arise that have not been existent in analog systems. Digitalization brings up the problem of information persistence as well. Source material and surveillance meta data can easily be stored. Without unavoidable technical mechanisms, only law can prevent unauthorized usage and distribution of data and can be ignored by malicious users.

Digitalization, Interconnection, persistence of information and evolving techniques have not only an immediate effect on surveillance technology, but also on technology for civil security and it is conceivable that there will be no distinction between surveillance technology and 'every day life technology'. In a worst case scenario this can lead to total surveillance.

However, current trends and enhancements in technology cannot be ignored and the open privacy and security challenges must be solved to ensure data protection for everybody. Existing approaches are too focused on video and not comprehensive enough. In doing so, a holistic approach is necessary that considers the change in perception of privacy in the current and future information age. Hence, technology cannot be examined isolated, law and society must be considered as well to achieve an appropriate solution.

### D. Existing Privacy and Security Approaches

Privacy in surveillance is a recent area of research and new solutions are required. In the area of video surveillance some approaches exist to ensure privacy and security, most of the approaches blur *regions of interest* (RoI) that might imperil privacy. In [23] Senior et. al. purpose a "privacy-preserving console" for video surveillance. The console rerenders the video stream and hides sensitive details, detected by video analysis. Depending on the authorization level, access is granted to rerendered videos (e.g. with blurred faces or even enriched with additional information) or the raw video stream. They also purpose a "privacy cam", which processes the video sources and transmits encrypted information streams. In [24] Chattopadhyay and Bould also present a privacy cam, which is implemented on a Blackfin DSP and blurs RoI based on PICO [25]. Another scrambling approach is presented in [26]. In [27] Schiff et. al. propose a respectful camera which reacts on visual markers worn by the subjects. In [28] the usage of "talking cameras" is reported, if a camera detects motion, it sends an acoustic message to a subject. Even if such cameras should prevent vandalism, they can ensures privacy as well, e.g., a camera can count down vocalized, before it starts recording. Fleck's approach to privacy [16] is based on smart cameras, which transmit events instead of video data. Fidaleo et. al. present in [29] a privacy enhanced software architecture with a centralized server that hosts a privacy buffer, which can remove private or identifiable information from the stream. Schafer and Scharter propose in [30] a flexible secret sharing approach to enhance privacy.

Approaches for security also exist and just as in the area of privacy research the approaches are focused on video surveillance systems. One way to provide confidentiality, integrity and authenticity (CIA, e.g. [31]) in video surveillance systems is to use video independent solutions that have been proved to be successful, as symmetric and asymmetric encryption, signatures, certificates and public key infrastructures (PKI), and existing security protocols (SSL, IPSec, Kerberos, etc.). However, in case of video data more specific approaches have been proposed that take advantage of video characteristics. To ensure authenticity of images and video, a lot of research has been done in the area of (robust) watermarking, e.g. [32][33][34][35]. To achieve confidentiality of transmitted video data several approaches exist that achieve better performance by utilizing video characteristics, e.g. [36][37][38]. Even if cryptography and watermarking seem to be quite similar, key differences exist [39]. Watermarks are only an option to embed the result of a cryptographic calculation.

Beside [29] all existing approaches are focused on video-based sensors, which is insufficient for modern multi-sensor systems. Moreover the mentioned approaches do not consider law or social aspects. Especially in the matter of privacy, user acceptance and compliance with data protection and law is important. In the FP6 Project DEVYINE<sup>1</sup> a video surveillance system for civil security has been developed and some legal issues have been proposed [40]. In the EU project RRIME<sup>2</sup> privacy enhancing technologies (PETs) are analyzed with respect to legal conditions.

### E. Outline

The paper is organized as follows. First it is shown, why a holistic approach is required to achieve security and privacy in modern surveillance systems. Following the legal situation for surveillance is presented and potential changes for future law are proposed. Afterwards the identified key challenges for privacy and security are shown. Then an overview about existing approaches is given and our approaches for privacy and security are presented. Concluding our approaches are discussed.

## II. HOLISTIC APPROACH

To develop efficient (adequate for several specific surveillance tasks) and accepted surveillance technologies, a holistic approach for privacy and security is required that considers law and social aspects. Generally, technology improves at first and subsequently the real potential emerges, alarms society and is then limited by law. This "chain" has never been a good solution, and is also inadequate for surveillance technologies. On the one side, relevant technologies improve with great speed and the gap to areas as social networks or ubiquitous applications is closing. On the other side perception and assessment of privacy change (extensive use of Twitter, Facebook, etc.), and it is questionable, whether data protection will exist in future and if so, a change towards enhanced data preservation is probable. Beside law and technology, social acceptance is essential for surveillance technology. It has been shown (e.g. [41]) that security and the sense of security are deeply divided and that national differences exist in the acceptance of surveillance, e.g. 90% of the respondent people of a survey in London think video surveillance is a "good thing", while only 25% do so in Vienna [42]. However, estimation and reality disperse, especially in political discussions in the press. Surveillance must be more transparent to archive more confidence and balance weight against the asymmetric relationship of vision between data controllers and data subjects [42]. Observed subjects need easy ways to interact with the system (or control it).

However, a holistic approach is required that considers law and social acceptance from the beginning. To achieve a future-proof solution a control loop must be established between the three disciplines, such a solution must be efficient, easy to use and must provide unavoidable security and

privacy mechanisms. It must be assumed that the potential of surveillance technology is exploited, even if it is prohibited by law. Hence prohibition is insufficient, security and privacy compliant solutions must be available, affordable and easy to use, so that no appeal exists for purchasing and abusing an overpowered surveillance system.

It is important to consider social and legal changes that might happen or would do well and surveillance systems must follow realistic requirements. Technological enhancement does also provide new possibility to achieve social acceptance and even better privacy [43]. Information can be collected in a task-based manner (collection limitation), can be detached from raw sensor material [21], and can be organized and represented in a privacy-compliant way.

## III. LEGISLATION

Surveillance systems must adhere to legal restrictions and must be compliant with data protection requirements. Directives on the protection of personal data [44] [45] have been implemented by the European commission and must be enforced by member states. However, the legal situation in continental Europe and the UK is different and also depends on the surveillance task. To achieve social acceptance, compliance with data protection and achievement of security objectives must be transparent to all concerned parties

Data protection is not a new problem, already in 1973 the *Fair Information Practices Principles* (FIP) have been released and later in 1980 the OECD published an overworked version in the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" that contain eight privacy principles, which are still valid. They provide a base for modern data protection guidelines as the EU directives. The FIP implicitly demand IT security, as mechanisms are required to provide confidentiality and to enforce data protection. In addition systems must be secured against attacks on availability.

### A. Law in continental Europe, UK and USA

Though the EU directives must be enforced by every member state, the legal situation is slightly different within continental Europe and drastically different in the United Kingdom. Following the legal situation is described roughly. Germany is taken as an example state in continental Europe.

1) *Germany (Continental Europe)*: In Germany a *right to one's own picture* exists, i.e. in general a citizen can decide, whether a picture of him can be made publicly accessible, or not. In addition §6b and §9 with appendix of the BDSG handle data protection in publicly accessible places and IT Security in surveillance systems<sup>3</sup>. It is demanded that the surveillance task is specified before the surveillance is started and that an observed subject is informed about it. In publicly accessible places surveillance is allowed to enforce householder's rights or if it is of higher interest (for concrete reasons). Processing of data is only allowed, if it is necessary. In general the

<sup>1</sup><http://www.dyvine.eu/index>

<sup>2</sup><https://www.prime-project.eu/>

<sup>3</sup>Depending on the scenario other law must also be considered, e.g. employment legislation.

interference in privacy must be balanced against the interest of the operator, to decide whether surveillance is allowed. Reuse of data is only allowed to ensure public safety or to track a criminal act. As soon as data is not needed anymore, it must be deleted.

For obsolete surveillance systems the law is sufficient and the paragraphs are a good instance for a directive being implemented in respective law.

2) *United Kingdom*: The legal system in the UK is primarily based on *Common Law* and secondary based on *Statutory Law*, i. e. the Statutory Law is enforced by the interpretation of laws. No written constitution exists and the constitutional order is based on single laws. In contrast to other European states the right to one's own picture does not exist and until 1998 no rules existed for the use of video surveillance. In 1998 the *Data Protection Act 1998* has been established that follows the EU directives. The act contains a Code of Practice which is comparable to the regulations in German law. Inter alia, the task must be specified beforehand, as well as the operator and surveillance must be indicated. Data should be deleted, if it is not needed anymore and access to data must be restricted. An essential difference is that in the UK no difference exists between reconnaissance surveys and personal data.

However, the problem is that the protection act is not enforced strictly. A reason for a surveillance task must be given, but can be of a low priority. Operators decide by themselves, whether it is necessary to delete data. Video surveillance is promoted by the state and the *Crime and Disorder Act* allows the cooperation of surveillance deployments run by the municipality, private enterprises and the police. The established surveillance network is not even remotely comprehensible.

The following exaggerated quote by Williams and Johnstone [46], may describe the situation in the UK: "A CCTV system can be set up by anyone, there is no need for a license and the central government does not control the use to which it is put."

3) *United States of America*: In the USA no common regulation exists for validity of video surveillance, it depends on the *right of privacy* in each state. As surveillance is not regulated clearly, court decisions and jurisdiction turn the balance. In [47] Widen examines smart cameras and the right to privacy. It is said that the protection of privacy provides little restriction on the use of surveillance cameras by public or private actors. A general rule is that a camera may view and record activities in public space. Hence it is important, where the surveillance deployment and the observed subject are placed. Surveillance is only prohibited with safety, if it takes place on property of the subject. However, smart surveillance may change this dramatically. For instance, the rules for surveillance of conversations differ from those for video. If a smart system has potentially the ability to read lips, what may happen sometime in future, the legal situation changes completely.

Law has been made in respect of analog technology and has been overrun by recent technology and user behavior. It is not sufficient anymore due to two reasons. The first reason is the mentioned sense of privacy, which is currently in a

process of change and can give rise to new legislation. Second, the usage of existing PET and currently developing solutions for data representation, organization, anonymizing, etc., have not been considered in current law. Without considering PET some privacy challenges in intelligent video surveillance in regard to law are presented by Clouder and Dumortier in [40]. New surveillance approaches have the potential to enforce data protection and data security on an unrevealed level. However, the future of surveillance technology is not fully predictable and must be viewed in a holistic approach.

### B. Potential Adaptations

Law in surveillance is complex and even current legislation has not been fully explored. Manipulation of (video) sensor data becomes much easier and there has not been any case about it by now. "Simple" authenticity proofs (e. g. Kalagate certification, see below) performed for video storage recorders that provide authenticity for an entire surveillance system may become insufficient, if they are not already.

Considering the legal situations, trends and enhancing technologies, we propose research in the following areas, that may lead to changes in future legislation.

1) *Internationalization*: Future data protection and privacy law, must be international. In future, personal (surveillance) data will be exchanged between different countries, which is complicated when taking differing legislations into account. The law, as it is enforced in Continental Europe provides a much better privacy protection than the law in the UK, and the US law is somewhere between. However, it must be explored how much privacy is really wanted by the subjects and international rules must be established.

2) *Data collection and Minimization*: As it can be seen in the UK, surveillance networks are interconnected already. Data is collected and stored, and it is impossible to verify compliance with law in the incomprehensible network. Naturally this is not a desirable situation, but it must be considered whether the principle of data minimization and collection, respectively, can be held. Realistic law is required that allows task-fulfilling collection and ensures users privacy.

3) *Privacy Enhancing Technologies*: It must be explored, how PET can help to enforce privacy in smart surveillance. Especially, if the principle of data minimization is questionable. PET, new methods for data organization and representation provide an enormous potential and must be considered in future law for protection of privacy.

## IV. SECURITY AND PRIVACY CHALLENGES

This work highlights the *security and privacy challenges* that must be mastered in modern surveillance systems; seven key challenges exist, four for security and three for privacy. Complete *safety* challenges should be mentioned, which are not discussed here. There are open questions regarding exceptions, exception handling and the resulting security issues in surveillance systems. Research must also be done to answer questions concerning reliability, which includes reliability of (surveillance specific) events, system control data, data storage and Quality of Service.

Security and privacy cannot be seen isolated, it is rather complementary and an adequate solution must cover both. Exact requirements for future surveillance systems are uncertain, hence the holistic approach must be followed that covers tendencies and surveillance systems must be adaptable to specific surveillance scenarios, i.e. privacy and security guidelines must be adaptable to the circumstances and the surveillance task. Following the identified seven key challenges are described.

#### A. Security

As modern surveillance systems are distributed and IP-based, they face the same security issues as distributed systems (*Secure architecture*). Additionally other issues arise that result from the flexibility and size of modern surveillance systems (*Flexible Architecture and Trust*), the interconnection of surveillance systems and sharing of information (*Access Controls and Information flow*), and the trust of the users and validity in court, respectively (*Certification*).

1) *Secure Architecture*: Issues concerning IT security of surveillance architectures can be divided in three parts: *basic security*, *security in open networks* and *storage of sensor data*.

Basic security covers the established security objectives (CIA). First confidential communication, which is easy to ensure in a static architecture, but is complicated in case of prior unknown participants, or often changing users. However, in most cases the problems can be reduced to key exchange and deployment. Likewise, authenticity and integrity of exchanged messages and communication endpoints is also hard to achieve, if no common trust anchor is established. Availability of sensors and surveillance services can become difficult in large systems. If a high amount of data is transmitted, as in current video surveillance deployments, the existing bandwidth can become a limitation and result in availability problems.

Due to the integration of modern systems in existing infrastructure (open networks), hosts and services can easily fall victim of IP-based attacks, as Denial of Service (DoS), spoofing, replay attacks and so on. Attackers can either take advantage of vulnerabilities in underlying frameworks, protocol implementations, operating systems, etc. or can try to develop specialized attacks on specific surveillance architectures. At last, storage of sensor data and the linkage to the data processing modules is of higher interest. It must be guaranteed that person related data cannot be stolen or changed and it must be infeasible to prevent storing (authenticity, integrity, availability). Any access to the storage must be logged, and access to data must be granted according to the proper authorization level. For instance, if data is rendered before storing [23], some regions of interest are only accessible to authorized judges.

To provide security for a single component is manageable, but to provide security for an entire surveillance deployment is a difficult task, which becomes even more complex in huge or flexible (changing users, tasks or sensors) systems. To validate security properties and to build trust, deployments can be built by using an open architecture or by certification of the entire system.

2) *Certification*: Up to now, no appropriate certification for modern surveillance systems exist. There is no international standardization for certification of such systems. In the UK a system can be certified by the "Kalagate Imagery Bureau"<sup>4</sup>. Potentially the bureau can certify entire deployments, but no "smart system" has been certified so far. In current deployments, sensor data (often collected by analog cameras) is digitally stored and the bureau offers certification of components, as recorders. The certification verifies that data can be stored in a secure manner (encryption, quality, signature, etc.). The certification is accepted in the UK, i.e. video data gained from a certified and physically secured deployment, is accepted, if it is brought to court. The certificate is not accepted in the most countries, if it is known to judge, it might help to admit the video proof, but it is not guaranteed. In Germany, for instance, recorders can be also certified by "UVV-Kassen" (capacity, linkage between date and storage, availability, authenticity) which is intended for banking, or by "VdS" (integrability, safety). The latter is intended for safety equipment.

Even in current applications it is insufficient to certify only one component of a surveillance system. It is estimated that manipulation is very challenging and can also be identified by experts. Even if it is hard to gain access to the system, manipulation becomes easier and the first law case about the authenticity of video data is only a matter of time. At latest, if a component is placed in an open network, such a certification becomes meaningless.

For the certification of IT Security objectives the "Common Criteria"<sup>5</sup> (CC) are an established international standard. In the CC a Protection Profile (PP) can be specified for a specific IT component and a PP for "Software for processing personal image data" [48] exists that specifies physical, organizational and technical requirements for security and data protection. These requirements comply with many legislations, but certification of a single component is still insufficient.

To ensure functionality, video surveillance systems can be certified by the British "I-Lids" standard<sup>6</sup>. For instance, multi-camera tracking or event detection can be certified.

To sum it up, distributors only certify components. Certification is expensive, it is indefinite what should be certified and significance of certificates must be questioned. Up to now, distributors are not forced to certify entire systems, which consist of many components and resulting no statement about the security quality can be made. An affordable international certification for entire systems is required. Components from different distributors must be interoperable and system operators must be supported during deployment (selection of protocols, sensors, etc.). For instance, only "kappa" provides IP-cameras (on request) with a crypto chip and certificate and these cameras are too slow to digitally sign each frame. However, this shows that there has been no need for certification up to now.

3) *Access Controls and Information Flow*: Access controls must prevent unauthorized access to any information provided

<sup>4</sup><http://www.kalagate.co.uk/>

<sup>5</sup><http://www.commoncriteriaportal.org/>

<sup>6</sup><http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/video-based-detection-systems/>

by a surveillance system that includes access to raw data and meta data. Any access by a user or task must be granted according to least privilege, i. e. only data concerning a specific surveillance task or even subtask is accessible and access should only be provided as long as necessary. Dynamic allocation of authorizations is challenging in huge, flexible networks or if data is exchanged between surveillance systems. Hence any information must be linked to the task within it has been collected and as the case may be to a specific sensor. It must be ensured that data from different tasks cannot be combined and any forbidden information flow must be prevented. Beside access controls for data access, access controls for injection of sensor data must also be established.

4) *Flexible Architecture and Trust*: Trust in a flexible infrastructure, sensors, tasks and other components can not easily be achieved. Definition and evaluation of trust models is difficult and no sufficient model for a (multi-party) surveillance scenario exists. It is also an open question how existing systems must be extended to provide trust. Prior unknown partners, spontaneous interconnection and a changing number of sensors make it difficult to validate integrity and authenticity of the system state or specific sensors (insertion, removal). Using wireless sensors makes integration of sensors easier, but it must still be ensured that detected events and control data is reliably transmitted. Hence surveillance specific protocols are required. In our task-oriented surveillance architecture NEST, we have integrated the *plug and protect* principle. Plug and protect can be divided in a functional part (e.g. automatic sensor calibration) and a security part (trust in sensors), our approach, a *web of trust for surveillance sensors*, is described below.

## B. Privacy

Privacy is a philosophical term and everybody has its own definition of it. In terms of surveillance, the FIP provide minimum requirements and national law must be considered as well. However, the sense of privacy changes with the surveillance context (task) and over time. Hence systems must be adaptable to changing privacy requirements.

The Privacy challenges in surveillance are: *data protection*, *trust in surveillance* and *privacy-aware data exchange and communication*. To enforce data protection access controls are required to ensure least privilege for every activity. Similar, security mechanisms for data exchange are required to ensure privacy. Eavesdropping, even on encrypted communication, can compromise privacy.

1) *Data Protection*: Any surveillance task must be specified exactly and only data concerning this task must be generated and collected by the surveillance system. Hence any data must refer to its surveillance task(s). For applicable solutions access controls must be quickly adaptable (granting and prohibition) to new surveillance tasks, which includes their generation and enforcement.

The FIP require data minimization. In modern surveillance systems this can be divided in *minimization of data collection*, *data processing* and *data storing*. To minimize data collection, only required (as few as possible) sensors must be used and

irrelevant data must be deleted instantly (at sensor level). This prevents area-wide surveillance and the creation of movement profiles. To ensure privacy as few as possible of the collected data and prior knowledge must be processed (semantic level). If, for instance, an identified object is processed, only relevant attributes must be accessible. Again, non-useful data must be deleted instantly. In the end surveillance data is stored, which is also done in a data minimizing way. Only relevant events must be stored and only sensor data that is related to these events. The sensor data must be stored privacy-compliant, i. e. according to authorization levels, only a subset of the stored data is accessible. Access to stored data must be as granular as possible. All minimization principles helps to ensure privacy, however, it is uncertain, whether minimal data collection can be kept up in future. Privacy must still be protected and it is even more important to develop systems that permit usage of data in an unapproved context. Usage in another surveillance task or deployment can be legal and wanted, and must then be feasible, but only in a controlled manner (see Data Exchange).

Additionally, to be compliant with law, any observed subject can request information about the personal data related to him and can dispose correction or erasing, efforts of the operator do not matter. Finally every action must be logged to achieve non-repudiation.

Ensuring compliance with the FIP and privacy enforcement is the outstanding key challenge for modern surveillance. Deployments that are not aware of privacy will not be compliant with law and will not be accepted by the users (society). Modern systems have the potential to ensure privacy on an unrivaled level. Hence one component of the NEST architecture is the *Privacy Manager*, which is described below. A more detailed description about privacy in surveillance and the Privacy Manager can be found in [49].

2) *Data Exchange and Communication*: As mentioned above, data can potentially be used in another surveillance task, or for the same task in another surveillance system. To guarantee privacy, person related data must be secured against unauthorized usage. Lifetime and usage in surveillance tasks must be restricted. Hence a form of *digital rights* must be embedded in the surveillance data. In modern surveillance any kind personal information can be exchanged (video, location, relations, etc.) and can be fused in a new data type for surveillance. Hence digital rights for surveillance meta data are required.

It must also be ensured that eavesdropping, which is easily possible in open networks, does not affect privacy. An attacker might record data traffic and draw conclusions from it. He can search for regularities to identify specific events or observed objects. An attacker can also carry out "known-plaintext" attacks, i. e. he gets intentionally observed to force specific events. However, such profiling possibilities must be prevented. Sufficient encryption mechanisms and protocols must be chosen to apply privacy-aware confidentiality.

3) *Trust of the Surveillance Subjects*: For observed objects it must be comprehensible that their privacy is respected and person related data is protected. Trust in a system might follow irrational reasons and it cannot be said which mechanisms enhance trust in privacy. Openness of the system architecture

and certification of privacy-compliance seem to be adequate solutions. Functionality of surveillance system must be specified exactly and must be restricted to its purpose and technical mechanisms for privacy enforcement must be certified by a trusted instance.

“Control of controllers” and control of one’s personal data collected by the systems will also enhance trust in the surveillance system. To enhance trust, an observed object must be able to interact with the system. Personal devices can be used to interact, but it can not be assumed that any monitored object has a personal device. Hence new approaches are required.

## V. PROMISING APPROACHES AND SHORTCOMINGS

Previous privacy research for surveillance, has been focused on video surveillance. Nevertheless, the approaches named in section I-D can enhance privacy in this subarea of modern surveillance. The privacy-preserving console [23] proposed by Senior et. al. heads in the right direction. Smart surveillance requires solutions that ensure privacy on a higher level of abstraction, as the Privacy Manager. By now, no adequate solutions exist, but approaches in other areas might help to solve the challenges. To solve the data exchange challenge, DRM methods can be adapted, as also proposed in [50]. To specify privacy levels and to express privacy policies, existing languages, as for instance P3P<sup>7</sup> may serve as a model for surveillance specific privacy policy languages. Privacy research in the area of ubiquitous computing is also promising, e. g. the research done by Langheinrich [51], and can help to find appropriate solutions for user interaction and hence trust. Finally, methods for anonymization, as k-anonymity [52] or t-closeness [53] are also promising to achieve privacy in surveillance. As modern surveillance covers a broad range of technologies, many approaches must be combined to solve the privacy challenges.

## VI. PRIVACY AND SECURITY ENFORCEMENT

A modern surveillance system must consider all of the challenges that have been named above and the issues must be addressed right from the beginning—*security by design* and *privacy by design*. In case of surveillance both is recent research and innovative surveillance technology requires innovative security and privacy solutions.

### A. NEST Architecture

In the smart surveillance architecture NEST an operator specifies surveillance tasks. He must not observe a great number of monitors and other sensors, the system notifies him about events concerning his tasks (*management by exception*). A surveillance tasks can be, for instance, to guide a visitor from the reception to the meeting room. The operator tags the visitor during registration at the reception and is notified, if the visitor enters areas that should not be on his way to the room. NEST is a Service Oriented Architecture (SOA) and the operator can create any surveillance task by composing services, e. g. path finding or person tracking services.

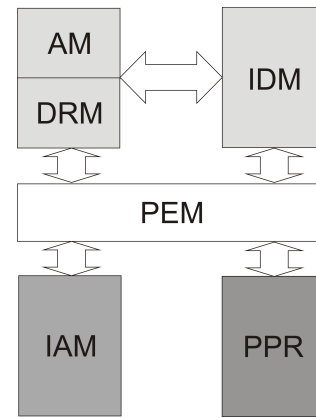


Fig. 1: Privacy Manager

Due to the flexible SOA design different sensor types can be integrated and a huge amount of data sources can be linked into the system. Any information is stored in the central Object Oriented World Model, it is extracted from the sensors and fused on a higher level of abstraction. Hence the OOWM is a good starting point to establish privacy and security.

Another unique characteristic of the NEST architecture is plug and protect. If a sensor is plugged into the network, it automatically registers in the surveillance deployment and transmits its configuration details. In an open-world scenario many sensors are not known beforehand, authenticity of sensors and trust in the corresponding data is challenge. In NEST a web of trust for surveillance sensors is established to build trust in the deployed sensors.

As shown above, many challenges exist and a lot of research must be done. In the NEST framework, we focus on the challenges that match the unique characteristics of the NEST architecture—Privacy and data protection via the Object Oriented World Model, SOA security for surveillance deployments and plug and protect. In the following the approaches for privacy enhancement and trust in surveillance sensors are presented.

### B. Privacy Manager

The Privacy Manager (PM) is described in the following, a more detailed description can be found in [43] and the architecture is shown in fig. 1. The PM is connected to the OOWM and ensures privacy compliant access to it. For surveillance tasks, it acts as a *privacy proxy*, a data request is send to the PM, which processes the request, decides whether it can be granted or not and finally releases privacy compliant data to the service. Besides a link to World Model, the PM is also linked to the task management system. This is required to grant task-based access to the World Model, which ensures access according to least privilege. The PM consists of the following components.

1) *Privacy Enforcement Module (PEM)*: The Privacy Enforcement Module is the central component, it receives and processes data requests, and hence controls all other modules. The privacy level can be adapted according to the the surveillance scenario. A privacy level is specified by privacy policies that are stored in the repository.

<sup>7</sup><http://www.w3.org/P3P/>

2) *Identity Management Module (IDM)*: Any object that is monitored must be identifiable to fulfill surveillance tasks. It can be distinguished between known person such as employees and unknown persons, e. g. customers. Attributes of known subjects easily become person related and must hence be treated differently than attributes of unknown people. However, the IDM manages the identities of all observed object and makes use of multiple roles (for each object) and relationships to enhance privacy and to separate identities for multiple surveillance tasks.

3) *Anonymization Module (AM)*: The AM is related to the IDM and ensures privacy conform access on information about objects. The AM enforces maximum privacy for different accesses by anonymization. If possible (depending on the surveillance task) location requests and attribute requests are anonymized. For instance, location based services are anonymized by grouping objects in the same area or by specification of privacy zones, in which no request about the exact location of an object is granted. In general as less as possible information (attributes) of an object should be provided to a service. Depending on the surveillance task, imprecision or intentional errors can be added intentionally.

4) *Digital Rights Management Module (DRM)*: Task of this Module is to attach digital rights to any information that is sent to a service or to another surveillance deployment (OOWM). This guarantees that data is only accessible during execution of a surveillance task or even just a subtask. Lifetime of data is restricted and data is only available for authorized services. However, even if the information flow can be controlled, services must be trusted. Once information has been observed, it might be reproduced and misused.

5) *Interaction Module (IAM)*: The IAM handles the interaction between an observed subject and the surveillance system. The subject can request personal data related to him and can induce correction or erasure. In some surveillance scenarios a subject can import his own policies. Different options for interaction with a surveillance system are imaginable, for instance: a personal device, a kiosk or simply pen and paper.

6) *Privacy Policy Repository (PPR)*: The PPR host privacy policies to ensure a certain level of privacy for the surveillance deployment. Policies concern one or more surveillance tasks (global policies) or can be user specific (personal policies). Global policies are enforced to achieve compliance with data data protection law and the FIP. By using personal policies the observed subject can specify a personal trade-off between functionality and privacy.

As shown in fig. 1, the PEM is the central component that controls all other modules and enforces privacy according to the policies in the repository. The IDM manages all identities of the objects in the World Model. Before information about an object is released, it is anonymized and digital rights are attached. Hence the DRM is connected to the AM and both interact directly with the IDM. The IAM handles user interaction that is enforced by the PEM, therefore the PEM modifies privacy policies or performs changes at world model.

### C. Security Manager (SM)

As mentioned, security is closely related to privacy. However, the SM manages cryptographic keys and certificates, ensures authenticity of service end points and confidentiality of transmitted data. This is realized by established cryptographic algorithms and IT security solutions. The SM also logs any (attempted) access to the world model. The security manager deploys and enforces the access controls derived from the privacy policies and security policies. The latter specify authorizations for services and resources that are not privacy related.

### D. Plug and Protect

One challenge for modern surveillance systems is the establishment of trust in unknown partners and sensors, even the authenticity of self-introduced sensors cannot always be ensured. Potential surveillance partners might not trust each other and establishment of a common root CA can be difficult. Hence, we propose a *web of trust* for building trust into surveillance sensors. The idea of a web of trust has been used in PGP<sup>8</sup> to establish trust in digital signatures. In the case of surveillance, a web of trust can be used to assign trust to known surveillance operators, which is used to calculate authenticity of sensors.

A surveillance system operator  $A$  collects public keys of other operators (parties) in his public key ring ( $K_{pub}^A$ ) and sets the *owner trust* for other surveillance system operators. He can set the trust to *complete*, if he has full confidence in an operator  $B$  and or to *marginal* in case of marginal trust. If  $A$  has given complete trust to  $B$ , he considers any sensor digitally signed by  $B$  to be authentic. In case of marginal trust, any sensor  $s_B$  signed by  $B$  is partly trusted, i. e. information gained by  $s_B$  is weighted less authentic. Another party  $C$  that is marginally trusted must sign  $s_B$  to achieve full authenticity of  $s_B$ . A sensor  $s$  is authentic, if  $A(s) = \frac{x(s)}{X} + \frac{y(s)}{Y} \geq 1$ ,  $x(s)$  denotes the marginal trusts and  $y(s)$  denotes the complete trusts for  $s$ .  $X$  and  $Y$  denote the number of required trusts to archive authenticity. If  $A(s) < 1$ , data received from  $s$  is not considered for surveillance tasks. As in PGP  $X = 2$  and  $Y = 1$  seem to be reasonable, but a surveillance operator can choose more restrict values. Optionally the information gained from  $s$ , can be weighted according  $A(s)$ .  $A$  can also establish direct trust in  $s$  by signing the sensor directly. To extend his web of trust  $A$  can specify *trusted introducers*. If  $B$  is a trusted introducer of  $A$ ,  $A$  trusts all operators  $b_i$ ,  $i \in \{1, \dots, n\}$ , trusted by  $B$  (marginal or complete).

Figure 2 shows a web of trust with 6 surveillance parties ( $A-F$ ).  $A$  has self-signed his own three sensors and one sensor run by  $C$ , hence they are all completely authentic.  $A$  has complete trust in  $B$  and resulting the sensor signed by  $B$  is also completely authentic.  $A$  marginally trusts  $C$  and  $D$ , hence in each domain one sensor is marginally authentic. The cumulative trust in  $C$  and  $D$  results in complete authenticity of one of the sensors operated by  $E$ . The other sensor is only signed by  $E$ ,  $A$  does not know  $E$ , hence this sensor is

<sup>8</sup><http://www.ietf.org/rfc/rfc4880.txt>

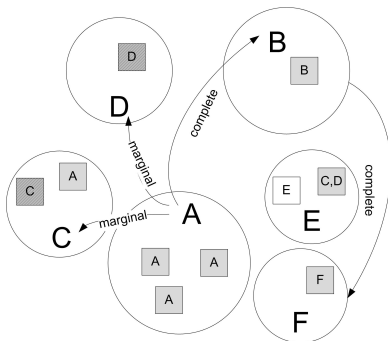


Fig. 2: Web of Trust for Surveillance Sensors

not authentic.  $B$  is a trusted introducer of  $A$ , thus the sensor operated by  $F$  is completely authentic.

However, the major issue of a web of trust is that operators could carelessly trust in other operators to get a huge network of authentic sensors, instead of having a smaller but trustable sensor network. The authenticity that is achieved by a web of trust reflects the trust in a sensor by the view of a system operator, it is not a qualified signature, i.e. data gained by trusted sensors must be authenticated additionally to guarantee that it can be used in court.

#### E. Integration in the NEST Test System

The Privacy Manager and Plug and Protect are currently integrated in a NEST prototype. To realize plug and protect a sensor registry has been implemented that serves as a repository for any information concerning the sensors. Services ask for information about sensors and can request access. As currently no real "smart sensor" exists on the market, they are simulated by sensors connected to personal computers. These smart sensors build the web of trust and register automatically at the sensor registry (of a surveillance operator). The public key ring is locally stored in the smart sensors and replicated at the sensor registry. The registry also contains the private key ring of an operator.

The Privacy Manager consists of the privacy modules mentioned above. For each module research must still be done to find future-proof solutions. Hence the manager is constructed modularly and methods can be exchanged. Each block is first implemented with basic functionality and then extended. Currently we focus on identity management for surveillance. The included privacy enhancing mechanisms should not only be applicable to surveillance scenarios. The privacy services can also be used in other scenarios and are easy to integrate due to the SOA approach. Experimental results will follow, when the integration is finished.

## VII. DISCUSSION

The Object Oriented World Model in the NEST architecture is a new approach for data representation in surveillance systems. The disjunction from the original sensor data provides a base for an abstract representation that allows fusion of multiple information sources. Whenever a request is sent to the OOWM by a surveillance task, the Privacy Manager

intercepts the query, checks the authorization and forwards the request to the OOWM. The OOWM delivers the response, the PM processes the data according to the privacy policies and then delivers the response to the requesting service. The service receives only data, which he is authorized to use and the response is also protected by digital rights. However, the PM generates a privacy-aware view for each surveillance task. The current legal situation for unintelligent surveillance has not been explored completely. Hence it is uncertain, whether abstract representation and privacy enhancing technologies will allow sharing and reuse of surveillance data by law, which would increase efficiency. It must also be explored, in what manner observed objects can interact with the system and how it enhances their trust in a surveillance deployments.

The proposed web of trust for surveillance sensors solves the challenge of confidence in surveillance sensors, but does not consider the quality of the information provided by the sensors. A lot of research has been done in the field of reputation system, and approaches, for instance, form peer-2-peer networks (e.g. [54]) or ad-hoc networks (e.g. [55]) may be applicable for surveillance.

The shown approaches enhance privacy and security in smart surveillance networks. For successful surveillance, i.e. for adequate task fulfilling and user accepted surveillance that is conform with regulations, all key challenges must be solved and research in privacy and security for surveillance must be done. Technology used in surveillance is also used in applications for civil security, hence the named trends (interconnection, digitalization, etc.) have also an impact there and it is important to develop privacy and security solutions. Eventually surveillance technology will merge with ubiquitous computing (Internet of things), social networks and other "Web 2.0" technologies. As released information cannot be withdrawn, insufficient data protection and security mechanisms will have inconceivable consequences. Evolution in surveillance will be depended on a future understanding of privacy and corresponding law and it can only be guesstimated what are requirements for prospective surveillance. Hence it is important that solutions are adaptable to different requirements.

## REFERENCES

- [1] European Commission Article 29 Working Party: Opinion 4/2004 on the processing of personal data by means of video surveillance. 11750/02/EN WP89 (February 2004)
- [2] Humer, S.: Digitale Identitäten. 1. edn. CSW-Verlag (April 2008)
- [3] Gras, M.: Kriminalprävention durch Videouberwachung. Gegenwart in Grossbritannien - Zukunft in Deutschland? Nomos Verlagsgesellschaft (2003)
- [4] Buellesfeld, D.: Polizeiliche Videouberwachung öffentlicher Strassen und Plätze zur Kriminalitätsvorsorge. Boorberg, R (2002)
- [5] Mccahill, M., Norris, C. In: Estimating the Extent, Sophistication and Legality of CCTV in London. Palgrave Macmillan, Basingstoke, Hampshire, England (2003)
- [6] Armstrong, G., Norris, C.: The Maximum Surveillance Society: The Rise of CCTV. 1. edn. Berg Publishers, Oxford (1999)
- [7] Töpfer, E.: Entgrenzte Raumkontrolle? Videoüberwachung im Neoliberalismus. In et al., V.E., ed.: Kontrollierte Urbanität. Zur Neoliberalisierung städtischer Sicherheitspolitik. transcript, Bielefeld (2007) 193–226
- [8] Colebatch, H.G.: Three strikes and you're ... in like flint. <http://spectator.org/archives/2006/04/10/three-strikes-and-youre-in-like-flint/> (last access 11.06.2009) (October 2006)

- [9] The Independent: Explosive used in bombs 'was of military origin'. <http://www.independent.co.uk/news/uk/crime/explosive-used-in-bombs-was-of-military-origin-498495.html> (last access 13.06.2009) (July 2005)
- [10] Buse, U., Schnibben, C.: der nackte Unterraum. Der Spiegel (July 1999)
- [11] Töpfer, E.: Jeden Bahnhof erfassen. <http://www.heise.de/tp/r4/artikel/20/20832/1.html> (last access 13.06.2009) (August 2005)
- [12] B Lo, J. Sun, S.V.: Fusing visual and audio information in a distributed intelligent surveillance system for public transport systems. *Acta Automatica Sinica* **29**(3) (2009) 393–407
- [13] Hampapur, A., Brown, L., Connell, J., Ekin, A., Haas, N., Lu, M., Merkl, H., Pankanti, S.: Smart video surveillance: exploring the concept of multiscale spatiotemporal tracking. *Signal Processing Magazine, IEEE* **22**(2) (March 2005) 38–51
- [14] Bauer, A., Eckel, S., Emter, T., Laubenheimer, A., Monari, E., Mossgraber, J., Reinert, F.: N.E.S.T. - Network Enabled Surveillance and Tracking. In Thoma, K., ed.: *Future security: 3rd Security Research Conference, Fraunhofer IRB Verlag* (September 2008) 349–353
- [15] J-L Bruyelle, L Kuhoudour, D.A.T.L.A.F.: A distributed multi-sensor surveillance system for public transport applications. In: *Intelligent Distributed Video Surveillance Systems. The Institution of Electrical Engineers* (2006) 185–224
- [16] Fleck, S., Strasser, W.: Smart camera based monitoring system and its application to assisted living. *Proceedings of the IEEE* **96**(10) (Oct. 2008) 1698–1714
- [17] Bramberger, M., Doblander, A., Maier, A., Rinner, B., Schwabach, H.: Distributed embedded smart cameras for surveillance applications. *Computer* **39**(2) (Feb. 2006) 68–75
- [18] Limbach, J.: 25 Jahre Bundesdatenschutz. In the celebration of 25 years of "Bundesdatenschutz" (June 2002)
- [19] Hampapur, A., Brown, L., Feris, R., Senior, A., Shu, C.F., Tian, Y., Zhai, Y., Lu, M.: Searching surveillance video. *Advanced Video and Signal Based Surveillance, 2007. AVSS 2007. IEEE Conference on Industrial special session* (Sept. 2007) 75–80
- [20] Emter, T., Gheta, I., Beyerer, J.: Object oriented environment model for video surveillance systems. In Thoma, K., ed.: *Future security: 3rd Security Research Conference, Fraunhofer IRB Verlag* (September 2008) 315–320
- [21] Bauer, A., Emter, T., Vagts, H., Beyerer, J.: Object oriented world model for surveillance systems. In: *Future security: 4rd Security Research Conference, Fraunhofer IRB Verlag* (2009)
- [22] Valera, M., Velastin, S.: Intelligent distributed surveillance systems: a review. *Vision, Image and Signal Processing, IEE Proceedings -* **152**(2) (April 2005) 192–204
- [23] Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., Ekin, A., Connell, J., Shu, C.F., Lu, M.: Enabling video privacy through computer vision. *Security & Privacy, IEEE* **3**(3) (May-June 2005) 50–57
- [24] Chattopadhyay, A., Boulton, T.E.: Privacycam: a privacy preserving camera using uclinux on the blackfin dsp. In: *CVPR, IEEE Computer Society* (2007)
- [25] Boulton, T.: Pico: Privacy through invertible cryptographic obscuration. (Nov. 2005) 27–38
- [26] Dufaux, F., Ebrahimi, T.: Scrambling for video surveillance with privacy. *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06. Conference on* (June 2006) 160–160
- [27] Schiff, J., Meingast, M., Mulligan, D., Sastry, S., Goldberg, K.: Respectful cameras: detecting visual markers in real-time to address privacy concerns. *Intelligent Robots and Systems, 2007. IROS 2007. IEEE/RSJ International Conference on* (29 2007-Nov. 2 2007) 971–978
- [28] Associated Press: Talking camera tackles city crime. <http://www.cbsnews.com/stories/2005/11/17/tech/main1054526.shtml> (last access 15.06.09) (November 2005)
- [29] Fidaleo, D.A., Nguyen, H.A., Trivedi, M.: The networked sensor tapestry (nest): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks. In: *VSSN '04: Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks*, New York, NY, USA, ACM (2004) 46–53
- [30] Schaffer, M., Schartner, P.: Video surveillance: A distributed approach to protect privacy (2005)
- [31] Dzung, D., Naedele, M., Von Hoff, T., Crevatin, M.: Security for industrial communication systems. *Proceedings of the IEEE* **93**(6) (June 2005) 1152–1177
- [32] Du, R., Fridrich, J.: Lossless authentication of mpeg-2 video. In: *Image Processing, 2002. Proceedings. 2002 International Conference on. Volume 2.* (2002) II–893–II–896 vol.2
- [33] Tzeng, C.H., Tsai, W.H.: A new technique for authentication of image/video for multimedia applications. In: *MM&#38;Sec '01: Proceedings of the 2001 workshop on Multimedia and security*, New York, NY, USA, ACM (2001) 23–26
- [34] Mobasser, B., Sieffert, M., Simard, R.: Content authentication and tamper detection in digital video. **1** (2000) 458–461 vol.1
- [35] Guo, Q., Liu, Z., Liu, S.: Robustness analysis of image watermarking based on discrete fractional random transform. *Optical Engineering* **47**(5) (2008) 057003
- [36] Li, Y., Cai, M.: H.264-based multiple security levels net video encryption scheme. In: *Electronic Computer Technology, 2009 International Conference on.* (Feb. 2009) 8–11
- [37] Chattopadhyay, T., Pal, A.: Two fold video encryption technique applicable to h.264 avc. In: *Advance Computing Conference, 2009. IACC 2009. IEEE International.* (March 2009) 785–789
- [38] Raju, C., Umadevi, G., Srinathan, K., Jawahar, C.: Fast and secure real-time video encryption. In: *Computer Vision, Graphics & Image Processing, 2008. ICVGIP '08. Sixth Indian Conference on.* (Dec. 2008) 257–264
- [39] Cox, I.J., Doerr, G., Furon, T.: Watermarking Is Not Cryptography. (2006)
- [40] Coudert, F., Dumortier, J.: Intelligent video surveillance networks: Data protection challenges. Availability, Reliability and Security, *International Conference on* **0** (2008) 975–981
- [41] Zurawski, N., Czerwinski, S.: Crime, maps and meaning: Views from a survey on safety and cctv in germany. *Surveillance & Society* **5**(1) (2008) 51–72
- [42] Hempel, L., Töpfer, E.: CCTV in Europe. Final Report, Urbaneye Working Paper No. 15 (August 2004)
- [43] Vagts, H., Bauer, A., Emter, T., Beyerer, J.: Privacy enforcement in surveillance systems. In: *Future security: 4rd Security Research Conference.* (2009)
- [44] European Parliament and Council: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) . *Official Journal of the European Communities* **L 201** (July 2002) 37–47
- [45] European Parliament and the Council: 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. *Official Journal of the European Communities* **L 281** (Oktober 1995) 31ff
- [46] Williams, K.S., Johnstone, C.: The politics of selective gaze: Closed circuit television and the policing of public space. In: *Crime, Law & Social Change.* (2000) 194, ff.
- [47] Widen, W.: Smart cameras and the right to privacy. *Proceedings of the IEEE* **96**(10) (Oct. 2008) 1688–1697
- [48] The Federal Commissioner for Data Protection and Freedom of Information (BSI): Common Criteria Protection Profile (PP) Software for processing personal image data (February 2008)
- [49] Vagts, H., Beyerer, J.: Security and privacy challenges in modern surveillance systems. In: *Future security: 4rd Security Research Conference.* (2009)
- [50] Serpanos, D., Papalambrou, A.: Security and privacy in distributed smart cameras. *Proceedings of the IEEE* **96**(10) (Oct. 2008) 1678–1687
- [51] Langheinrich, M.: Personal Privacy in Ubiquitous Computing – Tools and System Support. PhD thesis, ETH Zurich, Zurich, Switzerland (May 2005)
- [52] Sweeney, L.: k-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness, and knowledge-based systems* (2002)
- [53] Li, N., Li, T., Venkatasubramanian, S.: t-closeness: Privacy beyond k-anonymity and l-diversity. In: *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on.* (April 2007) 106–115
- [54] Xu, Z., He, Y., Deng, L.: A multilevel reputation system for peer-to-peer networks. In: *Grid and Cooperative Computing, 2007. GCC 2007. Sixth International Conference on.* (Aug. 2007) 67–74
- [55] Michiardi, P., Molva, R.: Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, Deventer, The Netherlands, The Netherlands, Kluwer, B.V.* (2002) 107–121