Privacy-preserving surveillance: an interdisciplinary approach

Pascal Birnstill*, Sebastian Bretthauer**, Simon Greiner***, and Erik Krempel****

Introduction

Intelligent video surveillance is an active and lively field of research, predominantly in the domains of image exploitation and situation assessment. The availability of privacy-invasive system functionality such as real-time object tracking and automatic extraction of biometric features is becoming reality. Not surprisingly, video surveillance generates an increasing interest among information security and privacy researchers.

A categorical argument against video surveillance targets the chilling effect of such systems, which arguably is in conflict with the fundamental right to free development of the individual. When faced with surveillance cameras, we cannot know whether we are currently observed or not. However, the mere possibility of being observed tends to change the way we behave, which usually is considered an undesired phenomenon in free societies and therefore addressed by legislation. The principle of proportionality, as laid down in Articles 8(2) and 52(1) of the Charter of Fundamental Rights of the European Union, demands a careful weighing of the purpose of a surveillance measure, ie, the legally protected interest to be defended, against the legitimate interests of people affected by the surveillance measure. However, we do observe that video surveillance is spreading rapidly, even though the proportionality of privacy invasion and utility may not always be justified.

In addition, even if we consider video surveillance to be necessary in particular cases, the question of how and to which extent privacy of the people concerned can be preserved must be evaluated.

Given that modern video surveillance technology works at the level of abstracted objects rather than raw video streams, we argue that the computer vision capabilities of such systems can also be exploited for improving the selectiveness of surveillance measures. Intelligent video surveillance systems are capable of fusing information extracted from video streams into abstracted objects, including attributes such as IDs by face recognition, location, or certain activities. Hence, we can analogously incorporate an authentication mechanism as an information source, which enables the system to determine (group) identities of people who are a priori known to be concerned by the surveillance measure, eg, employees of an airport as an environment,

Key Points

- Increasing capabilities of intelligent video surveillance systems impose new threats to privacy while, at the same time, offering opportunities for reducing the privacy invasiveness of surveillance measures as well as their selectivity.
- We show that aggregating more data about observed people can increase the selectivity of surveillance measures.
- In the case of video surveillance in a company environment, if we enable the system to authenticate employees and to know their current positions, we can ensure that no data about employees leave the surveillance system, ie, it is being visualized or made accessible to an operator.
- We discuss the legal implications of such a system with regard to German as well as European data protection law.
- Some weaknesses of § 6b BDSG (the German Federal Data Protection Act) concerning intelligent video surveillance are identified.

* Pascal Birnstill is with the Department of Secure Communication Architectures, Fraunhofer Institute of Optronics, System Technologies and Image Exploration IOSB, Karlsruhe, Germany.

** Sebastian Bretthauer is with the Center for Applied Legal Studies (ZAR), Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany.

*** Simon Greiner is associated with Institute of Theoretical Informatics, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany.

**** Erik Krempel is with the Department Secure Communication Architectures, Fraunhofer Institute of Optronics, System Technologies and Image Exploration IOSB, Karlsruhe, Germany.

which is typically equipped with extensive surveillance facilities. If we furthermore assume that the airport operating company trusts in its employees while air passengers should be observed for the sake of civil security, being able to distinguish between airport personnel and air passengers, the system can actively apply privacy-preserving mechanisms on person objects recognized as employees. Such privacy-preserving mechanisms may be applied to video stream visualization (eg blurring faces of employees) as well as to abstracted views (eg hiding or coarsening positions of employees on an overview map). By this means, we can improve the selectivity of surveillance measures, ie, employees who have to spend their whole work day in an area under video surveillance can to some extent be relieved from the pressure of video surveillance, while air passengers are being observed as required by the security task.

As stated above, this ability to enforce privacy-preserving mechanisms on particular groups comes at the cost of collecting additional data. In this paper, we investigate how to design modern video surveillance systems that collect certain kinds of data, which are only processed for the benefit of privacy. In particular, we have the paradoxical situation that tracking, which usually is considered to be privacy-invasive, is necessary for protecting privacy. We denote this finding as *tracking paradox*. In this work, we analyse the tracking paradox with respect to its technical and legal implications. Bigger parts of the technical investigations presented in the following have already been published in an invited paper at *Future Security 2013*. By now, this technical work has been complemented and enriched with an analysis of its legal implications.

From a technical perspective, we investigate how such an intelligent video surveillance system processes data. Using methods from formal software verification, we show that it is possible to implement a surveillance system, which collects and processes data about employees, while ensuring that no such data leave the system core, ie, the data can be accessed or analysed by an operator. For this, we provide a prototypical implementation of the module of a surveillance system, which is responsible for processing feature vectors and merging observations with previously observed objects. Using JML[1] annotation within the source code, we specify under which circumstances and in which granularity the module may expose information to the environment. We then apply the KeY tool[2] on our implementation in order to prove the non-existence of information flow, apart from those explicitly specified. By this means we show that it is feasible to prove that at most the specified information is revealed to the environment, while further information about employees is kept secret.

Concentrating on European and German data protection law we discuss the legal implications of a system according to our approach. All data protection regulations aim to protect the right of informational self-determination through a balancing of interests according to law. Insofar the regulations demand a careful consideration of the interests in carrying out a surveillance measure.

In Europe, *the Directive 95/46/EC on protection of individuals with regard of the processing of personal data and on the free movement of such data*[3] does not contain an explicit norm concerning video surveillance. The proposal for a *General Data Protection Regulation*[4] demands a so-called *Data Protection Impact Assessment.*[5] It stipulates that whenever processing operations pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope, or their purposes, the controller or processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations regarding the protection of personal data. As referred to in paragraph 1, this explicitly applies for monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale.

Germany, as an example within the European member states, has different sets of legal norms applicable to video surveillance. Section (§) 6b of the Federal Data Protection Act (BDSG)[6] is the main norm regulating monitoring of publicly accessible areas with optic-electronic devices. Additional regulations can be found in the federal law (eg §§28, 29, 32 I 2 BDSG), the federal state law (eg §20 a LDSG BW[7] or in area specific acts (eg §§26, 27 BPolG).[8] We focus on §6b BDSG as the

1 Gary T Leavens, Albert L Baker, and Clyde Ruby. 'Preliminary Design of JML: a Behavioral Interface Specification Language for JAVA' (2006) 31 SIGSOFT Softw Eng Notes 1–38.

2 Bernhard Beckert, Reiner Hähnle, and Peter H Schmitt (eds) *Verification of Object-Oriented Software: The KeY Approach*, LNCS vol. 4334 (Springer, Berlin, Germany 2007).

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on 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. No L 281/31.

4 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

5 Id., Article 33. See also David Wright and Paul De Hert, Privacy Impact Assessment, vol. 6 (Springer Science & Business Media, 2011).

6 Simitis, Spiros. BDSG, 7. Aufl. Baden-Baden, 2011.

7 Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz—LDSG) Baden Württemberg, <http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=DSG+BW&psml=bsbawueprod.psml&max=true>, 2000.

8 Gesetz über die Bundespolizei (BPolG), <http://www.gesetze-im-internet.de/bgsg_1994/>, 1994.

German Data Protection Law is generally considered to offer a high standard of data protection.

Related work

We concentrate on work on privacy policy enforcement in video surveillance systems, since our work is orthogonal to privacy-enhancing computer vision techniques, ie, privacy-enhancing technologies for surveillance camera's video streams.

In the article by Senior and others,[9] the authors introduce a privacy-preserving video console for hiding sensitive details in video streams depending on authorization levels. This suggests that the privacy level of exposed video data should be adjusted exclusively to the authorization level of the observer, as opposed to the authorization level induced by the surveillance purpose or by (groups of) observed persons.

Wickrasamuriya and others[10] enforce privacy policies for video re-rendering. Video scenes are not shown directly to the observer but rendered according to the observers' access rights. So, he might see a rendered scene where no persons are included or the full scene. Video surveillance is assumed to be restricted to critical regions. Cameras are deactivated by default, yet are activated based on motion detectors detecting people entering such regions. Policies specify access rights to regions and privacy levels for individuals or groups. People are authenticated using RFID tags. When entering a critical region with an RFID tag granting access, one may also be granted a high privacy level, ie, getting erased from visualized video data. This approach seems to be useful when utilizing video surveillance for observing people in constrained regions. However, even while staying in the observed area, people can transfer their (group) identity to someone else by passing on their RFID tag.

Authentication with an intelligent video surveillance system

In order to enforce (group) identity-based privacy requirements, eg, hiding employees in the video surveillance process, we need to enable respective persons to authenticate themselves with the system. We propose to use a two-step authentication scheme using a mobile communication device, eg, a smart phone or tablet.[11] First, a cryptographic authentication is performed over a wireless network, authenticating the mobile device as belonging to somebody from the group of employees (or, as the case may be, a particular person). In the second step, the surveillance system replies with a short-lived graphical code, which is easy to recognize for surveillance cameras. When the code is presented to a camera, the authentication as an employee is fused into the associated unknown person object captured by the camera. The object is hence reclassified as an employee object, and privacy-enhancing mechanisms matching this group identity are triggered and enforced. The association of an object and its (group) identity is maintained by employing the system's tracking capabilities, ie, keeping track of the position of a person recognized as an employee is crucial for being able to enforce the privacy requirements being due to the group of employees. As stated above, in comparison to a locatable token, this approach has the advantage that it is much harder to transfer ones identity to someone else. Note that selectively anonymizing or hiding employees in video streams while unknown persons are shown also requires tracking. The surveillance system can perform this kind of selective anonymization by tracking the positions of person objects known as employees or also by means of soft-biometric features such as the colour distribution of the person's visual appearance. Robust solutions will even have to combine both kinds of information.

The tracking paradox

In intelligent video surveillance, we denote the following phenomenon as tracking paradox: assume a video surveillance system that visualizes the positions of guests as pictographs on an abstract area map. Additionally, measures are taken to prevent the video surveillance system from visualizing or exposing any data about employees in the area under video surveillance. In order to allow for such behaviour, the system needs to track the positions of all objects (including employees) in order to protect the ones that are known as employees.

To understand how this paradox originates, it is important to recap how intelligent video surveillance systems process data. Computer vision algorithms extract information from surveillance cameras' video streams, ie, feature vectors including the position of the observation, which is then delivered to information fusion algorithms. These algorithms aggregate observations from various information sources, ie, multiple image or signal

9 A Senior, S Pankanti, A Hampapur and others. 'Enabling Video Privacy Through Computer Vision' (2005) 3 Security Privacy, IEEE, 50–57.

10 Jehan Wickramasuriya, Mahesh Datt, Sharad Mehrotra and others, 'Privacy Protecting Data Collection in Media Spaces' in Proceedings of the 12th Annual ACM International Conference on Multimedia (ACM, NY, USA, 2004).

11 Hauke Vagts and Jürgen Beyerer, 'Enhancing the Acceptance of Technology for Civil Security and Surveillance by Using Privacy Enhancing Technologies' In Future Security 2011 Conference Proceedings, pp 372–379. (Fraunhofer, Berlin 2011).

exploitation algorithms monitoring the same area, into distinct objects. These objects are then maintained in a world model data structure as introduced by Bauer and others.[12] A simple example of a fusion algorithm would aggregate all observations within the close proximity of an existing object to this particular object. If no proximal object exists, a new one is created.

Figure 1 visualizes the state of a surveillance system's world model at a given time (t). Currently the system has information about two different objects, denoted as Guest A and Guest B. In the next step (t') the system receives additional information, ie, an authentication token, that allows for classifying Guest B as an employee. According to the privacy policy, which forbids tracking of employees, assume that the system now deletes all information about this object. As a result, the object disappears from the map. Therefore, on the first glance, the system seems to adhere to the claimed privacy policy of not tracking employees. However, in step (t'') the tracking paradox comes into effect. The surveillance system again receives information about an object, which, according to its position, is unknown so far. As there is no object into which the received information can be fused, the system creates a new object called Guest C. Hence, the system is now tracking an employee, even though this employee has just successfully authenticated himself with the system and should be protected.

If we generalize the tracking paradox, we can phrase it as follows: if the classification into a protected group depends on a subject's private information, then it is impossible to distinguish between private information from protected and non-protected individuals.

Coping with the tracking paradox while still fulfilling (group) identity-based privacy requirements, the system's implementation needs to adhere to the following principle: *Collecting a subject's private data for classification purposes is allowed, if and only if it can be shown that it never exposes data of a member of a protected group.* As long as this principle holds, privacy privileges for groups or individuals can be enforced, while others can still be monitored for security reasons.

Implementation

We implemented a simplified version of a data store and a fusion algorithm as a Java object. The object maintains a list of employees and a list of guests holding their features. By using the three methods offered by the object, the environment can manipulate and read the stored data. Figure 2 shows the signature of the methods implemented and the fields maintained by the object.

Two arrays are used to store the features of all objects known to the system. Without loss of generality we simplified the implementation by choosing 2 two-dimensional Integer arrays instead of arrays of Objects. The array *guestVectors* stores the features of all guests, while *coworkerVectors* stores the information about employees.

Three methods can be used to update and read the stored information about objects. The method *updateObservation()* takes as argument a feature vector, which contains information about an observation as extracted from a camera stream. If the features can be fused with an object known to the system as a guest, the information of this person is updated using the values of the given argument. If no guest fits to the observation, the system checks, if there is an employee suitable for fusion. If neither exists, a new guest is created by adding a new entry to the field *guestVectors*.

The method *getGuest()* can be used to read the information of the guest stored at the given index. *Null* is returned if the index is out of bounds. The method *registerCoworker()* checks whether a guest exists in the system that fits to the feature vector given as an argument. If so, the information about this guest is removed from *guestVectors* and added to *coworkerVectors*.

While this implementation is rather simple, it provides all functionality necessary to analyse a data store with a fusion algorithm, ie, its behaviour reflects the behaviour of a real surveillance system on a higher level of abstraction. We aim to show that it is possible to implement a data store with a fusion algorithm, which ensures that no information about employees is exposed by the system. The stored information is necessary to decide for a given input vector whether it may be exposed to the environment or not.

Verification

We analysed the implementation presented above using self-composition,[13,14] in order to proof non-interference properties. In this approach, the data in the system are separated into a low and a high part. An environment may learn anything about the system's low values by running the programme, but must not learn anything

12 A Bauer, T Emter, H Vagts and others, 'Object Oriented World Model for Surveillance Systems' in Future Security: 4th Security Research Conference (Fraunhofer, Berlin 2009).

13 Rajeev Joshi and K. Rustan M. Leino, 'A Semantic Approach to Secure Information Flow' (2000) 37 Sci Comput Program, 113–38.

14 Torben Amtoft and Anindya Banerjee, 'Information Flow Analysis in Logical Form' in Static Analysis: 11th International Symposium, SAS 2004, Verona, Italy, August 26-28, 2004, Proceedings, vol. 11 (Springer Science & Business Media, 2004).

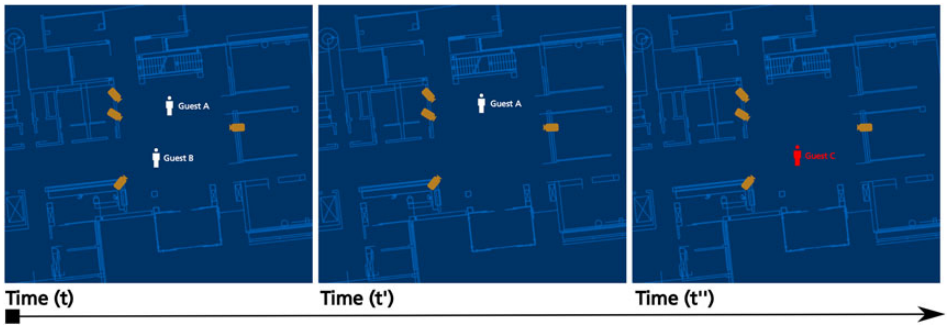

Figure 1. Data representation.

```
private int[][] guestVectors;
private int[][] coworkerVectors;

public void updateObservation(int[] observation);
public int[] getGuest(int pos);
public void registerCoworker(int[] observation);
```

Figure 2. Signatures of used fields and methods.

about other values. Formally, two runs of the programme are compared, both of which are started in states that agree on the low values, but may differ on the high values. A programme satisfies the non-interference property if the low values also agree in the post state. If the environment is considered to only be able to observe the low values, nothing can be learned about the high state of the system in the pre state by analysing the information given to it by running the programme.

The information flow which is assumed to be allowed and the functionality for each public method is specified using JML. A short example of the JML annotations used is shown in Figure 3. We do not present the specification of the functionality here, since this is out of scope of this paper. The information that we specified as low, ie, it may be known by the environment, includes the features of all guests known to the system, since this information is shown to the operator. The features that are extracted from a camera stream may also be disclosed under the condition that either the features describe a guest or a person that has not yet been authenticated as an employee. In the second case, the observation is assumed to show a new guest and therefore the features are also displayed to the operator.

Figure 4 shows a slightly simplified specification of the allowed information flow of the method *updateObservation()*.

The *requires* clause in line 2 describes some pre-conditions that have to be satisfied in the state before the method is called. We skip the details for the sake of brevity. In the *respects* clause in line 3 a list of expressions is given, the evaluation of which may be known to the environment before and after the execution of the method call. This clause is the specification of the information considered to be low.

Line 3 specifies the amount of guests known by the system to be low. Line 4 specifies that each feature of each guest, for example the position, may be known to the environment. The predicate *containsWorker* in line 6 expresses that there exists an employee in the system, into which the observation given as an argument can be fused. Note that only the existence may be exposed, but no further details like the employee's position or the amount of employees registered in the system. Line 7 specifies that the information whether or not a guest exists, into which the observation can be fused, may be released. Again, no details about the observation must be exposed.

Finally, line 8 and the following specify that the values of the observation vector may be known to the environment, if either there already exists a guest, which was observed again, or if there exists no employee, which was recognized. The first case is clear, since the environment may know guests' features. The second case describes the situation when an observation was made, but the operator cannot see a change on his screen. So, obviously an employee was recognized.

We used the KeY tool for verification of the implementation. It takes Java source code annotated with JML as input and uses symbolic execution in order to translate it into JavaDL (see detail in work from Weiß[15]). The KeY tool implements a sequent calculus, which is used to prove that the specification is satisfied by the implementation. Details about the implementation of self-composition in KeY can be found in work done by

15 Benjamin Weiß. 'Deductive Verification of Object-Oriented Software: Dynamic Frames, Dynamic Logic and Predicate Abstraction.' PhD thesis, Karlsruhe Institute of Technology (2011).

```
@ public normal_behaviour
@ requires observation.length == NUM_FEATURES &&
@   (\forall int i; 0 <= i && i < guestVectors.length;
@          guestVectors[i] != observation) &&
@       (\forall int i; 0 <= i && i < coworkerVectors.length;
@          coworkerVectors[i] != observation);
@ respects lowvalues,
@   (\exists int j; 0 <= j && j < coworkerVectors.length;(
@     (observation[POS_X]-coworkerVectors[j][POS_X])<BLURX &&
@     (coworkerVectors[j][POS_X]-observation[POS_X])<BLURX &&
@     (observation[POS_Y]-coworkerVectors[j][POS_Y])<BLURY &&
@     (coworkerVectors[j][POS_Y]-observation[POS_Y])<BLURY &&
@     observation[FEAT1] == coworkerVectors[j][FEAT1] &&
@     observation[FEAT2] == coworkerVectors[j][FEAT2] &&
@     observation[FEAT3] == coworkerVectors[j][FEAT3])),
...
```

Figure 3. Example of information flow contracts in JML.

```
@ public normal_behaviour
@ requires ...
@ respects guestVectors.length, guestVectors,
@     **list of all features of guests **,
@     containsCoworker(observation),
@     containsGuest(observation),
@     (containsGuest(observation) ||
@              !containsCoworker(observation))?
@         (** list of all features in observation **):
@         (null);
```

Figure 4. Simplified information flow contract for *updateObservation()*.

Scheben and Schmitt,[16] We verified the information flow specification for the biggest part of our implementation. These results indicate that it is feasible to implement this kind of secure data store, which does not release any data concerning employees. The positions of employees are solely tracked in order to allow the distinction between employees and unknown persons.

Legal considerations

After a thorough analysis of the technical part of the tracking paradox, we want to have a look at the legal aspects of smart privacy-preserving video surveillance.

Characteristics

The smart or intelligent video surveillance system, as outlined above, collects various information about employees in the monitored area. At the same time, it is able to increase the privacy of the observed people and to increase the selectivity of the surveillance measure. The prototypical system allows persons to authenticate themselves as employees. By tracking the positions of employees, the system ensures that no data about them are exposed. For example, such a system could show live video streams to the operator in which employees are blurred or completely removed while at the same time visitors are visible. While the proposed system collects more data about individuals, its actual impact on privacy is smaller in comparison with conventional video surveillance systems. Therefore, we investigate the technical progress as described above with regard to its compliance with legal requirements, in particular with European Law and section (§) 6b of the Federal Data Protection Act (BDSG).

European law

At the European level, the 'Directive 95/46/EC on protection of individuals with regard of the processing of personal data and on the free movement of such data'

16 Christoph Scheben and Peter H Schmitt, 'Verification of Information Flow Properties of JAVA Programs Without Approximations' in Formal Verification of Object-Oriented Software: International Conference, FoVeOO 2011, Turin, Italy, October 5–7, 2011, Revised Selected Papers. Vol. 7421 (Springer, 2012).

(Directive 95/46/EC) and the 'proposal for a General Data Protection Regulation' have to be legally assessed. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.[17] In comparison to the directive, which has to be implemented by the Member States and insofar is not directly legally binding by itself, the regulation is directly applicable. The 95/46/EC contains no explicit norm regarding video surveillance. The proposal for a General Data Protection Regulation only includes a so-called Data protection impact assessment.

Directive 95/46/EC

The usage of video surveillance must be in accordance with the principles of data protection. Although there is no explicit provision in the Directive 95/46/EC for video surveillance, different aspects of processing personal information from audio and video data are listed explicitly in different sections of the Directive.[18] The Directive should also be applicable to sound and image data relating to natural persons.[19] The principles of data protection must apply to any information concerning an identified or identifiable person. But they shall not apply to data rendered anonymous in a way such that the data subject is no longer identifiable.[20]

Therefore, the processing may only take place for explicit and legitimate purposes.[21] The purposes must be defined clearly and precisely.[22] Processing of personal data is allowed only if at least one of the criteria in Article 7 Directive 95/46/EC is fulfilled. Furthermore, the use of video surveillance and video monitoring itself must be proportionate. This means that video surveillance systems may only be deployed for purposes that actually justify recourse to such systems. The proportionality principle entails that these systems may be deployed if other prevention, protection and/or security measures, of physical and/or logical nature, requiring no image acquisition prove clearly insufficient and/or inapplicable with a view to the above legitimate purposes. At the same time, the principle of proportionality entails a duty of data minimization.[23]

The Article 29 Data Protecting Working Party has specified the criteria for assessing the legality and appropriateness of the installation of video surveillance systems in a working document.[24] However, this working document is not legally binding as the group itself gives only opinions and recommendations and therefore has only an advisory status.[25,26] The group recommends for evaluating the development of video surveillance to prevent a ruthless dynamic preventive monitoring. Also the European Data Protection Supervisor has published video surveillance guidelines.[27]

Regarding German law, the principle of Data reduction and data economy in § 3a BDSG performs a similar function. In particular, video surveillance systems, which have the ability to automatically trace routes and trails and/or reconstruct or foresee a person's behaviour, must be tested specifically. Even the European Data Protection Supervisor points out that high-tech and/or intelligent video surveillance requires a specific review process. Prior to installation and implementation a data protection impact assessment is useful, because the impact of the proposed system on the fundamental rights of persons can be determined and adverse effects can be mitigated or avoided.

Proposal for a General Data Protection Regulation. The proposal for a General Data Protection Regulation (GDPR) requires that a so-called Data protection impact assessment be carried out in the case of large-scale video surveillance.[28] It stipulates that whenever processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations regarding the protection of personal data. The processing operations referred to in paragraph 1 in particular present specific risks, ie, monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale. The assessment has to contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards,

17 Art. 288 Treaty on the functioning of the European Union (TFEU).

18 Recital 16 and 17 Directive 95/46/EC.

19 Recital 14 Directive 95/46/EC.

20 Recital 26 Directive 95/46/EC.

21 Art. 6 Directive 95/46/EC.

22 Dammann, U./Simitis, S. EG-Datenschutzrichtlinie Kommentar, Baden-Baden, 1997, p. 140, Art. 6 recital 7.

23 Dammann, U./Simitis, S. EG-Datenschutzrichtlinie Kommentar, Baden-Baden, 1997, p. 141, Art. 6 recital 11 and 12.

24 Art. 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance. 11750/02/EN. WP89.

25 Art. 29 (I) and Art. 30 (IV) Directive 95/46/EC.

26 Ehmann, E./Helfrich, M. EG-Datenschutzrichtlinie Kurzkommentar, Köln, 1999, p. 341, Art. 29 recital 2; Art. 288 TFEU.

27 European Data Protection Supervisor. The EDPS Video Surveillance guidelines. <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf>, 2010.

28 Art. 33 (II) lit. c GDPR.

security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned (Article 33, no. 3).

Article 82 (processing in the employment context) can apply if intelligent video surveillance is used and employees are monitored. In this case, within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees personal data in the employment context. Therefore, the open optical-electronic and/or open acoustic-electronic monitoring of parts of an undertaking which are not accessible to the public and are used primarily by employees for private activities, especially in bathrooms, changing rooms, rest areas, and bedrooms, shall be prohibited. Clandestine surveillance shall be inadmissible under all circumstances (Article 82 no. 1c lit b). These regulations are contrary to German law, because clandestine surveillance of employees is admissible as an exception when a criminal act or other severe breach to the detriment of the employer is specifically suspected.[29] The main criterion for distinction is the monitored area, because the proposal for a General Data Protection basically permits to monitor publicly accessible areas.

The proposal for a General Data Protection Regulation provides a very wide regulation that leaves much room for interpretation. New technological developments, such as the presented intelligent video surveillance system, are not mentioned in the proposal. An explicit regulation is desirable in order to avoid legal uncertainty from the beginning. Hereby, the German standard of § 6b BDSG could serve as a model. We focus on this regulation as the German Data Protection Law is considered to offer a high standard. § 6b BDSG is the central norm about monitoring of publicly accessible areas with optic-electronic devices.

§ 6b BDSG

Applicability

First of all, § 6b BDSG must be applicable, which is determined according to section § 1 para. 2 BDSG. Basically § 6b BDSG applies to the public and non-public area. Thus, an intelligent video surveillance system falls within the scope of § 6b BDSG and needs to comply with its requirements.

Publicly accessible areas

Application of § 6b BDSG requires, however, that the surveillance is carried out in a publicly accessible area. This includes areas, which can be used and are accessible by an undetermined group of people, or by people who have general characteristics, and which have the prime purpose of being accessed by such a group of people. Publicly accessible areas are, for example: platforms, gas stations, department stores, banks, beer gardens, car parks, libraries, town halls, universities, or public transport. Not publicly accessible areas are corporate and factory premises, gardens, storage, and staff rooms or offices and workplaces without public access.

As soon as an intelligent video surveillance system is used in a public area, all other requirements of § 6b BDSG must be fulfilled in order to have a legitimate video surveillance. § 6b BDSG is not applicable in the case of video surveillance in non-public areas.

Monitoring

Furthermore, the use of intelligent video surveillance systems must constitute monitoring. This means the visualization of occurrences and persons with the help of appropriate technical facilities.

Such kind of monitoring is classified as one type of data collection[30] (§ 3 para. 3 BDSG). In the first instance, it is of no importance whether the graphical material is saved or not saved, since the relevance in terms of data protection already results from pure monitoring.[31] Monitoring, according to § 6 para. 1 BDSG, needs to be distinguished from processing or using. Their admissibility requirements are standardized in § 3 paragraphs 4 and 5 BDSG. Therefore, § 6 b para. 1 BDSG primarily regulates monitoring, whereas an automatic analysis should be covered by § 6 b para. 3 BDSG.[32] But there is no monitoring in case that it takes place in a technical manner, which makes the recognition of certain persons or faces impossible.[33] The regulation does not apply if there are only overview pictures on which people cannot be individualized due to technical limitations even in a post-processing or by linking with additional knowledge. In principle, this will only be the case if a technical design is chosen that leads to anonymization according to § 3a BDSG.

However, intelligent video surveillance might allow to change the anonymous video images into the original

29 BAG, Urt. v. 27.3.2003 – 2 AZR 51/02=NJW 2003, 3436 ff.; BAG, Urt. v. 21.6.2012 - 2 AZR 153/11=ZD 2012, 568 ff.

30 Bergmann, L./Möhrle, R./Herb, A., Datenschutzrecht, 45. Lfg., Stand Juli 2012, § 6 b recital 19.

31 BT-Drs. 14/4329, p. 38.

32 Gerrit Hornung and Monika Desoi,'Smart Cameras' und automatische Verhaltensanalyse, K&R 2011, pp. 153–158 (157).

33 Däubler, W./Klebe, T./Wedde, P./Weichert, T. BDSG, 3. Auflage Frankfurt am Main, 2010, § 6 b recital 14.

ones. In these cases, a monitoring is achieved as you can again surveil the observed people.

For the context of § 6 b para. 1 BDSG, it is initially of no importance that an intelligent video system exists. Such systems are namely characterized by the capability of evaluating the collected data independently and performing error corrections or similar tasks through microprocessors.[34] This operation represents a processing in accordance with § 3 para. 4 BDSG, since processing is as well the modification of personal data. In contrast, a modification means the alteration of the substance of stored personal data (§ 3 para. 4 no. 2 BDSG). This includes any procedure which changes the information content.

At this stage already, the weakness of the regulatory framework becomes visible, which, among other reasons, is due to the fact that intelligent video surveillance is neither mentioned in the wording of the law nor in the explanatory memorandum. The mentioned system makes it possible to see employees blurred or even completely removed whereas other visitors are fully visible on the monitor. In respect of employees, the information is altered, because the operator cannot make any statements about the employees, for example which particular employee is shown on the screen, once they are blurred or even completely removed. Therefore, there is only monitoring of visitors, but not of employees. Furthermore, it is not clear whether monitoring exists in case that individuals are initially made unrecognizable in video stream, but the system still provides the opportunity to restore the original video later on. At this point, it becomes clear that it is difficult to classify new systems such as intelligent video surveillance systems in the context of § 6b para. 1 BDSG. It is also no longer possible to separate the step of data processing (§ 6b para. 3 BDSG) from § 6b para. 1 BDSG in such intelligent video systems.

Optic-electronic device

The intelligent video surveillance system needs to be qualified as an optic-electronic device. This refers to units of all types and designs, as far as they are suitable for observation. An optic-electronic method means the conversion of light into electrical signals, so that even digital cameras or mobile phones would lead to application of the provision. § 6b BDSG is not limited to digital camera technology. It also includes analogue systems. The technology of the electric signal processing is irrelevant. An intelligent video surveillance system satisfies these requirements without any doubts.

Legitimacy of monitoring

§ 6b para. 1 BDSG contains three allowable facts: to fulfil public tasks (no. 1), to exercise the right to determine who shall be allowed or denied access (no. 2) or to pursue rightful interests for precisely defined purposes (no. 3). Thus, the purpose of monitoring is essential and it must be determined objectively. The term 'to pursue rightful interests for precisely defined purposes' must be interpreted, restrictively. Every interest that may be of an economic or ideational nature is sufficient.

Depending on the application scenario it needs to be decided for which purpose the intelligent video surveillance system is used. Furthermore, monitoring must be necessary, and there must be no indications that the data subjects' legitimate interests prevail.

Necessity/requirement

Video surveillance is not permitted simply because the requirements of § 6b para. 1 no. 1–3 BDSG are fulfilled. It also is of high importance that the video surveillance measure is necessary. The necessity of a video surveillance measure requires that no measure is available which is less restrictive. The necessity must adhere to the principle of data reduction and data economy.[35] Therefore, video surveillance must be limited in space, scope, and time.

Principle of data reduction and data economy (§ 3a BDSG). The principle of data reduction and data economy is one of the fundamental principles in German Data protection law. There are also some connecting factors in the proposal for a General Data Protection Regulation. In Recital 30, the principle of data minimization is affirmed with the principle that data shall be limited to the necessary minimum for the purpose for which the data are processed. This is also described in Articles 5(c) and 23.

The rule should have effect in advance of the technology and the system structure, because privacy-enhancing technologies could prevent the emergence of preventable data collections and thus minimize threats to informational self-determination. The regulation can be qualified as a core element of a data protection system. Its function is to balance the interests, which are important when the admissibility of data processing is interpreted. It is a legal obligation to the controller.[36]

34 Christoph Bier and Indra Spiecker gen. Döhmann, Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz?, CR 2012, pages 610–618 (610).

35 Peter Gola and Christoph Klug, Videoüberwachung gemäß Paragraph 6b BDSG – Anmerkungen zu einer verunglückten Gesetzeslage, RDV 2004, pp. 65–74 (70).

36 § 3 para. 7 BDSG.

However, the law requires the controller to take all possible means to achieve the aim. Therefore, the controller has different possibilities which instruments he can use. The regulation contributes to the dynamic development of the technology by making technology-neutral specifications that can be used in a flexible and practical way. A breach of the regulation does not result in material illegality nor in a fine or criminal sanction.

Despite its wording, the principle of data economy is characterized by a two-tier model in its implementation. At first instance, the aim is to refrain from collecting, processing, and using personal data. Only if this goal cannot be achieved, the second instance becomes relevant. Subsequently, the operation process must be organized in a way that the collection and usage of personal data is minimized. The characteristics of the second stage are therefore to reduce the amount of data (quantity) and to reduce the depth of engagement (quality).[37] This aim can be achieved if the information of a person, which can be referred to him or her, is kept to a minimum. A special form of efficient data design exists if the system disables a certain form of personal data output. The aim of data economy can be achieved if personal data, which is collected and stored, are deleted, made anonymous, or made pseudonymous in the earliest possible processing step. The setting of phrase 1 tends to the selection and design of data processing systems that means a 'functional unit for processing data'. The design of data processing systems may refer to the implementation of software or the configuration of the used hardware components. Therefore, the controller must consider what data processing operations he wants to perform and whether the purpose of processing can be achieved without or at least with less personal data prior to purchasing and using such systems. The principle of data reduction and data economy can only be successful if controllers and manufacturers can be converted to participate actively.

In our setting. In the context of intelligent video surveillance, one main problem is the accumulation of more data than actually necessary. First, the system must collect information about employees and visitors. Secondly, the system can remove specific data, so that employees are blurred or removed in the video stream. The collection of the required information, which is necessary to blur or remove employees, could be represented as a breach of the principle of data economy. In the present case, however, the problem can be solved. The personal data of employees will be changed immediately after collecting the information so that the operator cannot see a clear picture. Only visitors are visible. Thus, the personal rights of employees are fully protected because identifying them is almost impossible.

Balancing of interests

Finally, a balancing of interests is required. Video surveillance is permitted only if there are no indications that the data subject's legitimate interests prevail. A balancing of interests between the constitutionally protected positions, namely the users of video surveillance technology, and the observed persons has to be done. The observed persons are protected by their right to informational self-determination. In the context of balancing of interests, the intensity of intrusion is essential. Basically, monitoring devices that are activated only when they are needed are preferable. Therefore, intelligent video surveillance systems should be used.

Thus, the question of the degree of intervention is important, since the weight of the procedure is especially determined by the nature and extent of the collected information, by the temporal and spatial extent of video surveillance, by concerned persons and the evaluation of the collected data. The advantage of intelligent video surveillance lies in making video data anonymous or pseudonymous in a first step. Nevertheless, a re-anonymization or re-pseudonymization is possible under certain conditions. This technical design is favourable for the balance of interests for those who are affected by video surveillance as well as for those who use video surveillance systems. Such a technical design is realized by the so-called tracking paradox.

The intrusiveness of the surveillance measures is not very high for employees because there will be no clear image visible on the monitor. This is different for visitors because they are visible on the screen. In conclusion, the circumstances of the case are relevant.

Result

The legal analysis has shown that comprehensive technical concepts like intelligent video surveillance require an extensive and detailed contemplation. Therefore, it was not possible to analyse § 6b BDSG completely. However, some weaknesses concerning intelligent video surveillance could be detected. For example, it is questionable whether there is monitoring in case that the observed persons are blurred or removed from the screen. Furthermore, the principle of data reduction and data economy must be taken into account. Intelligent

37 Däubler, W./Klebe, T./Wedde, P./Weichert, T., BDSG, 3. Auflage Frankfurt am Main, 2010, § 3 a recital 3.

video surveillance systems often collect more data than actually required.

Conclusion

In this work we have shown that data minimization does not necessarily lead to minimum privacy intrusiveness and best privacy protection. As the tracking paradox shows, in certain cases collecting additional data is necessary for data anonymization. If it is ensured that such additional data are used only for privacy protection purposes, while not being accessible and usable in any other context, then collecting more data actually increases the level of privacy. In particular, the selectivity of surveillance measures can be improved. Referring to our example scenario, we adhere to the privacy requirement of hiding employees by tracking their positions, while at the same time ensuring that positions of employees are never exposed to the environment. Our hitherto results give strong indication that it is feasible to implement and verify a data store with an information fusion algorithm, which ensures that no private data from objects of the protected class, eg, the class of employees, is ever exposed by the system.

Our analysis of § 6b BDSG has shown some weaknesses in the context of intelligent video surveillance. Nevertheless, there is at least one legal provision in the German data protection law concerning video surveillance. At European level, neither the Directive 95/46/EC nor the proposal for a General Data Protection Regulation contains a provision for using video surveillance and especially not for using intelligent video surveillance. There are only guidelines from the European Data Protection Supervisor and the Article 29 Data Protection Working Party. The proposal for a General Data Protection Regulation only includes a so-called Data protection impact assessment in Article 33 para. 2(c). A further differentiation has not been made. If a certain degree of a General Data Protection Regulation is established, this gap should be closed.

In addition, the regulation of § 6a BDSG in connection with intelligent video surveillance is completely ignored.[38] Decisions, which have legal consequences for or substantially impair the interests of the data subject, must not be based exclusively on the automated processing of personal data, which serves to evaluate individual personal characteristics (§ 6a para. 1 s. 1 BDSG).

Concerning German law and also European law, a variety of questions are still left open. Insofar users of intelligent video surveillance systems have to accept legal uncertainty. Therefore, new regulations, which particularly pay tribute to the technical progress in intelligent video surveillance, have to be developed, preferably in collaboration with engineers and lawyers.

doi:10.1093/idpl/ipv021
Advance Access Publication 25 September 2015

38 Christoph Bier and Indra Spiecker gen. Döhmann, Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz?, CR 2012, pp. 610–618 (614).