Privacy Analysis of a Mobile Sensor Application

Heinrich Hartmann, Tim Wambach, Maximilian Meffert, and Rüdiger Grimm

University of Koblenz-Landau

Abstract. TODO: (later)

Keywords: privacy protection, IT security analysis, sensor data, mobile phones, traffic survey

1 Introduction

TODO: RG
* Context: Reference model IT Security analysis
* Application: Travel Survey
* Different definitions of privacy in the literature.
* Study outcomes depend on privacy definition

In recent days the importance of privacy protection has been amplified by the reports about the mass surveillance of ordinary citizens on a global scale by the NSA and other intelligence agencies around the world.

While aiming at the noble cause of enhancing eParticipation using mobile technologies, Live+Gov systems do process a large variety data that is potentially infringing the citizens privacy. The captured data includes personal information like name, phone numbers and email addresses and sensor data from GPS and accelerometer sensors. Also with some applications it is possible to gather images and textual input from the citizen.

While the collection of this data is necessary for providing the advanced services that Live+Gov aims to deliver, at he same time, the available raw data can be used to draw a very detailed picture of the private life of the citizen. For instance can GPS location tracking be used to reveal shopping habits (e.g. when a car seller is visited) and associations to political groups (when a meeting is attended). Accelerometer data can be used to infer medical conditions like walking disabilities. Images can contain faces of nearby persons to with whom the citizen is associated. All this data is highly sensitive to the citizens privacy and can be used against the citizen if it falls in the wrong hands.

The great importance of protecting the citizens privacy should be apparent from these examples. The European Union, as well as many other countries in the past, has set out a number of directives that regulate the collection, processing and use of privacy sensitive data. We explain the most relevant legislation in Section **??**.

The ethical aspects of privacy have been the subject of study of many social scientists and philosophers. One scholar which is particularly relevant in our context is Charles Fried. He investiages, why we are intuitively so sensitive to violations of our privacy. For him privacy is not asserted as an intrinsic value by itself, he rather sated:

> *Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.*

Fried's study on the understanding of privacy provided a great contribution to the research on the same term in philosophy and computer science and despite the fact his text was published in 1970, he already included technologies to its viewpoint (like location monitoring) that are particularly relevant to our Context. We explain his theory in **??** *and follow his definition of privacy in this document.*

In this document we perform a thorough analysis of how to protect the privacy of a citizen and present several implementations that form the core of our privacy aware Sensor Data Storage and Mining Infrastructure.

We identify six main threats for the citizens privacy, and derive eight recommendations that should be followed in order to reduce the associated risks for hazards. This analysis form the guideline for the selection of 9 measures that were implemented in our system and documented in Chapter **??**.

2 Scenario Description: Mobile Traffic Survey

```
TODO: HH:
* System description: (Raw version copied from Privacy Analysis)
* Information needs of transport agency
```

IT-Systems & Interactions *This section outlines the general architecture (Figure 1) of IT systems for public monitoring comparable to the Live+Gov project. This includes a description of it technical infrastructure and the interactions between its components.*

The IT infrastructure of the Live+Gov system, i.e. the Live+Gov toolkit and the customization of the software components are described in detail in various project deliverables: D4.1, D4.3, D1.1, D5.1. In this section we give an abstraction of those systems from the perspective of WP1.

A citizen *(a) carries a mobile device running the* sensor collector *application (d). The sensor collector application is able to collect various kinds of sensor data (accelerometer, GPS, GSM, ...) and can sent the raw data back to the* data center *(c). The sensor collector can also be able to perform certain data mining operations.*

Examples of such data mining operations include human activity recognition,the detection of service lines, detection of characters and faces from images.

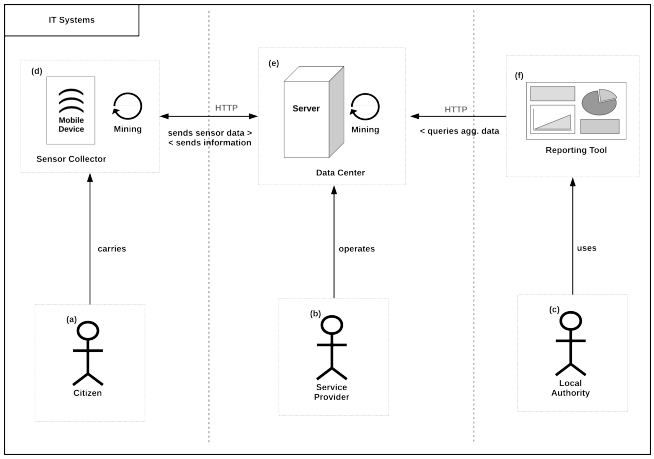
In the Live+Gov Project mobile devices are used in particular for the following activities:

1. *collection of GPS samples,*
2. *mining of Human activities (HAR) based on accelerometer samples,*
3. *collection of reports consisting of an image, free text and selected categories.*

The data center *stores and processes sensor data collected with the sensor collector application. It can also take into account data obtained from third parties, like the current positions of trains. The data center can sent mining end products (traffic jam reports, bus schedule) back to the mobile device of the citizen.*

In the Live+Gov Project data centers, in particular, perform the following activities:

1. *storage of login credentials, name, and email address for each citizen,*
2. *storage of collected GPS samples (user id, timestamp, GPS location),*



Legend:

- **(a) Citizen:** User of the L+G client application whose privacy is at stake.
- **(b) Service Provider:** Provides technical infrastructure.
- **(c) Local Authority:** Provider of the L+G system.
- **(d) Mobile Device:** Runs the L+G client application, produces and stores data sensitive to the users privacy.
- **(e) Data Center:** Runs the L+G services, processes and stores user data.
- **(f) Report Tool:** Interface to aggregated user data.

Fig. 1. IT Systems

3. *storage of HAR results (user id, timestamp, HAR result),*
4. *detection of service lines based received GPS samples (SLD),*
5. *storage of SLD results (userid, timestamp, SLD result),*
6. *sent back SLD results to mobile device,*
7. *storage of received reports (user id, timestamp, report),*
8. *detection of inherent patterns of the received reports.*

The System Provider *(b) provides and operates technical infrastructure like the Data Center and the* Reporting Tool *(f). The Reporting Tool queries the Data Center for aggregated data to visualize in form of charts and other means suitable to help understanding of monitored citizens.*

Local Authorities (c) use the reporting tool to get information in order to understand citizen movement and improve public services. In such systems, the most valuable information for local authorities is not the raw sensor data, but aggregated views on the mining end products.

In the Live+Gov Project the reporting tools allows, in particular the following queries:

1. *show aggregate information about which routes citizens take starting from a given location,*
2. *show the average waiting time of a citizen for each bus stop,*
3. *show routes where citizens where running to catch a bus,*

4. *show locations of all reports in a given time window,*
5. *visualize detected patterns in the report data,*
6. *view individual reports.*

3 Definition of Privacy

Defining privacy is a challenge which seems impossible. This is well put to words by Serge Gutwirth, who notes:

> The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as 'our' privacy, it still finds a way to remain elusive. [9]

In this section we introduce the concept of privacy as control over information. We specify types of information we have to deal with in the context of privacy. And finally we outline the impact mobile sensors can have on one's privacy.

3.1 Privacy as Control over Information

One possible definition of privacy is given by Charles Fried in his work *An Anatomy of Values*[7]. He questioned, why we are intuitively sensitive to privacy violations. But he did not assert privacy as an intrinsic value by itself, he rather stated:

> **Privacy is** not simply an absence of information about us in the minds of others; rather it is **the control we have over information about ourselves**. [7]

According to Fried privacy is our ability to create and modulate the relationships to other humans. Which makes us intuitively sensitive for its violation, because this affects what defines our identity. Also, the ability to build and maintain relationships is essential to society. This is what makes privacy valuable and deserving of protection. [5][7]

Relationship Creation. We share information of great intimacy only with persons we deem trustworthy. Moreover, we trust those persons to not reveal information about us to others by not constantly monitoring them, i.e. respecting their privacy. Trust needs the possibility of unknown failure. If we would constantly monitor our partners, they cannot fail unnoticed nor can they willingly share intimate information with us. By trusting them, we create the possibility for them to share intimate information with us. [7]

Relationship Modulation. Fried argues, depending on the person we are interacting with, we are changing the degree of intimacy we share. If we are to share private information with others, we are most likely aware that this action is privacy related. In that case we are able to selectively disclose information along the two dimensions of quantity and quality. [7]

Alternative Definitions. Using Fried's anatomy of privacy for this analysis is suitable because of two points. Despite the fact his text was published in 1970, he already included technologies to its viewpoint that did not only monitor location, but also record biometric data [7]. Secondly, the concept of control over information does not enforce data minimization. Fried's definition complies with what we call *self data protection*, where persons communicate their data self-determined. This is the opposite of *system data protection*, where the collection of certain data is prohibited.

TODO: RG: Discuss alternative definitions of privacy

3.2 The Seven Types of Privacy

In Fried's definition of privacy as control over information, the specification of what constitues such information remains open. There is a vast amount of information that relates to a person and we need to get a better understanding in order to perform a thorough analysis. To this end we use the the categorization by Friedewald, Finn and Wright [6] called the *Seven Types of Privacy*. The seven types of privacy are an extension to the four types of privacy by Roger Clarke [4], which are: *Privacy of the Person*, *Privacy of Personal Behaviour*, *Privacy of Personal Communication*, *Privacy of Personal Data*. It is important to note, that these categories do not form a taxonomy, since the categories are not mutually exclusive. For instance a written email is considered personal communication as well as personal data stored on a computer.

Moreover, Friedewald et al. argue that Clarke's types are outdated and no longer adequate in order to describe the privacy aspect of our modern, technology driven, world. In order to address this shortcoming they extend the former four to the now introduced seven types privacy as follows:

1. **Privacy of the Person** This privacy type is generally concerned with one could best understand as biometric privacy. Friedewald et al. paraphrase it as *"[...] the right to keep body functions and body characteristics [...] private"*. This includes but is not limited to measures like weight, height or shoulder width; biometric identifiers like fingerprints and DNA sequences; or medical conditions such as limping or having a cold.
2. **Privacy of Behaviour and Action** This privacy type is concerned with one's activities in public as well as in private spaces. It includes but is not limited to religious practices, political activities and sexual preferences or habits.
3. **Privacy of Communication** This privacy type is concerned with one's communication in a broad sense. It includes written correspondence, but also conversations conducted either vis-a-vis or via electronic devices. Friedewald et al. put it as the right to free discussion without unknown interception by third parties.
4. **Privacy of Data and Image** This privacy type is concerned with the secrecy of personal data, especially its automatic disclosure to other individuals

and organizations. It includes data such as paychecks, insurance information or records of public administration. However, it also refers to pictures taken without consent and digital identifiers like IP addresses or social security numbers.

5. **Privacy of Thoughts and Feelings** This privacy type is the counterpart to Privacy of the Person like body and mind are counterparts of one another. Comparable to the Privacy of Data and Image, Friedewald et al. state that one's thoughts and feelings must not be automatically revealed to others. This could simply happen by the disclosure of one's diary or by technologies which allow emotion detection through biometric means. One's body temperature or iris reflexes might infer stress or excitation.
6. **Privacy of Location and Space** This privacy type is concerned with one's movements in public spaces and the protection of private spaces. Friedewald et al. qualify the first dimension as one's right to move without being identified, tracked or monitored. The second dimension is qualified as one's general right to solitude, especially the right to the inviolability of the home.
7. **Privacy of Association** This privacy type is also put as group privacy. Friedewald et al. state that one must have the possibility with whomever without being recorded. Associations like friends or organizations such as political parties must not automatically be recorded because one associates with them, and vice-versa.

3.3 Sensor Data Privacy Impact

Modern mobile devices have a broad collection of sensors. Disclosure or processing of sensor data can impact one's privacy. In this section we identify groups of sensors and their potential impact on a certain type of privacy. Figure **??** qualifies that impact on a simple scale. Privacy of Data and Image is trivially threatened because here sensor data is individual data, a priori. Indirect impact is caused by combining sensor data with additional knowledge. For instance, comparing a contemporary map with locational data can imply behaviour if the position matches a church.

	Pricacy of the Person	Pricacy of Behaviour and Action	Pricacy of Communication	Pricacy of Data and Image	Pricacy of Thoughts and Feelings	Pricacy of Location and Space	Pricacy of Association
GPS Sensor	0.5	0.5	0	1	0	1	0.5
Motion Sensors	1	0.5	0	1	0	0	0
Networking Sensors	0.5	0.5	0	1	0	1	1

0: No Impact, 0.5: Indirect Impact, 1: Direct Impact

Fig. 2. Sensor Data Privacy Impact Matrix

GPS Sensor. The GPS sensor gives the current longitude and latitude, the current global position of the mobile device and its carrier, although there is some artificial inaccuracy within civil use. Therefore, the collection of GPS data violates directly the citizens privacy of Location and Space.

Motion Sensors. Accelerometer, Rotation Vector, Gyroscope and Magnetic field sensor measure the physical movement of the mobile device on all three axes. If the mobile device is carried "normally" its safe to say that those sensors also measure the moments of its carrier. So his privacy is infringed regarding biometric behaviour, i.e. the Privacy of the Person.

Network Sensors. The GSM and WLAN sensors reveal the position of the mobile device and its carrier, when used in connection with external databases. The both sensors give the exact cell or network, the mobile device has registered with at the current moment. Frequent connection to one particular network also reveals association, e.g. university networks.

The Bluetooth sensors record lists of the bluetooth clients in the direct neighbourhood. Since those clients are usually moving, inference of the position is usually not possible. Instead, bluetooth clients carried by a third person may infringe the Privacy of Association.

4 IT Security Reference Model

TODO: TW

The goal of this chapter to analyze and identify the threads to personal privacy that are posed by collecting, storing and processing sensor data from mobile phones. We derive concrete privacy protection measures that address the main risks involved with handling such data.

The complexity of our systems and the variety of threads make a great number of counter measures plausible. We approach this complexity with the aid of a general security analysis model developed in [8]. We give a brief introduction to this model and perform a IT Security Analysis with respect to the privacy asset for our system.

We follow the Reference Model for IT Security Analysis as described in [8]. It supersedes earlier efforts by e.g. [1]. The reference model consists of a model *and a* procedure*. The model aims to organize common security terminology in a reasonable and practical way. The procedure describes a method to analysis the IT system based on that model. In this section we give a brief overview over the reference model.*

4.1 Model

The model is depicted in Figure 4. It is organized in four views (round boxes) that contain a number of components (rectangular boxes).

The world view *contains all components describing the current state. It consists of the following components:*

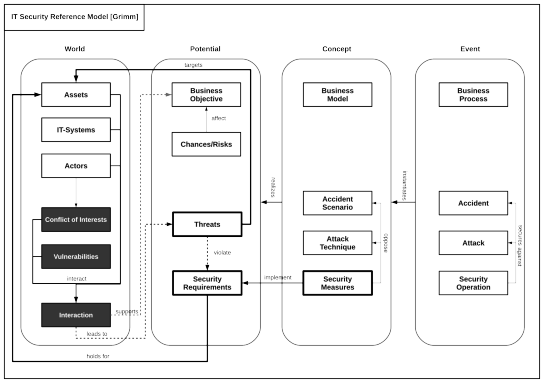


Fig. 3. The IT Security Reference Model (Grimm)

- ***Actors.*** *All identifiable stakeholders of the system under study. Typical actors include, users, developers, clients and externals.*
- ***Assets.*** *Things of value to one or more stakeholders. The value can be hard (money, data, etc.) or soft (trust, privacy,etc.). In our case the only asset we are concerned with is the privacy of the citizen.*
- ***IT-Systems.*** *The relevant IT-Systems under study. This encompasses hardware (e.g. servers, network infrastructure), as well as software and third party services. The level of granularity has to be detailed enough to express all possible threats to the assets at stake.*
- ***Conflicts of Interests.*** *Different actors have different interests which can be in conflict which each other. These conflicts of interest are the origin of all attacks to the system.*
  A typical conflict is the Criminal-User-Conflict*: A user wants to keep control over their private data. A criminal wants to gain money. The possibility of selling private data (user profiles) to advertisers, renders both interests conflicting.*
- ***Vulnerabilities.*** *All identifiable weaknesses in the IT-System.*
  In the example of the criminal-user-conflict, the criminal has to exploit a vulnerability, e.g. a weak password, to gain access to the private data about the user.
- ***Interactions.*** *This point captures all possible interactions between assets, IT-Systems, humans and vulnerabilites. It is described in more detail in the next view.*

The potential view *displays the intended and unintended interactions of the components in the world view. The intended interactions support the underlying business objectives. Unintended interactions lead to threats. The potential view consists of the following components.*

- ***Business Objectives.*** *Interaction of IT-system and actors that realize a business goals of the system owner.*
- ***Threats.*** *A threat is a potential interaction that destroys or harms assets of the system. Concrete realizations of threats can be* attacks *or* accidents*. Attacks are executed by an actor in response to a conflict of interest. Accidents are harmful interactions that are not willfully caused by an actor.*

- ***Chances/Risk.*** *Evaluation of chances and risks associated to the business objectives and threats. The risk associated to a threat is its expected loss. A chance associated to a intended interaction is its expected gain.*
  In the case that, the loss can be quantified monetary, and the likelihood of occurrence of a threat can be modeled probabilistically, the risk is given by the product

$$risk = loss \cdot P[threat].$$

  In practice such a quantitative risk evaluation is often not possible, and a qualitative, heuristic, analysis is performed instead.
- ***Security Requirements.*** *A set of interactions (e.g. threats) that shall not occur within the system in order to achieve its business objectives. Security requirements are targeted to protect one or more assets.*
  An example of a security requirement is that a given communication channel shall not be infringed by externals.

The concept view *is a realization of the potential view of the system. It specifies important interactions that require further planning. It contains the following components:*

- ***Business Model.*** *The plan to achieve business objectives.*
- ***Accident Scenario.*** *A concrete outline of an interaction that leads to an accident. In particular the asset under threatened and exploited vulnerability need to be described.*
- ***Attack Technique.*** *A specific technique or technology to attack IT-Systems (Man in the Middle, Phishing, etc.). In particular the attacking actor, the conflict of interest and the exploited vulnerability need to be described.*
- ***Security Measures.*** *It describes a plan of sufficient measures to secure the intended interactions and to avoid the unintended interactions. Each security measure targets a vulnerability of the system in order to reduce a risk for a certain thread.*

The event view *contains all actual events through out the lifetime of the system. The event view instantiates the concept view of the system. It contains the following components:*

- ***Business Process.*** *The actual, running instance of the business model.*
- ***Accidents.*** *All actually happened accidents.*
- ***Attacks.*** *All actually happened attacks.*
- ***Security Operations.*** *Instances of security measures.*

4.2 Procedure

The analysis procedure is an incremental and iterative process following the four views of the previously described model.

Step 1. World Analysis At first, one has to outline the current state of the system under study. This includes description of:

- *all* ***Assets*** *which must be protected*
- *all relevant* ***IT-Systems***
- *all involved* ***Humans*** *and their* ***Conflicts of Interests***
- *all known* ***Vulnerabilities***
- *and all important* ***Interactions*** *between the former components.*

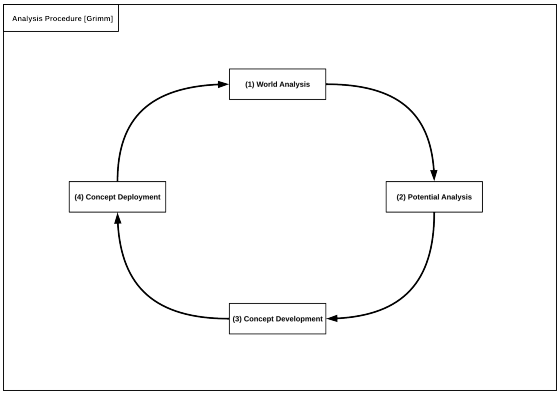


Fig. 4. The IT Security Reference Analysis (Grimm)

Step 2. Potential Analysis Secondly, one needs to outline the potential interactions of the system under study. This includes both the unintended interactions (threads) and the intended interactions (business objectives). This step produces four artifacts:

- *a* threat specification*, which identifies the threat, its targeted assets, the involved actors and their conflicts of interest.*
- *a* threat risk evaluation*, which quantifies the likelihood of a threat manifestation in relation to its associated loss.*
- *a* security requirement specification*, which specifies requirements in order to deal with identified hazards*

Step 3. Concept Development Based on ***Step 2.****, the identified hazards are used alongside realistic accident scenarios and attack techniques to create a* risk matrix*. With this matrix it is possible to decide if the risk is acceptable or not. Together with the previously specified security requirements, the matrix is used to define adequate security measures. Like a business model is an abstract concept to achieve business objectives, this step creates an concept to improve the system's security.*

Step 4. Concept Deployment Finally, the security measures have to be implemented. Additionally, all business operations, accidents, attacks and executed security operations will be recorded in the following time.

The implementation of security measures changes the world view (e.g. IT-systems, actors) and renders the conducted analysis outdated. So this analysis procedure needs to be conducted again.

4.3 Abstraction Levels of the Reference Model

The Reference Model can be used on different levels of abstraction. This means each component can be used within a wide range of granularity, for instance the security measure Encryption *can be explored in general or on the level of different concrete encryption tools; or on the even finer level of concrete algorithms.*

The utilized abstraction level is not important for the analysis procedure, it depends on the intended audience for the analysis. However, it is important to use one abstraction level consistently through out the analysis.

5 Privacy Analysis

TODO: TW

5.1 Step 1. World Analysis

Assets: Privacy *In this document we focus our attention to only one asset: The privacy of the citizen.*

Our definition of privacy is described in detail in Chapter ??. In Section ?? we define privacy as the "control over private data" and introduce the following seven different types of privacy:

1. *Privacy of the Person*
2. *Privacy of Behaviour and Action*
3. *Privacy of Communication*
4. *Privacy of Data and Image*
5. *Privacy of Thoughts and Feelings*
6. *Privacy of Location and Space*
7. *Privacy os Association*

We refer to Section ?? for more details.

Actors *This section describes the human actors previously introduced within the IT system architecture (2). Also the additional actor External is introduced as a person with no special access rights.*

Citizen. *Citizens are persons who use the mobile device as users of the provided software. Their main motivation for using the software is to gain a higher level of convenience in their daily activities. For example they may have access to real time bus schedules or reports about traffic jams, that help them to avoid long waiting times. Also they generally benefit from improvements of public infrastructure by local authorities, which is triggered by issue reports.*

By using the application citizens are sharing personal information like name and address, as well as data gathered from mobile sensor with the service provider. This data can be exploited in ways that are harmful to the citizen. This need to protect this protection is manifest in several laws and constitutions as the right to privacy and data protection. The citizen has a vital interest in having his legal rights protected and enforced.

If the right to privacy is violated, there is a magnitude of potential harms that interfere with other interests of the citizen. This includes just annoying spam, where their technical identity is used to send unwanted commercials. More severe phishing attacks can exploit personal information, and try to manipulate citizens into disclosing credentials like TAN numbers and disrespect their financial interests. Information about the current location (GPS) or frequently used routes (stalking) can be used to attack and directly harm the health of the citizen. Information about medical conditions inferred by sensor data (e.g. fintness trackers) are of interest to insurance companies, which may affect the pricing of policies and can interfere with financial interests of the citizen.

Also it is well established (cf. [3]) that the very act of being monitored can have impact on mental health and performance, promotes distrust and breeds conformity.

In short, citizens are interested in

- *physical wellbeing and health*
- *financial profit*
- *convenience*
- *legitimate use of personal data*
- *non-disclosure of personal data to peers of the citizen*
- *not being monitored.*

External. *Externals are persons who do not have privileged access to the IT systems, and are willing to break laws, security constrains and norms in order to promote their interests.*

If the external is in some kind of relationship to the citizen, like a friendship or business partnership, the external can have a direct interest in gaining information about the citizen in order to increase their power.

Another common interest of an external is financial profit. For example they want to obtain access to critical systems to steal sensitive data or to get the system under their control. Controlled systems could be leased as part of a bot net. Stolen data could simply be sold as is or used for illegitimate purposes, e.g. spam or phishing attacks - or excessive data mining.

Because local authorities are involved in the general outline of the Live+Gov system, the possibility for politically motivated attacks is given.

Externals could want to harm or destroy the systems in order to damage the reputation of local authorities (politicians or other officials) or to make a political statement of their own.

Another possible motivation for external activities could be social appreciation. A hacker could attack critical infrastructure just to prove his skills.

In short, externals are interested in

- *increase power over citizen*
- *financial profit*
- *political activism*
- *social standing.*

System Provider. *System Providers operate the technical infrastructure (hardware and software) of the IT System. They are private companies and legal persons in their own right, but also employ a number of people with diverging interests, including: administrators, who maintain and operate the running system; programmer/developer, who develop the system; a support manager, who handles customer relations.*

As companies, they are interested in gaining financial profit. Among other things, this depends on customer satisfaction, employee happiness and task complexity. Unsatisfied customers may not want to pay for the service or do not continue the business relation. Moreover, unsatisfied customers can create a bad reputation, which affects the market for future customers.

Customer satisfaction is connected with the quality of the offered product or service. This quality depends on the happiness of employees. Employees have a claim to professional excellence. They want to deliver a good job within their means. If employees cannot satisfy their demand for professional excellence, they might get discontent and deliver poor work. Moreover, unhappy employees can produce higher costs through sick days. The worst case scenario could be, that a discontent employee gets angry and steals data or harms the running systems.

At last, the financial success of system providers depends on the task complexity of the maintained infrastructure. The complexity of a task has to be in reasonable bounds,

so that system providers can complete it within time, with a satisfying quality. If a task has a higher complexity than expected, financial loss is almost certain. Either System Providers need to hire additional competence to meet schedule and requirements. Or system providers they stress the time-line, which also results in a higher man-hour salary ratio and additionally endangers customer satisfaction. Ultimately, high task complexities can affect employee happiness, if employees cannot complete it within their claim to professional excellence.

In short, System Providers are interested in

- *financial profit*
- *good working conditions*
- *professional excellence*
- *manageable complexity.*

Local Authority. *Local authorities are public offices (ministry, agency, department, ...) or other external public entities which act as direct customers of service providers. They purchase a system specialized for their needs. For example a department for urban mobility, orders a system to better understand usage patterns and make improvement to the urban traffic flow.*

Such systems are investments, and so naturally local authorities are interested in a profitable return, like increased ticket sales. However, the return of investment is not directly of financial nature. Like service providers their financial gain depends on customer satisfaction. Customers for local authorities are either citizens, who use their services, or politicians, who order their services. The satisfaction of both sides is interdependent.

Citizens are satisfied customers if the services, e.g. public mobility, work well. If citizens are happy, it is more likely that politicians gain reputation, as they organize the public services through local authorities.

The first important step of improving the public services is by obtaining business intelligence. For the urban mobility scenario the Live+Gov systems provide insight in form of traffic jam detection and usage pattern mining, which allow local authorities to focus their efforts to the most important sites.

Additionally, since local authorities act like corporations comparable to service providers, they are also interested in good working conditions. Discontent employees may harm the system by e.g. disclosure of privacy sensitive data.

In short, local authorities are interested in

- *financial profit*
- *political reputation*
- *business intelligence*
- *good working conditions.*

Conflicts of Interests *This section outlines the Conflicts of Interests (Figure 6) between the actors of the proposed IT system architecture.*

The individual interests of all actors is already described in the previous section and are not elaborated any further. The emphasis here is put on prominent existing conflicts, because they provide a foundation for vulnerabilities and subsequent threats.

System Complexity vs Privacy. *System Providers offer a service to Local Authorities, which is to provide and maintain a monitoring and mining system, e.g. for public mobility. This system shall produce business intelligence, so that Local Authorities can improve their public services. This task in it self has a high technical complexity*

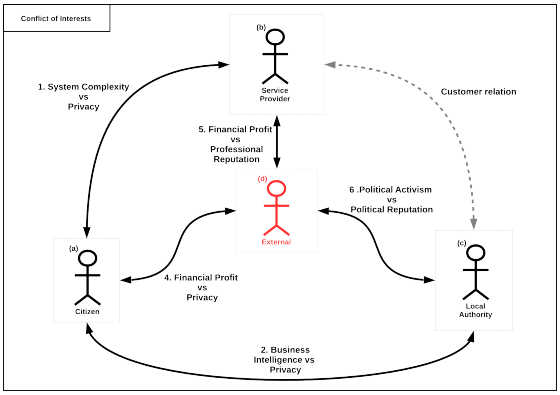


Fig. 5. Live+Gov Conflicts of Interests

and is the sole asset with financial return for System Providers. However, this task operates on privacy sensitive data provided by monitored Citizens. In order to ensure their privacy, System Provider would have to implement additional mechanisms, which allow Citizens to exercise control of their data. This will not only raise the complexity of the monitoring and mining system, System Providers also have to layout the complexity in a comprehensible manner. To effectively enable Citizens to preserve their privacy, they need to know what happens with their data.

Business Intelligence vs Privacy. *Local authorities order a monitoring and mining system from system providers, which allows them to produce business intelligence for public services. The system is an investment for local authorities, so they are interested in as much intelligence as possible to achieve a profitable return.*

The gained intelligence is the result of data mining conducted on privacy sensitive data of participating citizens. They are interested in the successful usage of their data, in a sense that they are also benefactors, e.g. improvement of public mobility. The main interest of citizens lies in maintaining control over their data and protecting their rights to privacy. In order do that, they need full disclosure of the processing steps and the purposes their data is used for, and to be given a choice whether such processing should be allowed for their own data.

Power of External vs. Privacy. *Externals which are in a social relation to the citizen can have an interest in obtaining further information in order to gain power. In the most simplistic example this could be a man wanting monitor the activities of his spouse. Another example is a Government spying on it's citizens in order to suppress opposition. An additional twist in the last example is, that there can be legal regulations that require the service provider to support the Governments invasion of the citizens privacy.*

Financial Profit of External vs Privacy. *Externals can gain financial profit from stealing privacy sensitive data. For example by selling raw contact information to advertisers or by selling mined data to insurance companies, or intermediaries like scoring companies. In such cases, citizens lose complete control over their data.*

Financial Profit of External vs Reputation of System Providers. *Externals have various business models as optional foundation for attacks on System Providers. For instance, they can try to invade the infrastructure for e-espionage reasons, to get*

control over servers to create a bot-net or to steal user data. All these approaches are motivated by financial interests. Gathered information can be sold, zombie servers can be leased.

A successful attack proves the technical competence of system providers wrong and subsequently harms their professional reputation. This can lead to a loss of future customers or a decrease of stock price for registered companies. Eventually also the financial interests of system providers are endangered.

Political Activism vs Reputation of Local Authority. *Besides monetary reasons, externals can be motivated by political reasons to attack the monitoring and mining system. Externals can break the system to make a political statement of their own, or they can steal user data to prove the system insecure. Both would harm the reputation of local authorities, who endangered the privacy of the citizens.*

Vulnerabilities *This section outlines the vulnerabilities (Figure 7) of the proposed monitoring and mining system. Note that vulnerabilities are not necessarily of technical nature. The weaknesses of IT systems are often created due to misuse or misconfiguration of the various components by one or more actors.*

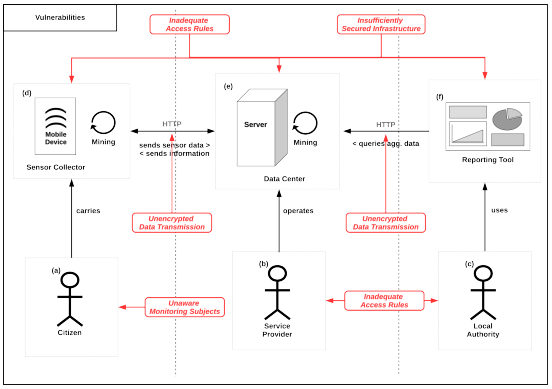


Fig. 6. Live+Gov Vulnerabilities

Insecure Infrastructure. *The proposed monitoring system consists of many hardware and software components, each with its own concrete weaknesses. For instance, operating systems can be outdated or not subject to frequent updates or virus scans. Web-applications can be carelessly implemented and not protected against SQL-Injections or Cross-Site-Scripting attacks. Databases can be ill-configured, so that access from outside the system is possible. All those weak points can be subject to various known exploit techniques.*

Insecure Data Transmission. *The proposed monitoring and mining system uses HTTP to exchange data between the Sensor Collector, the Data Center and the Report Tool. Per default, HTTP is a clear text protocol. This means, one can intercept the connection and read all sensitive information, which is send between the components. That is: passwords, raw sensor data and data mining results*

Unhappy Employees.

An Employee that is frustrated with his situation for a long time period constitutes a security vulnerability. On the one hand he might want to harm his employer directly, on the other he is increasingly susceptible for social engineering.

Inadequate Access Rules. *The proposed IT system infrastructure has various accesses to privacy sensitive data. System Provider staff has access to Data Center hardware and software like databases, web-servers and other inspection tools. Local Authority staff has access to the Report Tool. This all enables staff members to have potential access to privacy sensitive information. Those accesses have to be secured against unauthorized third parties. Moreover, we need to ensure that no single person has to many access rights. For example, a system administrator should not be able to secretly download the whole database on a flash-drive.*

Unaware Monitoring Subjects. *We define privacy as one's ability to control information about oneself. In order to do that, monitored subjects need to know, that they are monitored, who monitors them, what information is recorded and for what purposes. Subjects who are not aware of these things cannot effectively preserve control and thus lose their privacy. This vulnerability expresses itself as the lack of information material like a Privacy Policy including concise information about applied processing steps, access rules and disclosure to 3rd parties.*

5.2 Step 2. Potential Analysis

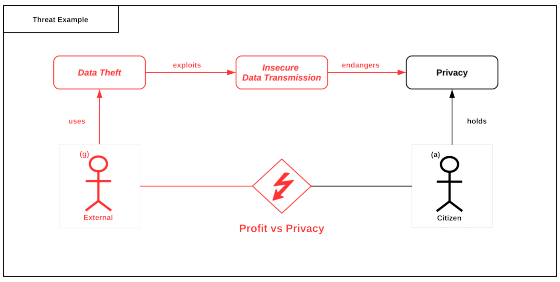


Fig. 7. Threat Example

Threat Specification *Recall from the security model description in Section* **??**, *that a threat is a potential interaction of the components that targets an asset. We restrict ourselves to the case of attacks, and the asset of privacy. An attack is an interaction that is executed by an actor in response to a conflict of interest by exploiting a vulnerability of the system. The alternative interaction of accidents are less relevant for us, since the violation of privacy always requires an actor that takes advantage of personal data.*

In Figure 8 we illustrate the structure of threats at the example of "Data Theft". Here the attack is executed by an external person, that harms the privacy of the citizen. He is motivated to do so by financial profit gained by selling personal information, which is in conflict with the citizens interest in his privacy. To get hold of the data the external exploits an insecured HTTP transfer of recorded data.

In this section we describe, in a similar fashion, threats for the citizen privacy in the Live+Gov system. This list can necessarily not be complete, but we make a best effort to cover the most relevant cases.

Threat	Conflict of Interest	Vulnerability	Affected Data
Insufficient Control Features	Privacy vs. System Complexity	Missing Privacy Awareness	All collected data
Exessive Data Mining	Privacy vs. Business Intelligence (LA), Privacy vs. Financial Profit (SP)	Lax data handling policies Missing Privacy Awareness Weak law enforcement	Mined Information
Data Theft	Privacy vs. Financial Profit Reputation (SP) vs. Political Activism Reputation (LA) vs. Political Activism	Insecure Infrastructure, Insecure Communication	Transmitted data Data stored in data center
Surveillance	Privacy vs. External Power	Insecure Infrastructure Insecure Communication	Transmitted data Data stored in data center
Information Leak	Privacy vs. Financial Profit Reputation (SP) vs. Political Activism Reputation (LA) vs. Political Activism	Unhappy Employee Lax Access Rules	Data stored in data center
Social Engineering	Privacy vs. Financial Profit Reputation (SP) vs. Political Activism Reputation (LA) vs. Political Activism	Unhappy Employee Lax Access Rules	Data stored in data center

Fig. 8. Threats

T1. Insufficient Control Features. *The System Provider does not offer tools for the Citizen to control his data. However, besides the missing features he provides a safe and secure system. This threat contradicts the definition of privacy as control over one's information about oneself. As soon as collected data of Citizens is stored on System Provider servers, all control over that data is lost. This is not necessarily due to bad intention, System Providers may simply have forgotten to include such features during the development process. Although, control capabilities for Citizens add to the system complexity, which could motivate to omit those. Therefore interests of Citizens and System Providers are in conflict, namely it is the Citizen's Privacy vs. System Complexity for System Providers. This is an abstract threat provoked by a general Missing Privacy Awareness in the minds of all actors in the Live+Gov context.*

T2. Excessive Data Mining. *The System Provider and/or the Local Authority secretly extract more private information from the collected data, than the Citizen agreed to. But results of the mining process create no disadvantages for Citizens, because there is no disclosure to third parties. This could be the case for a System Provider, who wants to test a new product and uses the pre-existing data collection. Or for a Local Authority, who wants to analyze the data collection regarding fare evasion. However, the Citizen has not agreed to such data processing nor could he, since it is conducted secretly. This disables a Citizen to control his data adequately. Thus there are two possible conflicts: Privacy vs. Financial Profit of Serivce Provider and Privacy vs. Buisness Intelligence of Local Authority The threat can be provoked by either lax data handling policies of both System Providers and Local Authorities, or a weak law enforcement of existing supervision. But the main issue, which can lead to such threats, is again a general Missing Privacy Awareness.*

T3. Data Theft *An External infiltrates infrastructure in order to steal personal data and sell it on the black market. Also the External might be motivated politically and wants to harm the reputation of the System Provider or the Local Authority. Anyways, this threat would be manifested through a technical attack on either hardware (Packet Capture) or software (buffer overflow, SQL injection). Such a successful attack could harm the reputation of both System Provider and Local Authority. The technical competence of System Providers would be proven wrong, therefore they would lose professional reputation. Local Authorities would lose their political reputation, as it would seem like they had endangered data of Citizens, which lose complete control. Thus this threat is*

defined by three conflicts: Privacy vs. Financial Profit, Reputation of Service Provider vs. Political Activism and Reputation of Local Authority vs. Political Activism. Also this threat describes the classical scenario, where attacks are provoked by Insecure Infrastructure (SQL injection) and Insecure Communication (Packet Capture).

T4. Surveillance

An External infiltrates infrastructure in order to obtain information about the citizen and exploit it directly. In this scenario the external is supposed to have some direct relationship to the citizen which motivates his interest to obtain personal information. Examples could be a public institution that wants to gain information about planned activities of the citizens (e.g. Nixon's Watergate scandal or the recent prosecution of Guardian journalists by GHCQ). Another example is an insurance company that seeks to get information about the citizens life-style in relation to the insured risk, like car accidents or health hazards.

In this threat the privacy interest of the citizen is in conflict with the aspirations for power over the citizen by the externals.

T5. Information Leak

Like an external person the Data Theft Scenario an employee of the service provider or the Local Authority has selfish interests to gain money, make political statements or harm his employer. In order to pursue this interest he can steal personal data and sell it or release it to the public. The corresponding conflicts of interests are: Privacy vs. Financial Profit of the Employee, Reputation of Service Provider vs. Political Activism of the Employee and Reputation of Local Authority vs. Political Activism of the Employee. The vulnerability constitutes of the existence of Unhappy employees itself and possibly lax access rules that enable the employee to obtain large amounts of data unnoticed.

T6. Social Engineering

This scenario an external manipulates an employee of a Service Provider or the Local Authority to leak information to the external person. It is thus combination of the Data Theft and Information Leak scenario. The conflicts of interest are Privacy vs. Financial Profit of the External, Reputation of Service Provider vs. Political Activism of the external and Reputation of Local Authority vs. Political Activism of the external. The exploited vulnerabilities are, again, the existence of Unhappy employees and possibly lax access rules that enable the employee to obtain large amounts of data unnoticed.

Threat Risk Evaluation *In this section we will associate to every identified threat a corresponding risk. Recall from* **??** *that a risk is the expected loss that is associated to the threat. Therefore, we have to quantify the likeliness of the threat to occure and the harm or loss done in this case. The quantification of likeliness will be solely based on rough judgment of the authors. The quantification of loss, will be made in a two step process. For each threat listed in table* **??**, *we have analyzed the affected personal data of the citizen. For each possible data type (e.g. GPS) we analyze the impact on the seven different types of privacy in Section 3.3. In combination we can quantify roughly the impact of each threat on the citizens privacy. Both evaluations are necessarily fraught with a high level of uncertainty.*

For the quantification of the loss in case of a threat scenario we use the following rough calibration:

- *3: High. Leak of information to peers (e.g. public) which impacts citizen.*
- *2: Medium. Undisclosed processing of personal data or disclosure to third parties that are unrelated to subject.*

- *1: Low. Loss of control over data.*
- *0: None*

For the quantification of likeliness the following scale is used:

- *4: Always.*
- *3: High. Occurs once in 10 cases*
- *2: Medium. Occurs once in 100 cases*
- *1: Low. Occurs once in 1 million cases*
- *0: Impossible*

The quantification of the risk, we add the values for loss and likeliness of the corresponding threats. Note, that loss and likeliness scales have a logarithmic character, so that that addition of those scales corresponds to multiplication of the usual scales.

The likeliness, loss and the resulting risks assigned to the threats are discussed in the following paragraphs and summarized in Figure 10.

T1. Insufficient Control Features. *The occurrence of this threat is dependent on the design on the system and given in our case, since we do not give the citizen control over his data once it is recorded. Therefore the Likeliness is evaluated as* 4 *(Always). The associated, risk is* 1 *Low on our scale, since no direct harm is done to the citizen by exploiting the data.*

Hence the resulting risk is calculated as $4 + 1 = 5$.

T2. Excessive Data Mining. *We assess the likeliness of excessive data mining to be* 3 *High, since these kind of analysis can be performed within the walls of the service provider, without somebody else noticing, and the service provider himself has an interest in this activity.*

The associated loss, on the other hand can be substantial (Medium 2*). For example when GPS data is linked to data from telephone books the identity of the citizen can be revealed and personal details like visits to doctors. In the threat scenario, this information is not leaked to third parties, (which would justify an even higher loss assessment), but the very existence of this information violates the citizens privacy.*

Hence the resulting risk is calculated as $3 + 2 = 5$.

T3. Data Theft. *The likeliness of a targeted attack by a third party is dependent on the popularity of the offered service and financial value of the captured information. Moreover, the amount of manual work required to infiltrate a custom build system is significantly higher that that of compromising a standard software solution. In the scenario we assume a moderate popularity in a single metropolitan area, with around 10.000 users and storage of data of only limited financial value (no addresses, no payment information). Therefore the likeliness assessment is* $1 - 2$ *(Low-Medium).*

The harm of leaked information to a criminal party is 3 *High. Hence the resulting risk is calculated as* $4 - 5$.

T4. Surveillance. *In the surveillance scenario an party related to the citizen, like a company where he is customer of, or a government agency, seeks to obtain sensitive information from our service.*

The likeliness of such an intrusion is hard to asses, and depends again on the popularity of the service. If a high popularity is reached we have recently learned that spying by government agencies is very likely to occur. The barrier for companies that do not operate the infrastructure used to transmit the data a surveillance attack is however very hard to perform. Therefore we assess the likeliness of the threat with $1-2$ *(Low-Medium).*

The harm of leaked information to a related party is 3 High. Hence the resulting risk is calculated as 4 – 5.

T5/6. Information Leak and Social Engineering.

In our scenario we assume that the culture and ethics inside the service provider company and local authority are very high, so that the information leak scenario has a likeliness of 1 (Low).

The harm of such an information leaked is 3 High, so that the resulting risk is calculated as 4.

Threat	Likeliness	Loss	Risk	Recommendation
T1. Insufficient Control Features	4	1	5	R1, R2
T2. Excessive Data Mining	3	2	5	R3, R4, R5
T3. Data Theft	1 - 2	3	4 - 5	R6
T4. Surveillance	1 - 2	3	4 - 5	R7
T5. Information Leak	1	3	4	R8
T6. Social Engineering	1	3	4	R8

Fig. 9. Live+Gov Risk Evaluation and Recommendations

Privacy Recommendations *In the preceding section we have identified the main risks for the users privacy. In this section we derive recommendations or requirements for a system that addresses these risks. Some of these requirements are implemented as security measures in our systems and discussed in the following chapter* **??**.

In order to address the threat with the highers risk, Insufficient Control (T1) of the citizen, we need to give the citizen back the control over its data inside the system. The most direct way to do this is to provide a web-based Privacy Dashboard (R1) *which allows the citizen to view, edit and delete all information about his person that is stored inside the system. Also control applied processing and disclosure of the data to third parties should be given to the user, at least in the form of an opt-out or veto option.*

A necessary pre-requirement for effective control of the citizen over his data is information and comprehension of the intended data capturing and processing steps. Therefore a Privacy Policy (R2) *that is easily readable and contains all important information is essential. Moreover, the existence of a Privacy Policy is a legal requirement (cf. Section* **??**).

The threat with the second largest risk is (T2) Excessive Data Mining. Contrary to common belief, it is neither legal nor ethical to process personal data for by new methods or for new purposes that were not stated and explained to the citizen at the time of data collection. Also the common practice of obtaining far-reaching permissions from the citizens inside the privacy policy is neither an ethical or legal solution to the problem (cf. Art. 6 in Section **??**).

To address this threat awareness about the limitations of data processors inside the company is a key element. As one mean to establish such a culture of privacy respect, we recommend to prepare an document called Data Handling Guidelines (R3) *intended for internal use that explains the concrete processing steps and purposes that are permitted by the citizens. This guideline should also be structured in a way that it covers the legal notification requirement from the EU Data Protection Directive (cf. Section* **??**). *In*

particular the following information should be provided for each processing task: The name of the controller, purpose of processing, description of the data categories, recipients of the data if disclosed, transfer to third countries and a description of security of processing.

If further processing should be performed, it is necessary to seek additional permissions from the citizen. A simple email explaining the planned processing steps, and asking for permission (R4) *would be enough for this purpose. The permission can be given via an embedded link that shall be followed in order to signal agreement.*

An alternative measure to address the risk of excessive data mining is the anonymization (R5) *of data. When all direct- or indirect links to the identity of the person are removed, no violation of the citizens privacy caused by arbitrary processing. However removing all such links is a challenging tasks, and full anonymity is often not achieved, cf. [10].*

The protection from threat scenario (T3) Data Theft is a case of classical IT infrastructure security (R6)*. The storage and processing infrastructure has to be secured using firewalls, up-to data software versions and proper authentication mechanisms.*

The protection from threat scenario (T4) Surveillance focuses on the communication channels. They are target of wiretapping attacks by intermediaries or externals with access to the communication infrastructure. Strong encryption (R7) *should be used to make it harder for externals to read the content of the transmitted data.*

Threat scenarios (T5) Information Leak and (T6) Social Engineering target the vulnerability of unhappy employees. Therefore a trustful, healthy company culture (R8) *should be maintained.*

In summary we recommend the following measures to secure the citizens privacy:

R1 Privacy Dashboard. A tool which allows the citizen to view, edit and delete all data personal data that is stored in the system.
R2 Privacy Policy. A document, that informs the citizen about the collection and processing of personal information. It should at least contain the legally required information.
R3 Issue Data Handling Guidelines that explain the permitted processing methods and purposes.
R4 Ask the citizens for permissions before applying further processing via Email.
R5 Anonymize personal data before processing.
R6 Securing of Storage and Processing infrastructure using e.g. firewalls.
R7 Securing communication channels using encryption.
R8 Maintain a healthy, trustful relationship with your employees.

The mapping of these recommendations to the threats is summarized in Figure 10.

6 Conclusion

```
TODO: later.
* Key aspect control, can be given back to citizens via ‘‘Privacy Dashboard’’
```

References

1. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. Dependable and Secure Computing, IEEE Transactions on 1(1), 11–33 (Jan 2004)

2. Bodorik, P., Jutla, D.N.: Sociotechnical architecture for online privacy. Security & Privacy 3, 29–39 (2005), http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=1423958
3. Chambers, C.: Nsa and gchq: the flawed psychology of government mass surveillance (2013), http://www.theguardian.com/science/head-quarters/2013/aug/26/nsa-gchq-psychology-government-mass-surveillance
4. Clarke, R.: Introduction to dataveillance and informatin privacy, and defintions of terms (1997), http://www.rogerclarke.com/DV/Intro.html, http://www.rogerclarke.com/DV/Intro.html
5. DeCew, J.: Privacy. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy. Fall 2013 edn. (2013), http://plato.stanford.edu/archives/fall2013/entries/privacy/
6. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European Data Protection: Coming of Age. Springer Netherlands (2013), http://link.springer.com/chapter/10.1007%2F978-94-007-5170-5_1
7. Fried, C.: Privacy: A rational context. In: An Anatomy of Values, pp. 137–152. Havard Univ. Press (1970)
8. Grimm, R., Simić-Draws, D., Bräunlich, K., Kasten, A., Meletiadou, A.: Referenzmodell für ein vorgehen bei der it-sicherheitsanalyse. Informatik-Spektrum (2014), http://link.springer.com/article/10.1007%2Fs00287-014-0807-3
9. Gutwirth, S.: Privacy and the information age (2002)
10. Krumm, J.: A survey of computational location privacy. Personal and Ubiquitous Computing 13(6), 391–399 (2009)