A Privacy Aware Mobile Sensor Application

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

University of Koblenz-Landau

Abstract. In our research work we have implemented a privacy aware mobile sensor application [diesen ersten Satz ggf. wieder streichen]. In this paper we outline a scenario of a mobile traffic survey and analyse its privacy risks according to a reference model for IT security analysis. This leads to concrete recommendations for privacy protecting measures that are implemented in the system, for example a Web-based dashboard which allows the users to view, modify and delete all personal data that is stored in the system.
Vorschlag HH: In this article we analyze the privacy aspects of a mobile sensor application used for recording urban travel patterns as part of a travel-survey service. This service has been developed and field-tested within the Live+Gov EU Project. The privacy analysis follows a structured approach established in [8]. Eight privacy recommendations are derived, and have already led to corresponding enhancements of the travel-survey service.

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

1 Introduction

The rise of mobile smart-phones equipped with a wide range of sensors and the abundance mobile internet connectivity has paved the way to a whole new generation of mobile services which ease the daily life of citizens using them. Apps like Google Maps[1] allows the user to navigate effectively in unknown cities; others track sports activities in order to optimize training plans or engage in virtual competitions.

Besides the immediate benefits these services reveal a wealth of private information about the citizen that capture a very detailed picture of his life. For instance, GPS location tracking can be used to infer shopping habits or associations with political groups (when meetings are attended) and accelerometer data can be used to detect medical conditions like walking disabilities. All this data is highly sensitive to the citizens privacy and can be used against the citizen if it falls into the wrong hands.

Providers of these new services are faced with a fundamental trade-off between features and convenience of the service and the protection of the citizen's privacy. The service has to collect enough data to support the basic service

[1] `http://www.google.com/mobile/maps/`

promises. If too much data is collected the privacy of the citizen is put at risk, with immediate implications for the customer trust relation and the acceptance of the service. Also leaks of private data can jeopardize the whole business.

In this article we study the privacy risks of a travel-survey service for urban mobility.

2 Scenario Description: Mobile Traffic Survey

Travel surveys are regularly conducted travel agencies which provide public transportation infrastructure. With these surveys the current usage of the public transportation system is assessed and the insights are used for future planning of bus, tram and subway lines, etc.. For each survey a large number of citizens (e.g. 5000) is asked to keep track of their travel patterns for a constraint period of time (e.g. one month). Traditionally the travel patterns have been recorded manually in the form of travel diaries. Modern smart-phones are equipped with a wide range of sensors (in particular GPS) that allow the recording of travel-patterns in a fully automated way.

Within the Live+Gov EU project, we have established a first prototypical implementation of such an automated travel-survey service. In this section we give a high level description of the generic service architecture. This description along with the introduced terminology will serve as a basis for our privacy analysis.

There are three stakeholders involved in the travel-survey service: The *citizen*, the *service provider* and the *travel agency*. The service provider is the operator of all IT systems and offers the travel-survey service to the travel agency. Figure 2 contains a schematic visualization of the relation between these stakeholders.

The citizen is a volunteer who is willing to share his personal travel patterns within the travel-survey event. He carries a mobile smart-phone which runs the *sensor collector application*. The application collects data from various sensors available on modern smart-phones. In particular accelerometer- and GPS-samples are collected. Based on the accelerometer data, the application extracts human activities (e.g. running, walking, standing). Also, the application can send raw-sensor data back to a central data center.

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. In particular, the data center determines if the citizen is using public transportation and if so which lines of service (bus, train, tram) are used. The data center can also sent mining end products and messages (e.g. traffic jam reports, bus schedule) back to the mobile device of the citizen.

The *service provider* provides and operates all technical infrastructure like the data center and the sensor application. He also operates a web-based *reporting tool* that aggregates information about travel patterns of citizens within the travel-survey. The reporting tool is used by the travel agency to gain insights for planning and accounting of the public transportation infrastructure.

3 Definition of Privacy

3.1 Privacy and Self Data Protection

More than one hundred years ago, 1890, the American politician Louis Brandis had specified privacy as the right to be left alone [**?**]. From the data processing point of view, this right is best expressed by the absence of information about a person in the mind of others. Indeed, this principle of "data minimization" is still fundamental to modern data protection legislation. The modern principles of data protection are codified by many legal systems in different countries, especially in Europe [**?**], and by the US save harbor principles. However, modern data protection is more than only the absence of personal data. It is based on the personal right on self-determination over information and communication [**?**]. This is, for example, very well expressed by Fried's definition of 1970:

> 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]

In order to realize this requirement in the modern IT world users are provided with user control functions, for example to decide about the access on their data for future use, and to view, modify, and delete unwanted data that had been collected. In its fundamental decision of May 13, 2014, the European Court has convicted Google to accept user demands to delete links to incorrect or irrelevant personal data in the Internet (C-131/12 – Google Spain SL). Such functions would constitute a so-called self-data-protection. It requires users to be highly aware of their rights and how to use them. Complementary, system-data-protection puts the load of data protection enforcement on the data collectors, ideally even without bothering the users. Typical system data protection functions are the deletion of personal data that are not bound to service purpose, the anonymization of personal data for research, and the abstinence from forwarding personal data to third parties. Together, system-data-protection and self-data-protection are supposed to provide a fair balance between the interests of service providers and their users. In our research work we focus on self-data-protection according to Fried's user control requirement [7]. A system data protection point of view would lead to other results, namely to a set of obligations for service providers. This is subject to further research.

3.2 The Seven Types of Privacy

In Fried's definition of privacy as control over information, the specification of what constitutes 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 categorization by Friedewald, Finn and Wright of 2013 called the Seven Types of Privacy [6]. These are an extension to the four types of privacy by Roger Clarke of 1997 [4]. It is important to note, that these categories are not mutually exclusive.

For instance a written email is considered personal communication as well as personal data stored on a computer. However, the categories are very helpful for a privacy analysis with a focus on self-data-protection. The seven types of privacy are as follows:

1. Privacy of the Person (with respect to body functions and body characteristics)
2. Privacy of Behavior 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 of Association (with persons, e.g. friends, and organizations, e.g. political parties)

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 1 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. 1. 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 Privacy Analysis

The goal of this chapter is to analyze and identify the threats 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.

In our analysis 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 organizes a common security terminology in a reasonable and practical way. The procedure describes a method for analyzing the IT system based on that model. The reference model provides four views: (1) the real world of persons and their assets, (2) the potential world of requirements and threats, (3) measures and plans specified by programs, business models and attack strategies, and, finally, (4) events of running programs, data accesses and performed attacks as well as their defense. In the following sections we apply the proposed procedures of the reference model to our scenario of a travel service that collects personal data from mobile users in order to serve the users and to enhance the service. The service intends to respect the privacy of its users.

In sections 4.1 and 4.2 we apply the first two steps of the reference model [8], which are related to the views on the real world and on the measures and plans. In section 4.3 we apply the third step of the reference model by providing specific privacy recommendations and requirements as a result of the previous analysis that the system must comply with.

4.1 Step 1. World Analysis

The first step is the *world view* where all components are described in their current state. It consists of the following components: Assets, IT-Systems, Actors, Conflicts of Interests, Vulnerabilities, and Interactions.

The relevant **IT-Systems** were already described in Section **??**. **Interactions** between assets, IT-Systems, humans, and vulnerabilites as partly described in Section **??** and will be further analyzed in Section 4.2.

Assets In this scenario we focus our attention to only one asset: The privacy of the citizen. Our definition of privacy is described in detail in Section 3.

Actors This section describes the human actors previously introduced within the IT system architecture (**??**). Although the text is only a short description, a list of the most important interests is provided for each actor.

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 (cf. [3]).

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, and 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.

A 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. Stolen data could simply be sold as is or used for illegitimate purposes, e.g. spam or phishing attacks - or excessive data mining.

In short, externals could be interested in: increase power over citizen, financial profit, political activism, and their 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, programmer/developer, and a support manager.

As companies, they are interested in gaining financial profit. 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.

System Providers are interested in: financial profit, manageable complexity, professional excellence, and good working conditions.

Local Authority. Local authorities are public offices (ministry, agency, department, ...) or other external public entities which act as direct customers of

service providers. 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.

Local authorities are interested in: financial profit, political reputation, business intelligence, and good working conditions.

Conflicts of Interests Different actors have different interests which can be in conflict each other. This section outlines the Conflicts of Interests 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, so that Local Authorities can improve their public services. This task in it self has a high technical complexity and operates on privacy sensitive data provided by monitored Citizens.

Business Intelligence vs Privacy. Local authorities order a monitoring and mining system from system providers as much as possible, which allows them to produce business intelligence for public services. They are interested in the successful usage of their data, although the interest of citizens lies in maintaining control over their data and protecting their rights to privacy.

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.

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 network or to steal user data. A successful attack proves the technical competence of system providers wrong and subsequently harms their professional reputation.

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 2) of the proposed monitoring and mining system.

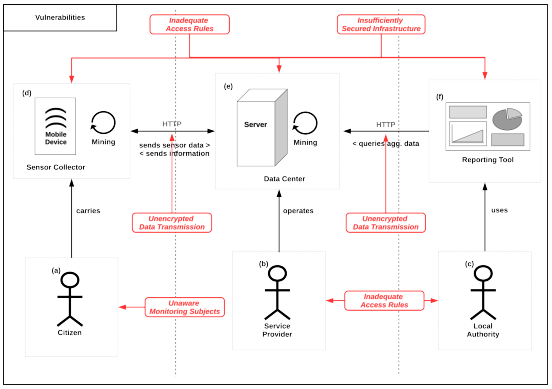

Fig. 2. Overview of vulnerabilities of the Live+Gov System; legend see **??**

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.

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. Data can be intercept and read all sensitive information, which is send between the components e.g. 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.

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.

4.2 Step 2. Potential World Analysis

The *Potential World Analysis* displays the intended and unintended interactions of the components in the world view.

The intended interactions support the underlying business objectives. Unintended interactions can lead to threats. Obviously this provides a conflict of interest with the victim's business model, to keep the asset away from unauthorized access. From the point of view of the victim, an attack would be an unintended interaction.

The potential world view consists of the following components: Business Objectives, Threats, hances/Risk, and Security Requirements. **Business Objectives** of the system owner were already described in Section **??** and 4.1. **Security Requirement**s are included to our analysis in Section 4.3.

Threats 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. We describe threats for the citizen privacy in the system. This list can necessarily not be complete, but we make a best effort to cover the most relevant cases.

T1. Insufficient Control Features. As soon as collected data of Citizens is stored on System Provider servers, all control over that data is lost. 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.

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.

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. Such a successful attack could harm the reputation of both System Provider and Local Authority. 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). 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.

Chances/Risk In this section we will associate to every identified threat a corresponding risk. 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 the previous section, 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 between 3 (high) and 0 (none). For the quantification of likeliness the following scale between 4 (always) and 0 (impossible) is used. 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 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 3.

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).

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. 3. Live+Gov Risk Evaluation and Recommendations

4.3 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..

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 and a legal requirement.

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. 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. 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 3.

5 Conclusion

Our goal was to find a balance between the demand of the Local Authority for location-based data to improve their public services on one side, and to keep the privacy of citizens as untouched as possible on the other side. In a structured manner we identified all actors and what kind of conflict of interests can occour. Doing this, we found potential risks and provided finally specific recommendations how to protect the citizen's privacy. One central idea of these recommendations is to give the citizen as much control over their data back

as possible. This can be e.g. done via a Privacy Dashboard that gives a full overview about all personal data that is stored on the system. By implementing these privacy recommendations we found a way to satisfy the above-mentioned demand of both sides and comply with legal data protection requirements in addition.

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)