Towards a Privacy Scorecard – Initial Design Exemplified on an Intelligent Transport Systems Service

Aida Omerovic, Marit Kjøsnes Natvig and Isabelle C. R. Tardy
SINTEF, Norway
{aida.omerovic, marit.k.natvig, isabelle.tardy}@sintef.no

Keywords: Privacy Compliance, Privacy Scorecard, Intelligent Transport Systems.

Abstract: Increasingly many services depend on access to data that are traceable to individuals, the so-called "personally identifiable information" (PII). The ecosystem of PII-dependent services is growing, becoming highly complex and dynamic. As a result, a wide variety of PII is constantly collected, stored, exchanged, and applied by all kinds of services. Practice of PII handling among service providers varies, as does the insight and influence of the end-users on how their own PII is treated. For a user, privacy represents a condition for his/her trust and service adoption. It is moreover essential for a service provider to be able to claim privacy awareness over time. This is particularly important as the new EU privacy regulation is about to become operative, thus enforcing strict privacy requirements on the service providers and giving new rights to the users. In order to preserve user trust and manage the technical and legal privacy requirements, a practically usable support to continuously and transparently plan and follow-up privacy compliance, is needed. To this end, we propose an initial version of a so-called "Privacy Scorecard", that is, a decision support for a service provider aimed to facilitate identification, specification, measurement and follow-up of fulfilment of privacy goals in a relatively transparent and comprehensible manner. In this position paper, we present initial design and intended usage of the Privacy Scorecard. We also exemplify how it can be applied to a concrete service. The initial findings indicate feasibility of the approach and suggest directions for further work, including refinement of the scorecard design and usage guidelines, tool support for visualization, as well as further empirical evaluation.

1 INTRODUCTION

Digital services increasingly rely on Personally Identifiable Information (PII). It places PII at the cornerstone of the realization of these services. The emerging service innovations from domains such as smart cities, telecom, social media and entertainment, all depend on PII. For users privacy represents a condition for his/her trust, and for service providers it is essential to be able to claim privacy awareness as a prerequisite for their offerings. We therefore claim that efficiently and properly handled PII is a facilitator for innovation of services involving, for example, personalization and analytics, while lack of privacy compliance often is an obstacle for innovation. This is particularly important as the new EU General Data Protection Regulation (GDPR) poses strict restrictions on lawful processing of personal data, thus enforcing privacy requirements on the service providers and giving new rights to the users. Non-compliance with this regulation, which applies from May 2018, will according to the regulation result in fines up to 20 million EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (EU, 2016).

We have in our earlier research (Erdogan et al., 2016) conducted a "problem analysis" including a mapping literature study of privacy assessment methods, a case study addressing services for multimodal transport, as well as in-depth interviews of central Norwegian public and private actors involved in Intelligent Transport Systems (ITS) services. The goal was to identify state of the practice and needs for privacy assessment support in general and within ITS in particular. Our findings suggest that:

- ITS services are distinguished by location-based PII and very dynamic (due to frequently changing service interactions, usage, and technical design).
- The ecosystems of services are very complex

Omerovic, A., Natvig, M. and Tardy, I.
Towards a Privacy Scorecard – Initial Design Exemplified on an Intelligent Transport Systems Service.
DOI: 10.5220/0006284405850593
In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pages 585-593
ISBN: 978-989-758-209-7

(due to many dependencies between services and actors, PII needs to be exchanged in order for services to work as intended). E.g. in multimodal transport planning, actors/services providing different kinds of transport modalities (car, bike, bus, train, boat, plane, etc.) need to collaborate and exchange PII. Moreover, one single service may be provided, developed and operated by different actors, all handling PII.

- The (legal and technical) privacy requirements are, for most actors, complicated, demanding to understand, operationalize and follow up.
- There is a lack of transparency between the technical measures and the requirements being addressed by the measures. There is also a lack of transparency between system vulnerabilities and privacy risks.
- The user consents are not sufficiently comprehensible. They are also non-trivial to keep up to date upon changes in the services.
- There is a lack of comprehensible and transparent decision support for privacy management which would make the dynamic aspects of privacy compliance a first class citizen.

Other studies also argue that there are many privacy concerns within ITS solutions due to the wide-spread data registration, exchange of data between systems, and monitoring/tracking of persons and vehicles (Vandezande et al., 2012). Much of this data originates from connected persons and connected things associated with persons (Psaraki et al., 2012). Aggregated data may also show patterns in behaviour, who a person interacts with, preferences, and similar.

The complex and dynamic nature of ITS introduces challenges that need to be properly addressed when assessing privacy compliance of ITS. The literature however lacks methods to specifically assess privacy compliance of digital services in general and ITS services in particular.

State of the art suggests several general Privacy Impact Assessment (PIA) methods typically based on standards such as ISO 27005 (ISO 27005, 2011), NIST SP 800-30 (NIST, 2012), ISO 29100 (ISO 29100, 2011), and ISO 22307 (ISO 22307, 2008). These methods are often too generic and carried out at a high-level of abstraction. Domain specific PIA approaches have been proposed for location-based systems (Ren et al. 2011), Vehicular Ad Hoc Networks (Friginal et al. 2014), cloud computing (Tancock et al., 2013; Theoharidou et al., 2013), Android apps (Mylonas et al., 2014) and smart grid applications (Knirsch et al., 2015). Common for both general and domain-specific PIA approaches is that they focus on identification and handling of privacy risks, rather than compliance to privacy requirements.

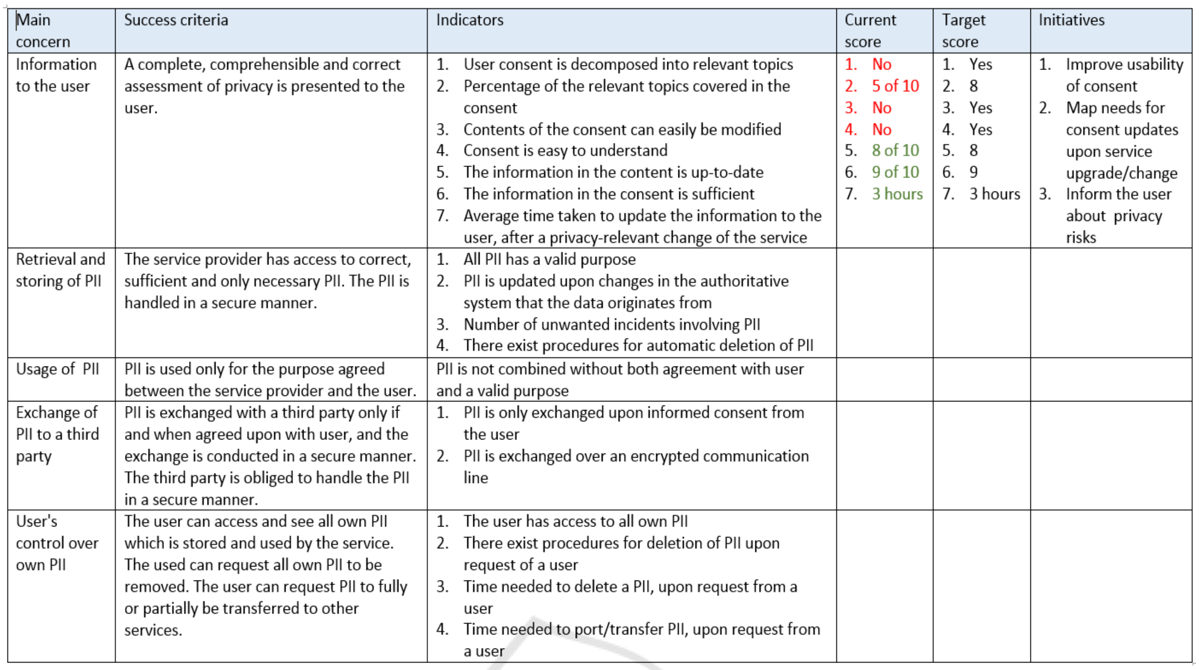
To address the above mentioned challenges, we need comprehensible decision support for privacy compliance management that will help bridge the gap between overall privacy-specific goals and the specific system design measures. It should facilitate transparency between fulfilment of privacy requirements and service design decisions. It should also reflect the impact of the dynamic properties of the services to the privacy goals. Inspired by the Balanced Scorecard (Kaplan & Norton, 1995), in this position paper we propose an initial design of "Privacy Scorecard" as an aid for privacy compliance management, aimed for service providers. The scorecard is system lifecycle agnostic, but the contents included may refer to details only available at certain stages.

Firstly (Section 2), we present a generic initial version of the Privacy Scorecard. We present how it was developed and how it is intended to be used. Secondly (Section 3), we apply the Privacy Scorecard on an example service from Intelligent Transport Systems (ITS) and report on results and experiences. Thirdly (Section 4), we discuss the findings and lessons learned from development and application of the Scorecard. We also discuss threats to validity and reliability. Finally (Section 5), we summarize conclusions and plans for further work.

2 PRIVACY SCORECARD – INITIAL DESIGN

The starting point were the results of our problem analysis, the identified needs for privacy compliance decision support, and an idea of designing a dynamic yet easily understandable "scorecard" for privacy. Three researchers (who had also been fully involved in the problem analysis) were gathered for a workshop. Each of them has at least a decade of relevant professional experience and academic degree from the respective fields, namely risk and compliance management in software engineering, system architecture of ITS (including ITS domain expertise), and communication systems in internet of things (including ITS domain expertise).

We had prior elementary knowledge about the Balanced Scorecard. The goal of the workshop was to develop a generic Privacy Scorecard that could later be instantiated on specific cases. The first step



Main concern	Success criteria	Indicators	Current score	Target score	Initiatives
Information to the user	A complete, comprehensible and correct assessment of privacy is presented to the user.	1. User consent is decomposed into relevant topics 2. Percentage of the relevant topics covered in the consent 3. Contents of the consent can easily be modified 4. Consent is easy to understand 5. The information in the content is up-to-date 6. The information in the consent is sufficient 7. Average time taken to update the information to the user, after a privacy-relevant change of the service	1. No 2. 5 of 10 3. No 4. No 5. 8 of 10 6. 9 of 10 7. 3 hours	1. Yes 2. 8 3. Yes 4. Yes 5. 8 6. 9 7. 3 hours	1. Improve usability of consent 2. Map needs for consent updates upon service upgrade/change 3. Inform the user about privacy risks
Retrieval and storing of PII	The service provider has access to correct, sufficient and only necessary PII. The PII is handled in a secure manner.	1. All PII has a valid purpose 2. PII is updated upon changes in the authoritative system that the data originates from 3. Number of unwanted incidents involving PII 4. There exist procedures for automatic deletion of PII			
Usage of PII	PII is used only for the purpose agreed between the service provider and the user.	PII is not combined without both agreement with user and a valid purpose			
Exchange of PII to a third party	PII is exchanged with a third party only if and when agreed upon with user, and the exchange is conducted in a secure manner. The third party is obliged to handle the PII in a secure manner.	1. PII is only exchanged upon informed consent from the user 2. PII is exchanged over an encrypted communication line			
User's control over own PII	The user can access and see all own PII which is stored and used by the service. The used can request all own PII to be removed. The user can request PII to fully or partially be transferred to other services.	1. The user has access to all own PII 2. There exist procedures for deletion of PII upon request of a user 3. Time needed to delete a PII, upon request from a user 4. Time needed to port/transfer PII, upon request from a user			

Figure 1: The initial generic Privacy Scorecard. The contents provided are incomplete and intended for illustration purpose. The last three columns are entirely case specific.

was design of a canvas for the Privacy Scorecard, i.e. the overall structure including columns and titles. Each column would be related to the one on its left hand side. Our leftmost (top abstraction) level was an overview of main privacy-specific concerns. Five concerns were identified:

- Quality of the privacy related information that is provided to the user.
- Retrieval and storing of PII by service provider.
- Usage of PII by the service provider.
- Exchange of PII to a third party.
- User's control over own PII.

The meaning of each main concern was elaborated through success criteria in the newt column. Once the concerns were fully understood and characterized through the success criteria, we identified a set of indicators for each concern (column three). The indicators are intended to provide quantifiable fulfilment degrees of the relevant properties of the concerns. Next, a column dedicated current score (i.e., estimated value) of each indicator is created. The target (desired) score of each indicator is expressed in the next column. Colours are used on current score values to express whether and to what degree the current indicator scores meet the target score values. Note that the scorecard assumes that each indicator is specified in more detail outside the scorecard. It is also assumed that the measurement scale of each indicator is specified in more detail outside the scorecard. A rationale for the target score should also be provided outside the scorecard. The last column lists the measures that are expected to improve the indicator scores towards the desired scores, and as such contribute to fulfilment of the privacy concerns. Figure 1 shows the resulting generic scorecard. Note that none of the columns of the generic Privacy Scorecard is intended to be complete, but rather to represent a starting point for instantiation on specific cases. Especially the last three columns will be case-specific. They are therefore only provided for exemplification purpose of first concern in Figure 1. Here, we provide main principles and a template of the approach, while instantiation is subject to domain knowledge and the special privacy goals and requirements of the service under analysis.

The intended target group for the Privacy Scorecard are service providers. The scorecard is not intended to be a substitute for privacy compliance management, but rather a complement to it. Thus, a full-scale legal and technical privacy requirements management is beyond the scope of the scorecard.

The following procedure summarizes our guidance for use of the Privacy Scorecard:

1. **Specify the Target of the Analysis.** Specify scope of the analysis, objective of the target system/service, usage, assumptions, and interactions with other systems/services. State

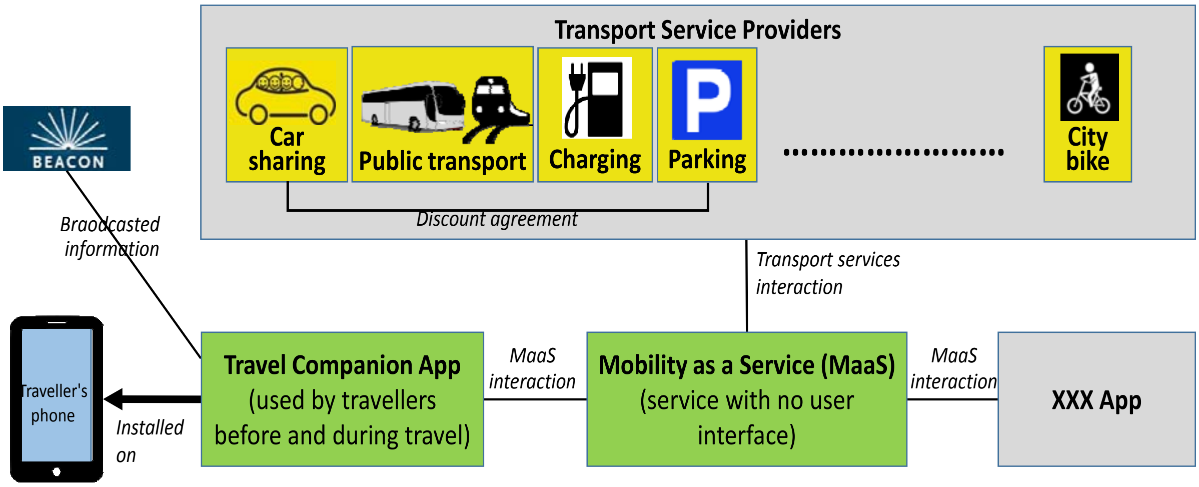


Figure 2: Mobility as a Service (MaaS) example.

who the stakeholder(s) are. State what PII is involved and how it is handled. Identify user consent practice and needs. Specify who we assess the privacy on behalf of ("commissioner").

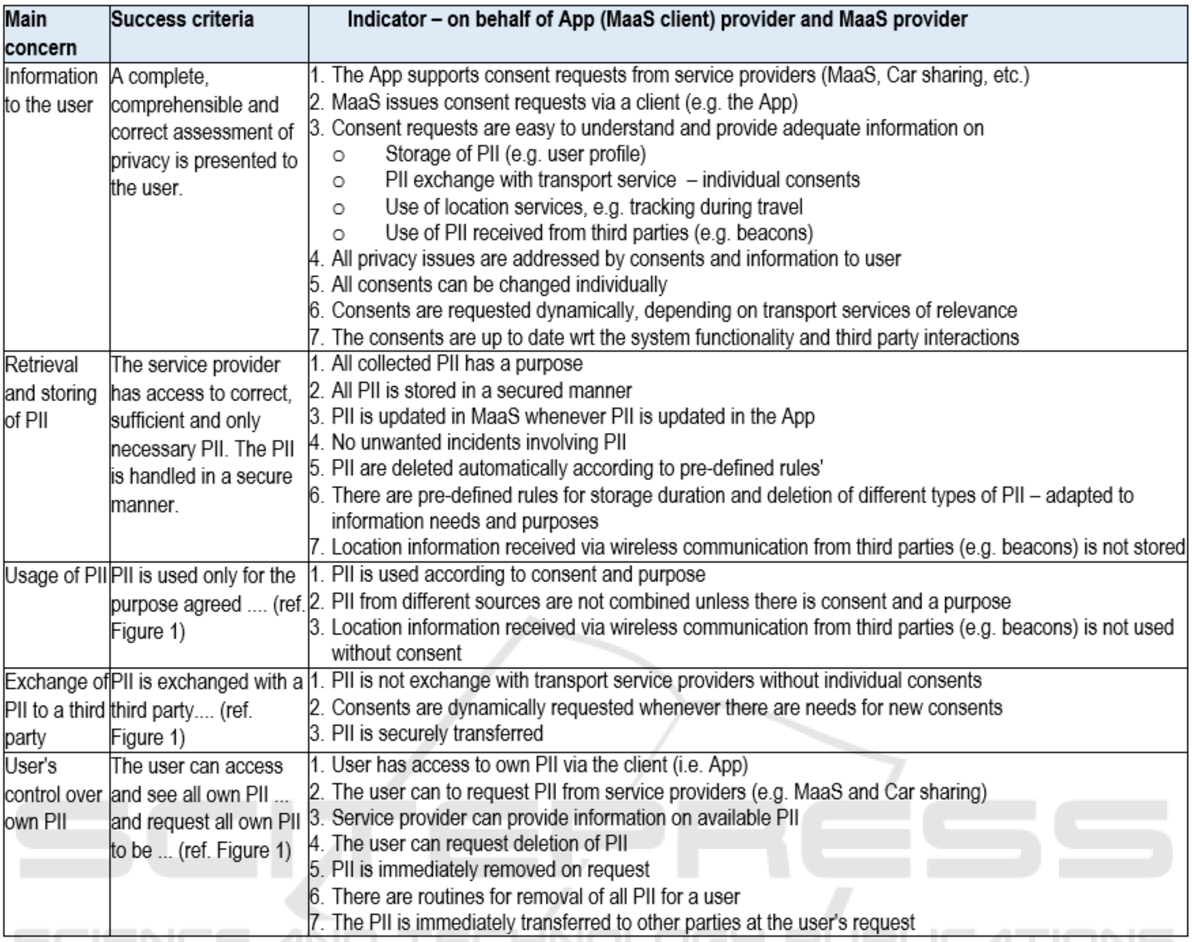
2. **Identify the Privacy Regulations, Requirements, Strategies and Goals of the Commissioner with Respect to the System/Service of the Analysis.** Sources: expert opinions, requirements specification, strategies/goals of the service provider, laws and regulations, and agreements with the users.
3. **Identify Main Privacy Concerns.** Limit the number of concerns between four and ten.
4. **Explain Meaning of Each Concern Through Success Criteria in Column Two.**
5. **Identify and Specify Indicators Relevant to Each Concern.** Use a separate form to specify meaning and properties of each indicator, a measurement scale for the indicator, and its target score. State the approach to expressing uncertainty, how to obtain an estimate, what measurement sources are, and how often to update the indicator value.
6. **Specify the Target Score of Each Indicator.**
7. **Identify and Specify the Initiatives.** Identify and describe on-going and planned measures expected to contribute to the improvement of indicator scores and fulfilment of the expressed concerns. A separate template should include detailed specification of the initiatives, including the plans for realization, dependencies with other initiatives, expected results, assumptions, cost, and roles involved.
8. **Specify Revision Plans.** Specify guidelines, responsibilities and triggers for revision and updates of contents of the scorecard. Particularly, changed privacy requirements, laws, regulations, system architecture, usage, kinds and numbers of users, requirements strategies, goals and prior assumptions, may trigged needs for revision of the scorecard in terms of new or updated contents.

3 APPLYING PRIVACY SCORECARD ON AN EXAMPLE SERVICE

In this section, we present the results obtained from applying the Privacy Scorecard approach on a concrete example from the ITS domain. First, we explain the service under analysis and setup of the trial. Second, we present the steps undergone and the results obtained. Finally, we summarize the lessons learned from applying the approach.

3.1 The Service under Analysis

A journey may be composed of many legs offered by different transport service providers. In the emerging Mobility as a Service (MaaS) concept, major transportation needs of a traveller are met over one interface offered by a MaaS service provider (Hietanen, 2014). MaaS may support the use of public transport alone or door-to-door transport facilitated by combinations of transport services (public transport, city bikes, taxis, car sharing, etc). Figure 2 illustrates a possible realisation of MaaS.



Main concern	Success criteria	Indicator – on behalf of App (MaaS client) provider and MaaS provider
Information to the user	A complete, comprehensible and correct assessment of privacy is presented to the user.	1. The App supports consent requests from service providers (MaaS, Car sharing, etc.) 2. MaaS issues consent requests via a client (e.g. the App) 3. Consent requests are easy to understand and provide adequate information on ○ Storage of PII (e.g. user profile) ○ PII exchange with transport service – individual consents ○ Use of location services, e.g. tracking during travel ○ Use of PII received from third parties (e.g. beacons) 4. All privacy issues are addressed by consents and information to user 5. All consents can be changed individually 6. Consents are requested dynamically, depending on transport services of relevance 7. The consents are up to date wrt the system functionality and third party interactions
Retrieval and storing of PII	The service provider has access to correct, sufficient and only necessary PII. The PII is handled in a secure manner.	1. All collected PII has a purpose 2. All PII is stored in a secured manner 3. PII is updated in MaaS whenever PII is updated in the App 4. No unwanted incidents involving PII 5. PII are deleted automatically according to pre-defined rules' 6. There are pre-defined rules for storage duration and deletion of different types of PII – adapted to information needs and purposes 7. Location information received via wireless communication from third parties (e.g. beacons) is not stored
Usage of PII	PII is used only for the purpose agreed .... (ref. Figure 1)	1. PII is used according to consent and purpose 2. PII from different sources are not combined unless there is consent and a purpose 3. Location information received via wireless communication from third parties (e.g. beacons) is not used without consent
Exchange of PII to a third party	PII is exchanged with a third party.... (ref. Figure 1)	1. PII is not exchange with transport service providers without individual consents 2. Consents are dynamically requested whenever there are needs for new consents 3. PII is securely transferred
User's control over own PII	The user can access and see all own PII ... and request all own PII to be ... (ref. Figure 1)	1. User has access to own PII via the client (i.e. App) 2. The user can to request PII from service providers (e.g. MaaS and Car sharing) 3. Service provider can provide information on available PII 4. The user can request deletion of PII 5. PII is immediately removed on request 6. There are routines for removal of all PII for a user 7. The PII is immediately transferred to other parties at the user's request

Figure 3: Privacy Scorecard applied on the Mobility as a Service (MaaS) example.

This example is constructed based on knowledge and experience of the two domain experts on ITS, who conducted this trial of Privacy Scorecard on Maas. MaaS may be accessed via several Apps. The Travel Companion App is one of them. Transport needs and preferences of the user are received via the App, and MaaS composes transport alternatives, processes bookings, issues tickets, etc. During the transport phase, MaaS provides situational support adapted to the location information received from the App.

MaaS communicates with various transport service providers and PII may also be exchanged to facilitate the required functionality. The traveller interacts directly with the App and PII is communicated from the App to MaaS and further on to the respective transport service providers. Should there be a new transport service offered, the Maas would know about it, and if this new service provider needs PII, Maas must interact with the App to ask for consents. The new choice for transport service can be booked, provided the user has agreed on exchange of PII. The process requires that the App and the MaaS as well as the transport service providers have common service platforms supporting the required consent interactions.

The PII of relevance in the MaaS case may be information about the traveller (user profile with contact information, preferences, etc.), location information (current location, tracking information and foreseen locations), payment information, information regarding use of transport services, etc.

PII may be used for purposes that the traveller is not aware of. The App, MaaS and other services may for example store, analyse and combine PII to be able to learn about the traveller and provide customized user support. PII may also come from different sources. An App on a smart phone using Bluetooth may for example detect signals from beacons in the vicinity using open interfaces, and the App may track the traveller regardless of whether the App has access to location information or not.

The AltBeacon (AltBeacon, 2016) specification does for example define such an open message format for beacons. An example of beacon application is Place Tips (Place Tips, 2016), an app shown to people in a given vicinity and who have given Facebook permission to access their location from their smart phone. Content is shown to people coming in the same vicinity.

3.2 Privacy Scorecard Applied on MaaS

Figure 3 summarizes results of applying the generic Privacy Scorecard (Figure 1) on our MaaS example service. Two domain experts discussed the MaaS system architecture and the functionalities of the system components, and filled in the scorecard in about one working day. The indicators from Figure 1 were used as inspiration for discussions targeting each main concern. The resulting scorecard is yet preliminary and must be refined as the solution is further elaborated.

Consents are crucial for the *information to the user* concern. MaaS has however, no user interface, and there must be a secure service interface between MaaS and its clients (i.e. the Apps) for interactions with the user on consents. MaaS may also have to request consents on behalf of the transport service providers via this interface. The Car Sharing services provider may for example need a consent before PII is shared with the Parking provider to arrange for a discount on parking provided exclusively to those who share their car.

The *retrieval and storing of PII* and the *usage of PII* concerns must address and consider the purpose of each individual PII. Location or tracking information collected by the App is, for example, meant to facilitate situational user support and should not be stored for a long time or used for other purposes. Signals from beacons should not be decoded to find locations unless a consent is agreed upon.

Consents are also required for *exchange of PII to a third party*, as exemplified for both the MaaS and the Car Sharing service above.

The *user's control over own PII* must be effectuated via the App. On request, MaaS must provide information on all PII associated with a user, and the user must be allowed to request deletions of such information. If a user decides to switch to another MaaS provider, PII must be transferred to the new provider.

3.3 Lessons Learned

Here we summarize the lessons learned from applying the Privacy Scorecard on the MaaS service.

While the main concerns, success criteria and indicators provided in Figure 3 were useful for the structuring of discussions, it was more challenging to complete the rest of the table. The scores and initiatives columns are difficult to assess while analysing the system at a relatively high level.

We learned that an understanding of the system architecture is crucial. The roles of system components, the flows of PII and the use of PII in the respective functions must be understood.

Therefore, indicators must be reviewed and updated as the work on the system architecture progresses, probably as an iterative process. In addition to the importance of the system architecture, we also had to understand the threats represented by external factors, e.g. beacons.

Following an iterative process, we should be able to detail the system analysis to a sufficient level in order to be able to assess relevant scores for the indicators and suggest initiatives. Scores must also be adapted to the individual indicators. Preferably, MaaS and the App should be analysed separately in two separate scorecards. The rationale for this is that they may have different providers and challenges.

At last, the indicators from the generic template, which we originally (in Figure 1) considered as relevant candidates, have to a large extent been confirmed while applying the Privacy Scorecard on MaaS. However, the indicators have also been adapted to the case, and they may be complemented when further system analysis is conducted. Accordingly, the solutions on how to improve the parameters "initiatives" will also need to be developed.

All in all, we have through the analysis gained an improved insight of the service under analysis, as well as a thorough understanding of the privacy concerns.

4 DISCUSSION

During development of the generic Privacy Scorecard canvas (Figure 1), we observed that some of the indicators semantically overlapped with each other. This may be misleading when providing an overall assessment and visualizing the scores in one common view. It should be dealt with through more detailed guidance for indicator specification and better visualization of the scorecard in a manner that takes into account dependencies.

Another need observed during development of the generic scorecard, is support for expressing uncertainty of the indicator estimates. Either the indicators are based on domain expert knowledge or measurements, some degree of uncertainty (due to lack of knowledge or variability) will be inherent. The explicit uncertainty information should be included in the scorecard, in order to provide more reliable decision support and possibly prioritize further verification of some indicator estimates.

The guidance for application of the scorecard provided in Section 2 is intended to be agnostic of the development approach (e.g. waterfall, agile, etc.). Particularly, the last step (revision) should facilitate updates upon changes. Part of future work should, however, be customization of the guideline to the specific development approaches.

Application of the approach on an example during the time limit of one working day, of course has clear limitations in terms of realism and actual exposure of the approach. Although the Privacy Scorecard canvas was not fully instantiated on MaaS, the initial results of the trial indicate feasibility of applying the approach within limited time. The fact that new knowledge was gained about the system under analysis and its privacy characteristics, suggests usefulness of the approach.

We assume that a more detailed guidance and a domain-customized Privacy Scorecard canvas, would facilitate application of the approach. In that case, the trial would likely be more efficient and require less resources.

We need to further empirically evaluate not only feasibility but also performance of the Privacy Scorecard approach in more realistic settings. There is also a need for a baseline for comparing this approach with the alternative PIA methods, in order to assess characteristics such as usability, usefulness and cost-effectiveness of our approach compared to the alternative ones. It should be a part of the future work.

Privacy Scorecard is developed by domain experts, although it is, once developed, meant to be used as decision support for privacy evaluation and handling by non-privacy-experts as well. Further refinement of the design of the Privacy Scorecard canvas needs to provide a detailed account of the design rationale and ensure that it fully meets the needs of both the experts developing it, and the non-privacy-experts using it.

Correctness and relevance of the results (i.e., contents of the scorecard) would have been desirable to assess through more empirical evaluation. This was unfortunately impossible within the frame of this study. Instead, we have relied on the analysis group with relevant domain knowledge and diversity.

We cannot exclude possibility of inconsistent understanding of the Privacy Scorecard approach or the MaaS example, although the active participation of the analysis group in all steps undertaken should have reduced the likelihood of that risk. At the same time, it is, in terms of evaluation of comprehensibility, a weakness that the domain experts who tried out the approach also participated in design of the generic canvas. As such, it is also a threat to reliability of the evaluation results, as we cannot know to what degree another analysis group would have obtained the same results.

Privacy Scorecard should be scalable with respect to the range of concerns (reflecting different privacy requirements) that need to be covered by the scorecard. The approach should also scale with respect to the complexity and size of the service under analysis. Further empirical evaluation is needed for assessing these two aspects of scalability.

Overall, we have drawn important findings and learned lessons from developing and instantiating the approach in the MaaS example. Although the mentioned threats to validity and reliability are present in the study, we argue that the initial results partially indicate feasibility and suggest preliminary strengths and weaknesses of the approach. Hence, further development of the approach would make sense, focusing on refinement of the scorecard canvas, more detailed guidance for use, as well as further empirical evaluation.

5 CONCLUSIONS AND FUTURE WORK

Digital services are increasingly becoming dependent on personally identifiable information. Such services are a part of a complex and dynamic ecosystem characterized by frequent changes and many dependencies. Privacy is a condition for trust of users and adoption of the services. At the same time, a service provider has to deal with many legal and technical privacy requirements. Assessment of privacy and compliance with requirements is demanding, and state of the art lacks decision support which is comprehensible and transparent.

This position paper proposes initial version of a so-called "Privacy Scorecard", that is, a decision support for a service provider aimed to facilitate management of privacy goals. We have presented the initial design and intended usage of the approach. We have also partially tried out the approach and shown how it can be applied to a constructed example. The example was motivated by a real-life scenario of so-called Mobility-as-a Service, and designed by two domain experts. The initial findings indicate feasibility of instantiating the approach, therein identifying and specifying privacy-relevant concerns of the service. The approach has also facilitated gaining new knowledge about (privacy enhancing) design of the service under analysis.

We have also gained useful insight into the strengths and weaknesses of the approach as well as suggested directions for future research. The directions include refinement of the scorecard design and usage guidelines, tool support for visualization, as well as further empirical evaluation. Particularly, the following needs have been highlighted:

- more detailed support for design and estimation of privacy indicators,
- more detailed support for follow-up of the initiatives (progress, cost, responsibilities),
- support for expressing dependencies between the initiatives,
- support for cost-benefit analysis (cost being the expenditure implementing the initiatives, and benefit being improvement of privacy concerns) for selection of the initiatives,
- tool support for real-time follow up of the scores and visualization of the trends,
- empirical evaluation of usefulness and performance of the approach,
- more detailed usage guideline including customization of the guideline to the specific development approaches, and
- specializations of the Privacy Scorecard canvas with respect to different industry sectors and domains.

ACKNOWLEDGEMENTS

This work has been conducted as part of the PrivacyAssessment@SmartCity project funded by SINTEF.

REFERENCES

Altbeacon. http://altbeacon.org/ Last accessed: Nov. 2, 2016.

European Parliament, Council of the European Union. Regulation (EU) 2016/679 - *Protection of natural persons with regard to the processing of personal data and on the free movement of such data*, 2016.

Erdogan, G., Omerovic, A., Natvig, M. K., Tardy, I.C.R., 2016. Technical report A27830. *Needs and challenges concerning privacy risk management within Intelligent Transport Systems - Problem analysis in project PrivacyAssessment@SmartCity*. SINTEF.

Frigal, J., Guiochet, J., Killijian, M.-O. *Towards a Privacy Risk Assessment Methodology for Location-Based Systems*. In Proc. 10th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pages 748-753. Springer, 2014.

Hietanen, S.. *Mobility as a Service - the new transport model*? Eurotransport Magazine, 12(2):2-4, 2014.

ISO/IEC 27005:2011(E), International Organization for Standardization. Information technology - Security techniques - Information security risk management, 2011.

ISO/IEC 29100:2011(E), International Organization for Standardization. *Information technology - Security techniques - Privacy framework*, 2011.

ISO 22307:2008(E), International Organization for Standardization. Financial services - Privacy impact assessment, 2008.

Kaplan, R.S., Norton, D.P. *Putting the balanced scorecard to work*. Performance measurement, management, and appraisal sourcebook, 66, p.17511. 1995.

Knirsch, F., Engel, D., Neureiter, C., Frincu, M. Prasanna, V. *Model-driven Privacy Assessment in the Smart Grid*. In Proc. 1st International Conference on Information Systems Security and Privacy, pages 173-181. SCITEPRESS, 2015.

Mylonas, A., Theoharidou, M., Gritzalis, D. *Assessing Privacy Risks in Android: A User-Centric Approach*. In Proc. 1st International Workshop on Risk Assessment and Risk-driven Testing (RISK'13), pages 21-37. Springer, 2014.

NIST SP 800-30,National Institute of Standards and Technology. Guide for Conducting Risk Assessment, 2012.

Psaraki, V., Pagoni, I. Schafer, A. *Techno-economic assessment of the potential of intelligent transport systems to reduce CO2 emissions*. IET Intelligent Transport Systems, 6(4):355-363, 2012.

Place Tips, https://www.facebook.com/business/news/place-tips-for-businesses Last accessed: Nov. 2, 2016.

Ren, D., Du, S., Zhu, H. *A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs*. In Proc. IEEE International Conference on Communications (ICC'11), pages 1-5. IEEE Computer Society, 2011.

Tancock, D. Pearson, S. Charlesworth, A. *A Privacy Impact Assessment Tool for Cloud Computing*, pages 73-123. Springer, 2013.

Theoharidou, M., Papanikolaou, N., Pearson, S. Gritzalis, D. *Privacy Risk, Security, Accountability in the Cloud*. In Proc. 5th International Conference on Cloud

Computing Technology and Science, pages 177-184. IEEE Computer Society, 2013.

Vandezande, N., Janssen, K. *The ITS Directive: More than a timeframe with privacy concerns and a means for access to public data for digital road maps?* Computer Law & Security Review, 28(4):416-428, 2012.