# ProTACD: A Generic Privacy Process for Vehicle Development

Naim Asaj*, Florian Schaub†, Michael Müter*, Albert Held*, Michael Weber†
*Daimler AG, Research, Dep. Infotainment & Telematics, Ulm / Böblingen, Germany
Email: { naim.asaj | michael.mueter | albert.held }@daimler.com
†Institute of Media Informatics, Ulm University, Ulm, Germany
Email: { florian.schaub | michael.weber }@uni-ulm.de

***Abstract*—The growth in information technology and connectivity has enabled a significant range of new functionalities in modern automobiles, such as telematics wireless interfaces via Wi-Fi. At the same time, the protection of privacy is becoming a major concern and questions are being raised regarding the need for current privacy concepts to be extended or even replaced by integrative and structured privacy approaches. This might be necessary to uncover isolated and unexpected privacy threats, e.g., tracking of multiple in-car wireless sensors. We identify the key challenges for privacy enforcement in the vehicle's lifecycle and propose a generic, yet integrative, privacy process for vehicle development (ProTACD). The final decision to enforce and deploy privacy features in vehicular development requires several prerequisites to be provided by ProTACD. In this paper, we outline the phases and interactions of ProTACD, and discuss its general objectives and differences from other approaches.**

## I. Introduction

Current in-vehicle networks consist of up to 90 electronic control units (ECUs) to fulfill certain automotive requirements. Moreover, vehicles are being extended with wireless communication systems such as GSM, UMTS, LTE, Wi-Fi, and Bluetooth. In the future, these interfaces will serve as enabling technologies for enhanced telematics platforms and automotive apps, e.g., location-based services and social networks.

Held and Kroh [1] predict that the percentage of vehicles with enhanced telematics platforms, applications, and other consumer devices, such as mobile and smartphones, will increase in the future. In addition to the benefits of such integrated connectivity and functionality, an increased need for security arises, especially in the context of maintaining privacy. Such connectivity will open new avenues in which a vehicle's privacy can be threatened by someone tapping into vehicle data, such as vehicle location and speed, the driver's personal information, or the vehicle's device identifiers [2]. The protection of automotive systems in terms of vehicle-related security has been a well-established research area for many years. Several security concepts in the automotive field have been investigated by researchers [3] and original equipment manufacturers (OEMs) [4]. However, security alone is no "universal remedy" for all privacy issues, and thus, vehicle-related privacy aspects have become a key factor in automobiles, and are just starting to be recognized as important deployment issues [5, 6].

In this regard, the realization of privacy in automobiles has often been considered to be a singular task, despite the recognized need for holistic IT security concepts in the automotive domain [7]. Therefore, we propose ProTACD *(PROcesses and Technologies for Automotive privaCy Development)* as a generic but structured and integrative privacy process that helps to provide sustainable privacy protection and increased privacy awareness for OEMs and drivers alike. At the same time, ProTACD considers the specific requirements posed by the automotive domain, such as legal aspects, safety (e.g., driver distraction), and multidisciplinary domains.[1]

ProTACD embraces the privacy-by-design (PbD) [8] paradigm, where privacy intentions are embedded into architectures and processes already in early design phases. For this reason, automotive privacy approaches must become proactive in the design phase rather than reactive efforts. Main emphasis should be the support and deployment of privacy in the automotive domain. However, due to the involved multidisciplinary domains and their privacy implications, automotive characteristics must be included in the process of deploying privacy features. For example, a privacy assessment comparable to those in the security domain must be employed to determine the criticality and priority of potential privacy implications.

The proposed ProTACD process comprises different automotive aspects, highlights open challenges, and guides the deployment of privacy. The main phases included in ProTACD are data acquisition, data modeling, privacy assessment, privacy design patterns, and privacy feature deployment. In the following, each phase of ProTACD will be described in detail and the main functions of each phase will be placed into the context of the overall approach.

In Section II, we first give an overview of related work in the field of vehicle privacy approaches. Subsequently, an overview of automotive-specific privacy design requirements is provided in Section III, followed by a detailed description of ProTACD in Section IV. In Section V, we evaluate the main objectives of ProTACD, and discuss the benefits as well as limitations of ProTACD in contrast to existing approaches. In Section VI, we conclude the paper and present an outlook of our future work.

[1]Multidisciplinary domains include different responsibilities, functions, requirements, and conditions.

3rd IEEE International Symposium on Security and Privacy in Internet of Things (SPIoT '13), Melbourne, Australia, July 2013.
Author version. Definitive version at ieeexplore.ieee.org

## II. Related Work

The development of emerging technologies, such as car-to-x communication (C2X), together with challenges faced in the area of intelligent transportation systems (ITS) have prompted significant research in security, trust, and privacy aspects [9, 10]. While this pioneering work has mainly focused on special conditions in the C2X field, other studies have focused particularly on automotive telematics privacy.

Duri et al. [11] proposed a generic data protection platform architecture for all entities participating in the telematics service chain, i.e., the vehicle, the telematics service provider, and applications service provider. Essential privacy functions provided by the platform include data aggregation close to the source and user privacy policies. Similar work has also been conducted in [12, 13], where the need for data management in automotive systems and a multi-application platform is stated, and consequently, various security and privacy aspects have been discussed.

There has also been research on location privacy in automotive telematics [14, 15], where special emphasis has been placed on mobile communication, positioning, and computing technologies in automobiles, focusing on the convergence of wireless communications. Furthermore, Kung et al. [16] embrace the concept of PbD for ITS applications, where different challenges for ITS deployment are discussed. In [17], the authors address the PbD approach with a formal privacy verification using ontologies in information systems. Additionaly, dealing with privacy issues have also been suggested towards incorporating privacy into system design processes, especially in the field of software engineering [18, 19].

There exist also several international security standards, such as Common Criteria (ISO/IEC 15408 [20]) or the information security management system (ISO/IEC 27001 [21]) that guide evaluation and establishment of security into company products and management levels as well as a range of risk analysis methods, such as ISO/IEC 27005 [22].

In addition to security procedures, privacy impact assessment (PIA) approaches emerged. PIAs primarily aim to identify privacy implications and controls by systematically evaluating the underlying system against possible effects that are associated with privacy threats. For example, the ICO PIA handbook [23] has been designed as a comprehensive guide for organizations that deal with personal data. In this regard, the German Federal Office for Information Security (BSI) also introduced a PIA framework specifically designed for RFID applications [24].

Unfortunately, while currently employed privacy approaches aim to fulfill certain aspects of privacy for the automotive domain (e.g., pseudonymization for a particular identifier [25, 26]), none of them consider a multidisciplinary viewpoint on the overall lifecycle of the vehicle, the interaction and dependency of vehicular data, and the multitude of sub-components and systems. Furthermore, some existing security processes do not entirely cover all the privacy concerns of the automotive domain, because (1) they are especially designed for security threats in standard IT systems, and (2) they do not consider specific automotive constraints (e.g., predominant embedded devices, in-vehicle networks, and vehicular architectures). Even if many of the security standards consider basic privacy aspects, none of them consider the privacy requirements from the privacy and stakeholder perspective.

Consequently, novel PIA processes have been designed and introduced to extend the existing security procedures. A PIA can be seen as "a process, which helps assess privacy risks to individuals in the collection, use and disclosure of information" [23]. It is noteworthy that PIAs are not intended to replace privacy or data protection audits, because audits are undertaken on projects already running, whereas PIAs are applicable from the early system design phase onward. However, Oetzel and Spiekermann [27] stated that, "existing PIA approaches lack easy applicability because they are either insufficiently structured or imprecise and lengthy," and then suggested a specific PIA for RFID applications that has been ratified by the BSI. Surprisingly, Wright [28] concluded that even mandatory PIAs will not be sufficient enough, and that reliable privacy protection should be a combination of tools, strategies, policies, architectures, PETs, and PIAs.

## III. Automotive-Specific Privacy Design Requirements

In addition to various security aspects, privacy is an important requirement when dealing with sensitive data in the automotive domain, e.g., sensor-derived and personal driver data. By considering different privacy aspects as well as the specific characteristics of automobiles, new challenges arise that posit several design requirements that must be considered when designing privacy concepts for automobiles.

*1) Privacy awareness:* The use of sensitive and personal information is constantly increasing in the automotive domain [5]. We see examples of this in autonomous systems, such as advanced driver assistance systems [2], or in new automotive applications, such as pay-as-you-drive car insurance [29] and automotive social networking [6]. In addition, privacy violations may be facilitated by the increased complexity of modern vehicles. Therefore, privacy awareness plays a key role in the automotive domain, and should be addressed to provide optimum levels of privacy protection. By privacy awareness we refer to the awareness of OEMs (including engineers) and drivers about potential and actual privacy implications in the vehicle. This requires identifying privacy implications and highlighting them in order to create (or increase) awareness about privacy issues.[2]

*2) Holistic privacy view:* The privacy perspective should cover as wide a scope as possible to gain the highest impact when introducing privacy concepts. Although singular privacy measures can have a significant benefit, a holistic viewpoint on the underlying landscape promises to improve privacy. In this regard, the efficiency of most privacy measures decreases or becomes even non-existent by increasing the scope being

[2]analogous to IT security awareness, where security threats are shown to create security awareness.

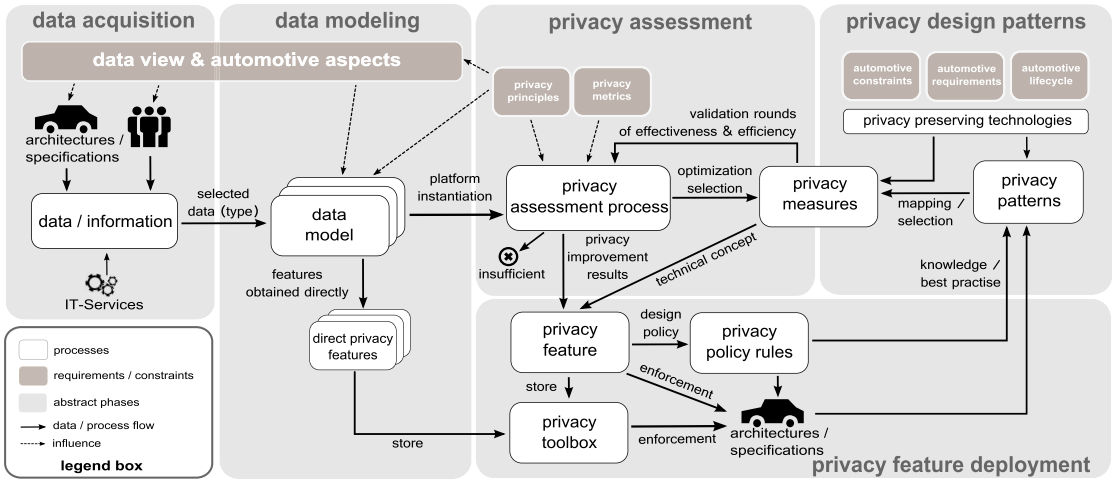


Fig. 1. Generic overview of ProTACD's phases, technologies, and components [icons: picol.org].

considered, i.e., considering the vehicle as a whole rather than individual sub-systems. Yet, a broader view of the vehicle can lead to the discovery of novel privacy threats, e.g., the recently discovered privacy implications of wireless tire pressure monitoring systems [2]. This also includes the extension of the data viewpoint by considering not only specific vehicular data, such as location information, but also a large set of specific data types (e.g., data on application level), or at best, all data that are available in the vehicle (e.g., diagnostic data, sensor data, OEM-specific data, etc.).

*3) Proactive privacy:* A general challenge is to shift privacy measures to proactive rather than reactive concepts [16, 17]. In this way, privacy threats may be neutralized or avoided before they have the opportunity to occur. In particular, drivers can disengage from specific privacy threats without the need for user interaction, e.g., to promote minimal driver distraction in automobiles. This means embedding privacy with *low driver distraction* in a vehicle's architectures and processes from an early design phase on, e.g., on the operating system level [6].

*4) Vehicle development constraints:* The development of an automobile comprises many complex processes, requirements, and constraints that may have a significant influence on the impact of privacy concepts. Typical constraints in the development of vehicle components (e.g., telematics head units and in-vehicle networks) are multidisciplinary influences, e.g., cost minimization, legal aspects, safety, and specific supplier conditions. Thus, any attempt to introduce privacy concepts for vehicles must consider these aspects as well as the technical characteristics of the vehicle architecture, which may be critical in the design of privacy improvements.

*5) Vehicle lifecycle:* Owing to the nature of automobiles, three distinguishable phases are common in the automotive domain. Each phase has its own specific characteristics that introduce unique constraints to the automotive privacy process. The first phase in the vehicle lifecycle is the *development phase*, where a range of conceptual and architectural work is conducted, and component specifications are defined. In terms of proactive privacy, this phase is very important because significant privacy measures can be analyzed and introduced in this phase. The second phase is the *production period* of an automobile, after which privacy measures should be available, e.g., when installing additional (third party) applications into the vehicle's telematics system that may alter the current privacy-optimized system. The third phase exists when *production is completed* and the maintenance of vehicle spare parts is required. However, during this phase, new privacy threats are still possible and remain crucial, e.g., accessing sensitive ECU logs by diagnostics software [30].

## IV. Structured and Integrative Privacy Process

ProTACD has been designed as a generic privacy process in order to be integrative, as otherwise the privacy process would need to be defined for every new vehicle model. Therefore, the main aim is to provide an integrative privacy process that can be adapted to the specific requirements of an OEM. In the design of ProTACD, we considered the design requirements mentioned in the previous section (see Sec. III). Currently, ProTACD focuses primarily on the vehicle development phase, and provides a trade-off between development constraints and privacy by integrating such constraints into the process. The other phases of the vehicle lifecycle require further specific requirements that cannot be achieved with the current privacy process. The goal at this stage is to support privacy during the design phase of the vehicle and its system components, following the concept of PbD and privacy by default [8].

Therefore, ProTACD supports the identification of privacy-critical aspects by employing an appropriate privacy assessment approach, and accordingly supports the selection of specific privacy measures, e.g., privacy-enhancing technologies (PETs), such as anonymization and data aggregation mechanisms. Moreover, the measures are based on a per-case basis, i.e., the privacy process considers specific aspects such as risk estimation and multidisciplinarity as part of a privacy threat, and thus decides the privacy measures that are best suited to a particular case.

TABLE I
TYPICAL DATA SOURCES DURING THE DEVELOPMENT OF AN AUTOMOBILE.

| No. | data source | description |
|---|---|---|
| S-1 | functional specification | requirements, feature lists, conceptual specifications, user interfaces, app descriptions, etc. |
| S-2 | architectural specification | system architectures, in-vehicle network architectures, backend architectures, telematics arch., etc. |
| S-3 | component specification | third party modules, e.g., chipsets, Wi-Fi adapter, Bluetooth, NFC, GSM, etc. |
| S-4 | communication matrix | compliance of message/data com. between entities (e.g., CAN-Matrix for the in-vehicle network) |
| S-5 | connected consumer devices | smartphones, tablet PCs, personalized remote keys, etc. |

To gain the most benefits of ProTACD, it must be handled and maintained in a centralized way by an appropriate corporate division such as the data protection department of an OEM. The main phases of ProTACD are data acquisition, data modeling, privacy assessment, privacy design patterns, and privacy feature deployment. In the following, we discuss the different phases in detail along with the overall ProTACD procedure and its interactions. An overview of ProTACD is depicted in Fig. 1.

### A. Data acquisition ($P_D$)

Owing to the increasing amount of vehicular data, complex situations emerge during data collection and handling. Thus, the data acquisition phase is a fundamental step, where the appropriate selection of data can be obtained. Instead of focusing on singular data (e.g., location information), we propose a holistic acquisition phase that considers vehicular data across different vehicle domains or various categories, e.g., by collecting and analyzing different specification documents, and retrieving the appropriate data from that (similar to the data collection in common PIAs [23, 24]). However, this also depends on the OEM strategy followed, and on the specific data that needs to be collected from the documents.

In the design phase of a vehicle, the data acquisition phase comprises specific information sources (see Table I). The main sources are the functional and architectural specifications of the vehicle, the specific component descriptions, and the intended IT-Services, e.g., standard automotive apps. Information about personal preferences are limited at this stage, and are therefore considered to provide the highest privacy protection by default, i.e., following different privacy principles [31] such as data minimization. Data minimization would reduce the privacy impact of sensitive data (e.g., location information) by applying different techniques to that data (e.g., location obfuscation [32]).

Data in the data acquisition phase can have different influences. In ProTACD, data is based on the data view and specific automotive aspects, e.g., the scope of data, development, and legal constraints. Therefore, the selection (or consideration) of specific data for the privacy process depends on the underlying view and intention. As identified in Section III, a holistic privacy view in the data acquisition phase promises to provide the highest impact for privacy protection.

Such a holistic view can have different variations, including the consideration of data across specific abstraction levels (e.g., on application layers) or the consideration of particular sub-systems in a vertical view (e.g., the communication stack across each layer). In general, the variations of a holistic view are not limited, provided that the broader scope helps to improve privacy. For this purpose, we are currently working with a type-oriented variation that takes into account particular types of data. There exist various types of data that can be considered for the data acquisition phase. Here, we describe the main types of vehicular data, where each type has its own unique characteristics in the automotive domain.

- **vehicle identifying data:** data with the potential to uniquely identify a vehicle within a certain context, e.g., vehicle identification number (VIN), serial numbers of ECUs, and vehicle certificates.
- **driver/passenger identifying data:** data with the potential to uniquely identify a person (driver or passengers of a vehicle) within a certain context, e.g., full name, personal number, credentials, and CE-device information.
- **sensor-derived data:** data that is quantified from a vehicle's sensor and that has been derived (or calculated) from different combinations of sensors, e.g., temperature, speed, and location.
- **domain-specific data:** data that belongs to a specific vehicle domain, e.g., infotainment-domain, telematics-domain, chassis-domain, and powertrain-domain.
- **attribute-based data:** data that fulfills specific conditions based on selected attributes, e.g., size, source, and usage.

### B. Data modeling ($P_M$)

Data can be complex and unstructured when considering a wide variety of vehicular and personal information from a holistic viewpoint. To cope with this issue, particular data models can be integrated into the ProTACD process in the data modeling phase that reflect and structure the underlying data of the data acquisition phase. Examples of such data models include a physical scheme of the source or destination of vehicular sensor data, e.g., which ECU produces which sensor data and which enitity uses it. The term data model is kept intentionally abstract in ProTACD to allow introduction of different models in the realization of ProTACD. However, we argue that the concept of a data model must be based on specific types of data and specific automotive constraints, e.g., the basic automotive architectural structure. The core of a data model indicates the feasibility with which it can analyze different data in a combined way in order to maximize the impact of further results, i.e., specific privacy features. The data modeling phase also considers privacy principles that are based on the focus of identity and data protection.

The additional function of the data model is to provide

a platform where privacy assessment approaches regarding common privacy aspects can be investigated, determined, and applied. For this purpose, we are currently developing a data model in the form of a *vehicle identity graph* [33], which handles the set of identifiable data in the vehicle. In ProTACD, the vehicle identity graph can serve as one possible data model, in order to improve the unlinkability of a set of identifiers by considering and analyzing their privacy impact in a combined way. Furthermore, the designed data models should not only be practical in the sense that they act as a platform for privacy assessment approaches, but also be usable for further privacy aspects regarding privacy features, including in-car identity management platforms that can be directly stored in ProTACD's privacy toolbox (see Fig. 1).

### C. Privacy assessment ($P_A$)

The objective of this phase is to identify and highlight critical privacy aspects and to evaluate the effectiveness and efficiency of privacy measures. One example is the criticality of certain vehicular data that are available, generated, or stored in the vehicle, e.g., device identifiers, vehicle location and speed, and the vehicle identification number. The privacy assessment in the development phase of an automobile is driven by the desire to minimize risks and maximize protection by employing proactive (rather than reactive) measures.

The main components in this phase are the underlying data models, privacy principles, and particularly specific privacy metrics. Thus, ProTACD pretends to provide a set of privacy metrics for different privacy aspects. For this purpose, privacy metrics are being investigated for the realization of ProTACD, including the provision of an information-theoretical approach that has proven promising in regard to measuring the impact of the information content of specific data such as identifiers. Currently, we are analyzing this approach on a real dataset of VINs (vehicle identification numbers), where the results will be published in a separate study.

The privacy assessment phase allows the examination of data to determine which combination of data or vehicle domains (depending on the data model) are affected by critical privacy threats (see Fig. 1). Based on this premise, it is possible to identify the most critical and most likely privacy violations and to select them for appropriate privacy measures, e.g., the anonymization of data. The validation step of the applied privacy measure ensures that the privacy impact has been discernibly reduced by repeating the privacy assessment on the same basis, and thereby enhancing the vehicle's overall privacy. In addition, with the validation step, we derive an efficiency confirmation in which the original privacy impact estimation and the analog privacy improvement are documented, e.g., an explanatory statement for the necessity and efficiency of the privacy feature owing to the reasonable balance between indirect features and cost minimization. In this way it is more likely to support and address special automotive constraints found particularly within the development phase of an automobile.

### D. Privacy design patterns ($P_P$)

To facilitate timely and optimized privacy measures, we argue that the approach of privacy patterns [34, 35] for the automotive domain provides numerous advantages during the development phase of an automobile. In general, a privacy measure is a course of actions to enhance and protect privacy. The main components of this phase are a set of privacy-preserving technologies (PETs); several automotive aspects such as constraints, requirements, and lifecycle characteristics; and particularly automotive privacy patterns (see Fig. 1).

In our context, a privacy pattern is a general reclaimable solution to a commonly occurring privacy issue. However, a privacy pattern is not a completed solution that can be assigned directly into a vehicle's architecture or specification without prior customization. It is more a reference or recommendation of controls, and how to face a privacy issue in an optimal way. Hence, the approach can serve as a broad solution that can be used for different privacy issues on different production lines.

It is clear that privacy measures must be complemented by employing technical protection approaches, e.g., location obfuscation [36]. To support and optimize these approaches using a set of common privacy-preserving technologies, ProTACD comprises the concept of automotive privacy design patterns, e.g., pseudonymization rules, access restrictions to sensitive data, or privacy-preserving identification and authentication techniques for in-vehicle wireless sensors.

In this way, it is possible to facilitate documented privacy patterns that are developed in conjunction with automotive aspects. This in turn permits the optimization of the applied privacy measures, while simultaneously reducing incorrect decisions regarding the selection and adaption of appropriate privacy technologies in the automotive domain. Instead of providing a set of fixed privacy patterns, our approach integrates feedback mechanisms where adaptations based on new findings can be performed (see Fig. 1). This guarantees a continuous evolution and improvement in the privacy patterns. For an initial set of privacy patterns, we first suggest building a framework for selecting appropriate privacy patterns, and then analyze existing privacy patterns and adapt them to automotive constraints. A similar approach has been proposed in [37].

### E. Privacy feature deployment ($P_{FD}$)

The privacy feature deployment phase comprises four different components: privacy features, privacy toolbox, privacy policy rules, and vehicle architecture (see Fig. 1). The main goal of our approach is to support the enforcement of privacy features during the vehicle development phase by identifying privacy-critical aspects and risk probabilities.

A privacy feature may consist of the technical realization concept (based on common privacy patterns) and a list of parameters that highlight the privacy assessment results and privacy advancements. Because the deployment of derived privacy features is not always directly feasible, due to different automotive constraints including major architectural modification or safety concerns, ProTACD contains a kind of privacy toolbox to store privacy features. Thus, documentation

is conducted by collecting each privacy feature in the privacy toolbox, where consequent usage could be enforced on upcoming production lines. Furthermore, we believe that specific privacy features can lead to new information regarding design policies for the vehicle's privacy that can be directly included in the design process of the vehicle and its components or can be further harnessed as an input for automotive privacy patterns (see Sec. IV-D). Typically, the enforcement of privacy features in the vehicle's architecture or specification enables the collection of additional knowledge (or best practices) that can be included in the automotive privacy process. Therefore, a general backflow of best practices and other findings to the privacy patterns guarantees an optimal degree of utilization.

### F. Interaction and dependencies of the phases

From the above descriptions and sequence, it follows that some phases of ProTACD exhibit strong interactions and dependencies. The abstract flow of the phases is illustrated in Fig. 2. In general, the process always starts with $P_D$ and lays the grounds for $P_M$. Depending on the data provided by $P_D$, the data model will be designed in $P_M$. Here, it is essential that not only the data but also automotive aspects and specific privacy principles (e.g., untraceability) are considered. The transition $T_{P_M \to P_A}$ is where the data model is instantiated to serve as a platform for privacy assessment. However, ProTACD is designed to contain several different data models that depend on the underlying data type (see Sec. IV-A). This means that multiple transitions $T^i_{P_M \to P_A}$ can exist in parallel, to speed up the privacy assessment for different data types.

From Fig. 2, we observe that $P_P$ operates independent of the remaining phases because it has no transition from other phases. This is because $P_P$ is aimed to be a framework (similar to [37]), where privacy patterns will be recommended based on input parameters, such as a privacy risk estimation (e.g., low risk, mid risk, and high risk) and context information (e.g., data type, attributes, and vehicle domain). Therefore, regular updates and extensions of the privacy design patterns are possible to include new PETs into phase $P_P$, and hence, to improve the overall efficiency of the privacy process.

Phase $P_A$ consolidates $P_M$ and $P_P$, where the major goal is to obtain and minimize estimated privacy implications. For each estimated privacy risk, the most appropriate solution from $P_P$ can be applied, e.g., a privacy design pattern such as pseudonymization. To prove the effectiveness and efficiency, several iterations in $P_A^{\circlearrowleft}$ can be performed. We argue that the efficiency allows us to indicate whether and how the current approach positively affects the estimated and overall privacy risk. An iteration in $P_A^{\circlearrowleft}$ leads to a new privacy assessment, therefore, the efficiency is defined as the difference between the original privacy risk $PR$ and the new risk $PR'$. Based on the iterations and the determined privacy risk reduction (efficiency), the process has several possibilities for triggering the next steps in $P_A$ that follow a set of rules and variables including a threshold value $t$, the determined efficiency $\omega$, the current number of iterations $i$, and the maximum iterations $i_{max}$. The basic rules can be defined as follows:

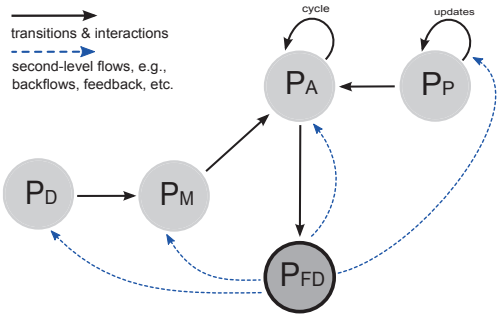


Fig. 2. Basic interactions (black-solid) and second-level flows (blue-dotted) of ProTACD's phases.

1) If $\omega < t$ and $i \leq i_{max}$, then $P_A^{\circlearrowleft}$ repeats for the same case, but with another (or stronger) privacy design pattern.
2) If $\omega < t$ and $i > i_{max}$, then $P_A^{\circlearrowleft}$ breaks for the selected case and selects another reasonable case to be reduced in their privacy impact.
3) If $\omega \geq t$ and $i \leq i_{max}$, then $P_A^{\circlearrowleft}$ stops successfully for the selected case. Then, the process either makes the transition $T_{P_A \to P_{FD}}$ or picks up another reasonable case.

The threshold $t$ and the maximum number of iterations $i_{max}$ can be defined by an appropriate corporate division such as the data protection department of an OEM. In general, the higher the threshold $t$, the better the design pattern has to fit, and thus, the more likely it is to find the best suited and most efficient improvement for a specific case. However, a high threshold $t$ also means that there is an increased likelihood of not finding any satisfying solution. Furthermore, a high value of $i_{max}$ causes time-consuming iterations in $P_A^{\circlearrowleft}$, while increasing the probability of finding an acceptable privacy feature for a particular case in $P_A$. Therefore, parameter selection must be guided by a risk-cost tradeoff.

Once the transition $T_{P_A \to P_{FD}}$ has been carried out, internal sub-processes in $P_{FD}$ can create new findings and results in order to update or even extend the privacy design patterns in the process. Thus, every time the transition $T_{P_A \to P_{FD}}$ is carried out, a backflow of feedback and information $SLF_{P_{FD} \to P_P}$ (second-level flow) is feasible. Moreover, from $P_D$, several additional second-level flows (blue-dotted lines in Fig. 2) are possible, e.g., $SLF_{P_{FD} \to P_A}$ resuming the privacy assessment and improving further reasonable cases (in case the transition $T_{P_A \to P_{FD}}$ occurred too early). In general, we define the transition $T_{P_A \to P_{FD}}$ as the ultimate objective in the privacy process, because each transition of $T_{P_A \to P_{FD}}$ implies that a privacy feature has been identified and documented, which in turn leads to an improvement in overall privacy.

## V. Evaluation

The enforcement of practical privacy features in the automotive domain is a relatively new task with the potential to produce unexpected influences. For example, distinct or unfamiliar interactions with interdisciplinary architectural components could lead to significant development implications and costs. This is also true in the case of issues that cannot be

influenced such as firm deadlines and management decisions. Therefore, ProTACD provides the recommendation, support, disclosure, and proof of the need for various privacy measures, but does not determine their ultimate enforcement and implementation. Moreover, ProTACD is designed to fit into the typical vehicle development process, where new vehicle models and components are developed on the basis of previous vehicle series in order to better utilize the degree of reusability. Therefore, ProTACD comprises phases and components that can be "reused" on upcoming production lines, e.g., design patterns $P_P$, whereas other phases of ProTACD might be re-initialized from scratch such as the data acquisition phase $P_D$. In addition, compared to other privacy approaches in the automotive domain (see Sec. II), where the focus is on providing purely technical solutions for a single privacy task (stand-alone solutions), our generic privacy process also addresses strong development constraints and considers different multidisciplinary privacy viewpoints. We believe that we can achieve as much privacy as possible in a vehicle by disclosing and showing unknown and unexpected privacy violations before they occur. In this way, the current process addresses most of the automotive-specific privacy requirements (see Table II). However, individual differences in the lifecycle of vehicles require additional extensions of the privacy process.

### A. Fulfillment of design requirements

The automotive-specific privacy design requirements described in Sec. III bear the fundamental aspects required to design ProTACD. Therefore, we address all identified design requirements during the conception and development of our approach as shown in Table II. In general, all identified requirements have been addressed, either by the generic process of ProTACD or by specific phases. For instance, the *holistic privacy view* is addressed by the overall privacy process of ProTACD and in particular by $P_D$ and $P_M$. This is enforced by the general policy to acquire multiple data across different domains, communication layers, and particularly by the type-oriented variation in $P_D$, e.g., vehicle identifying data. Moreover, by modeling the acquired data in $P_M$, we also can obtain the relation between previously unlinked and independent data, significantly increasing the holistic viewpoint in the process.

The *proactive privacy* design requirement is especially targeted by the overall privacy process of ProTACD as well as the fact that we aim to uncover and highlight previously unknown and unexpected privacy implications in $P_A$. In particular, *privacy awareness* is also an aim of ProTACD and shows the existence and magnitude of privacy implications in a documented way ($P_A$ and $P_{FD}$). In general, a higher privacy awareness implies a better sensibilization (or understanding) of the need and enforcement of privacy features in current and upcoming automobiles.

The requirement *vehicle development constraints* captures specific constraints in the automotive domain to avoid impractical privacy features, e.g., multidisciplinary influences, cost minimization, legal aspects, and safety. This requirement is addressed in all phases of ProTACD as shown in Table II.

TABLE II
SUMMARY OF DESIGN REQUIREMENTS EVALUATION.

| requirements (Sec. III) | by ProTACD | phase $P_D$ | phase $P_M$ | phase $P_A$ | phase $P_P$ | phase $P_{FD}$ |
|---|---|---|---|---|---|---|
| privacy awareness | ● | ○ | ○ | ● | ○ | ◐ |
| holistic privacy view | ● | ● | ● | ○ | ○ | ○ |
| proactive privacy | ● | ○ | ○ | ● | ◐ | ◐ |
| vehicle dev. constraints | ● | ◐ | ◐ | ● | ● | ● |
| vehicle lifecycle | ◐ | ○ | ○ | ○ | ◐ | ○ |

not addressed (○), partially addressed (◐), addressed (●)

Finally, the last point that we want to discuss is the *vehicle lifecycle*. The lifecycle of an automobile has three different phases (see Sec. III), and the most suitable phase for the prevention of privacy threats by default is the *development phase*. So far, ProTACD supports only privacy features during the *development phase* of an automobile. Thus, this requirement has been partially addressed by ProTACD and by employing the concept of privacy design patterns $P_P$. As a result, ProTACD fulfills the majority of privacy design requirements identified in Section III as well as addresses the basic weaknesses of current approaches, as examined in Sec. II.

### B. General analysis and discussion

ProTACD is a highly generic privacy process for the automotive domain that comprises several of specific aspects. ProTACD aims to complement existing security processes during vehicular development by exclusively focusing on privacy (similar to general PIA approaches). Moreover, our generic privacy process aims to move even beyond the limitations mentioned in Sec. II by incorporating automotive-specific privacy aspects that are vital to the provision of strong and sustainable privacy protection in the automotive domain.

However, ProTACD serves as a generic privacy process for any OEM with respect to privacy in vehicular development. Therefore, we have designed ProTACD as a generic privacy process for the automotive domain, where a concrete adaptation or incarnation of ProTACD incorporates the existing privacy and data protection strategy followed by OEMs as well as the implementation of ProTACD's phases. For example, a policy that states in the data acquisition phase which data is to be considered for analysis or the variation of the holistic viewpoint (see Sec. IV-A). Therefore, flexibility and abstraction of specific details are essential for such an approach. ProTACD aims this by providing a mix of generalization and structuring fundamental aspects.

However, so far ProTACD is limited to the development phase of an automobile. The initial introduction of ProTACD is also combined with relatively high efforts and costs because several realization steps need to be concerned, such as initial data models, privacy patterns, etc. However, once these steps are established by an OEM they can be used for different production lines, and thus keeping the effort comparable to a typical adjustment in the vehicle development phase.

## VI. Conclusion and Outlook

As information technology and connectivity are becoming seamlessly integrated into modern automobiles, the appropriate solutions to protect drivers' and vehicles' privacy are indispensable. However, current approaches regarding vehicle-related privacy do not specifically consider automotive constraints. To address these aspects, we identified automotive-specific privacy design requirements and proposed the concept of ProTACD that aims to provide privacy features during the development phase of an automobile. The key design aspect of ProTACD is based on a *privacy-by-design* approach, where privacy features can be integrated during the design and development phase of an automobile. One feature of ProTACD is the privacy assessment process that enables us to determine which data or vehicle domains are affected by critical privacy threats. Consequently, in our generic privacy process we recommend the provision of specific privacy metrics in $P_A$ to determine implications for different privacy principles, e.g., anonymity and data minimization. The main goal is to provide a generic and structured privacy process that supports OEMs in defining major privacy and development criteria for the design and application of privacy protection features. We believe that a realization of ProTACD posits benefits and yields many advantages for both drivers and OEMs by allowing for the recommendation, support, disclosure, and proof of the need for privacy measures. However, over time, new privacy requirements arise, and the automotive context changes. ProTACD is flexible enough to adapt to such changes to ensure that process results provide as much privacy as possible under the given generic approach.

In future work, we will provide an extensive investigation of the phases of ProTACD in order to provide privacy features during the *production period* of a vehicle (e.g., for installable telematics applications). At the same time, we are working on the realization (or adaptation) of several components of ProTACD, including data models [33], privacy metrics, and a framework for privacy design patterns in order to gradually integrate ProTACD into the vehicle development cycle of a particular OEM.

## References


[1] A. Held and R. Kroh, "It-security and privacy for telematics services," *PAMPAS'2*, September 2002.

[2] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *USENIX Security Symposium*, 2010, pp. 323–338.

[3] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *IV'11*. IEEE, 2011.

[4] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *IV'11*. IEEE, 2011.

[5] N. Asaj, "Datenschutz im Fahrzeug - Übersicht, Aspekte und erste Lösungsansätze," *Datenschutz und Datensicherheit (DuD)*, August 2011.

[6] D. Herges, N. Asaj, B. Koenings, F. Schaub, and M. Weber, "Ginger: An access control framework for telematics applications," in *TrustCom'12*. IEEE, 2012.

[7] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks - practical examples and selected short-term countermeasures," in *SAFECOMP'08*. Springer, 2008.

[8] M. Langheinrich, "Privacy by design - principles of privacy-aware ubiquitous systems," in *UbiComp'01*. Springer, 2001.

[9] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *PASSAT'09*. IEEE, 2009.

[10] Z. Ma, F. Kargl, and M. Weber, "A location privacy metric for V2X communication systems," in *Sarnoff'09*. IEEE, 2009.

[11] S. Duri, J. Elliott, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang, "Data protection and data sharing in telematics," *Mob. Netw. Appl.*, vol. 9, pp. 693–701, December 2004.

[12] S. Schulze, M. Pukall, G. Saake, T. Hoppe, and J. Dittmann, "On the need of data management in automotive systems," in *BTW'09*. Gesellschaft für Informatik (GI), 2009.

[13] J. Maerien, S. Michiels, S. Van Baelen, C. Huygens, and W. Joosen, "A secure multi-application platform for vehicle telematics," in *Vehicular Technology Conference*. IEEE, Sep. 2010.

[14] I. M. Usman and S. Lim, "Location privacy in automotive telematics," *Handbook of Research on Geoinformatics*, pp. 293–301, 2009.

[15] J. Krumm, "A survey of computational location privacy," *Personal Ubiquitous Comput.*, vol. 13, no. 6, pp. 391–399, Aug. 2009.

[16] A. Kung, J.-C. Freytag, and F. Kargl, "Privacy-by-design in ITS applications - the way forward," in *D-SPAN'11*. IEEE, 2011.

[17] M. Kost, J.-C. Freytag, F. Kargl, and A. Kung, "Privacy verification using ontologies," in *ARES'11*. IEEE, 2011.

[18] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Dealing with privacy issues during the system design process," in *ISSPIT'05*. IEEE, 2005.

[19] C. Kalloniatis, E. Kavakli, and Gritzalis, "Addressing privacy requirements in system design: the PriS method," *Requir. Eng.*, vol. 13, no. 3, pp. 241–255, Aug 2008.

[20] *Common Criteria for Information Technology Security Evaluation*, International Standard ISO/IEC 15 408, 2005.

[21] *Information technology – Security techniques – Information security management systems – Requirements*, International Standard ISO/IEC 27 001, 2005.

[22] "ISO/IEC 27005 Information technology - Security Techniques - Information security risk management," ISO, Tech. Rep., Jun. 2008.

[23] Information Commissioners Office (ICO), "Privacy impact assessment handbook. version 2.0." June 2009.

[24] M. C. Oetzel, S. Spiekermann, I. Grüning, H. Kelter, and S. Mull, "Privacy Impact Assessment Guideline for RFID Applications," German Federal Office for Information Security (BSI), Tech. Rep., 2011.

[25] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *VANET'07*. ACM, 2007.

[26] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-Tokens for conditional pseudonymity in VANETs," in *WCNC'10*. IEEE, 2010.

[27] M. C. Oetzel and S. Spiekermann, "Privacy-by-design through systematic privacy impact assessment-a design science approach," in *ECIS*, 2012.

[28] D. Wright, "Should privacy impact assessments be mandatory?" *Commun. ACM*, vol. 54, no. 8, pp. 121–131, Aug. 2011.

[29] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, "Pripayd: privacy friendly pay-as-you-drive insurance," in *WPES'07*. ACM, 2007.

[30] T. Hoppe, S. Kiltz, and J. Dittmann, "Automotive IT-security as a challenge: Basic attacks from the black box perspective on the example of privacy threats," in *SAFECOMP'09*. Springer, 2009.

[31] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," Aug. 2010, v0.34.

[32] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *MobiSys'03*, ser. MobiSys '03. ACM, 2003.

[33] N. Asaj, B. Wiedersheim, A. Held, and M. Weber, "Towards an identity-based data model for an automotive privacy process," in *PASSAT'12*. IEEE, September 2012.

[34] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Using privacy process patterns for incorporating privacy requirements into the system design process," in *ARES'07*, April 2007.

[35] M. Hafiz, "A collection of privacy design patterns," in *PLoP'06*. ACM, 2006.

[36] K. W. Tan, Y. Lin, and K. Mouratidis, "Spatial cloaking revisited: Distinguishing information leakage from anonymity," in *SSTD'09*. Springer-Verlag, 2009.

[37] S. Pearson and Y. Shen, "Context-aware privacy design pattern selection," in *TrustBus'10*. Springer-Verlag, 2010.