Privacy-by-Design in ITS Applications

The Way Forward

Antonio Kung
Trialog
Paris, France
antonio.kung@trialog.com

Johann-Christoph Freytag
DBIS
Humboldt-Universität zu Berlin
Berlin, German
freytag@dbis.informatik.hu-berlin.de

Frank Kargl
DIES Research Group
University of Twente
Enschede, Netherlands
f.kargl@utwente.nl

***Abstract*: This paper analyses how ITS applications may embrace a privacy-by-design approach. We take a holistic viewpoint based on three founding principles: data minimization, enforcement and transparency. The impact on architecture and technology is presented. Three challenges for ITS deployment are further discussed: the intrinsic instability of the resulting engineering process; the impact on future ITS platforms; the difficulty to reach consensus. Finally, tangible steps are identified on how to go forward in terms of further research work as well as building further industry consensus.**

Keyword: ITS; privacy; privacy-by-design; data minimization; enforcement; transparency; consensus for deployment.

I. INTRODUCTION

Intelligent Transport Systems (ITS) refers to the integration of information and communications technology into the transport infrastructure in order to enable the deployment of safety applications, traffic applications, and applications supporting other user needs. ITS involves communication within vehicles (e.g. a sensor transmits data to an in-vehicle subsystem), communication between vehicles (e.g. a vehicle transmits road status information to another vehicle), and communication between vehicles and other infrastructure stations (e.g. a vehicle transmits information to a road side unit or a remote traffic centre, or a vehicle receives position information).

The deployment of ITS involves addressing pervasive computing challenges [1]. ITS also includes physical processes, like the dynamics of vehicles. Therefore, deployment of ITS consequently has to address further challenges related to cyber physical systems [2]. Last but not least, ITS applications involve vehicle positioning and user supporting applications, therefore raising privacy issues related to location-oriented service such as those described in [3] as well as to aggregation of application data [4].

At the end of 2006, the Article 29 Working Party [21] issued a study on the emergency call application (eCall) [22]. Raising concerns on collected location oriented data, the study recommended implementing an option allowing vehicle drivers to disable the operation of eCall. The European Commission consequently organized discussions within the eSafety Forum [23] which resulted in the creation of the eSecurity Working Group [24]. In 2009, the European Data Protection Supervisor (EDPS) raised concern regarding the ITS Directive [5] calling for the use of *Privacy-by-Design*, i.e. a design process where privacy requirements are integrated from the start. As a consequence, the working group issued a report including a recommendation to work on the definition of privacy-by-design for ITS applications [6].

Privacy-by-Design (PbD) concepts were first proposed by policy makers in the 90s [25]. Recently, there have been attempts to provide an engineering understanding. Spiekermann and Cranor [7] identify and contrast two approaches: privacy-by-architecture and privacy-by-policy. The former focuses on data minimization while the latter focuses on enforcing policies in data processing. Gürses, Troncoso and Diaz [8] take the position that data minimization should be the foundational principle for Privacy-by-Design. The European Commission's FP7 project PRECIOSA [26] focuses on the design of a privacy policy enforcement system based on a protected distributed perimeter [9]. It also recognized the need for combining data minimization with privacy policy enforcement in an analysis of guidelines for PbD in ITS applications [10].

This paper takes this analysis further by providing a holistic viewpoint on how to apply PbD to ITS applications. The paper is structured as follows: Section II analyses PbD. It first defines three key principles, i.e. data minimization, enforcement and transparency, before describing the resulting PbD process and showing how the process can be applied to the example application of electronic tolling. Section III analyses the influence of PbD on technology and architecture. We discuss the impact of applying each of the three key principles as well as their impact on ITS communication and on the application deployment process. Section IV presents three challenges for ITS deployment: the intrinsic instability of the resulting engineering process, the impact on future ITS platforms, and the difficulty to reach consensus. Finally Section V proposes tangible steps on how to advance in terms of further research work as well as continued industry consensus building towards deployment.

978-1-4577-0351-5/11/$26.00 ©2011 IEEE

II. PRIVACY-BY-DESIGN

A. Principles of Privacy-by-Design

PbD involves three principles: data minimization, enforcement, and transparency.

Data minimization is related to the collection limitation principle for privacy of the OECD guidelines [27] which states that there should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. We restate the data minimization principle as follows: the collection of personal information should be kept to a strict minimum in the design of an application. Furthermore, the design process should take the default option that no identifiable data is collected.

This statement is not restrictive when we consider newly developed technology which allows replacing personal data by equivalent provable anonymous credentials or data sets. So instead of storing personal data, applications store related anonymous credentials or data sets. This approach was applied in [11] to design a location privacy preserving pay-as-you drive insurance application for vehicles. No location data is collected for invoicing. Rather, data is kept local within the vehicle, where provable statements about driver insurance fees are computed on the fly. Note that data minimization does not prevent data to be used and manipulated; it just prevents some data from being collected.

Enforcement is related to the security safeguards principle for privacy of the OECD guidelines, which states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. We restate the enforcement principle as follows: an application should be designed to provide maximum protection of personal data during operation. Furthermore, the design process should take the default option that all personal data is protected by technical means.

The rationale for the enforcement principle is to prevent accidental or malicious leaking of personal data. The massive deployment of ITS applications for millions of vehicles implies that a single failure or accident could have a huge negative impact. Technology for protection of stored personal data was exemplified by Hippocratic databases [12]. This was taken further by Kargl et al. [13] who present a data-centric approach for protecting personal data in a cooperative ITS environment. This approach was developed as part of the PRECIOSA project.

Transparency is related to the openness, the individual participation, and the accountability principles of the OECD guidelines. Means should be readily available to establish the existence and nature of personal data and the main purposes for their use. Furthermore, any individual should have the right to get information on data collected about him. Finally, a data controller should be accountable for complying with the measures required for privacy preservation. We restate the transparency principle as follows: applications should be designed and operated so that maximum transparency can be provided to stakeholders on the way privacy preservation is ensured. Furthermore, the design process should include specific verification procedures (e.g. open design, auditing), while the operation should include technical features for dynamic verification capabilities.

The rationale for transparency is trust. Applications involve users, service providers, and suppliers. Such stakeholders must be provided with guarantees that an application will behave properly. Transparency could have an impact on the design of the application itself because of the need to integrate dynamic verification.

Privacy Impact Assessment (PIA) [28] is an example of informational measures for transparency at the process level. Random spot checks for electronic tolling in a privacy-preserving solution [14] are an example of an implementation measure for transparency at operation level (such checks are actually considered as an application requirement). Such checks allow toll chargers to verify that toll service providers function properly. A toll charger can use various means for identifying vehicles in a given route segment (e.g. a camera with license plate reading capability) in order to request verification by the service provider that a vehicle has effectively been charged.

PbD can only work if all three principles are taken into account. Enforcement and transparency without minimization could result in a system with no privacy preservation. Minimization and transparency without enforcement could result in a system that is vulnerable to privacy leaks. Finally, minimization and enforcement without transparency could result in a system which will not be trusted by users.

B. Sketch of Overall Process

Figure 1 depicts the impact of PbD on a mainstream engineering process. The left column displays the five classic mainstream phases: *requirements*, *design*, *implementation*, *verification*, and *operation*. This is compared to the three PbD stages as displayed in the column to its right: *privacy requirements*, *privacy-aware design and implementation,* and *privacy verification and assurance*.

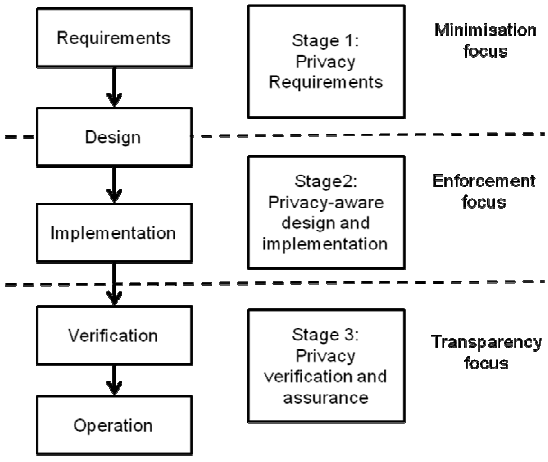

Figure 1. Impact of Privacy-by-Design on a Process.

The *privacy requirements* analysis stage focuses on data minimization. It takes as input application requirements, in

978-1-4577-0351-5/11/$26.00 ©2011 IEEE

particular the set of potential personal data involved, i.e. data that an application might process if no data minimization is applied. It considers privacy requirements by evaluating critically all personal data items to see whether they can be eliminated from the design as they are unnecessary to implement the required functionality or whether suitable data transformations can be applied through mechanisms such as anonymous credentials, aggregation, obfuscation, and change of resolution. The results of this stage are a minimized set of collected data, a set of operation data associated with the data policies corresponding to the minimization decision, and a set of privacy enhancing technologies to be used for data transformation.

The *privacy-aware design and implementation* stage focuses on enforcement of privacy protection. Each processed data item and its associated privacy policy is critically considered to see whether suitable technical enforcement can be applied through mechanisms such as access control, isolation, perimeter protection, or Hippocratic databases, or privacy policy enforcement. The result of this stage is a mapping of the set of operation data and data policies onto a set of privacy enhancing technologies to be used for enforcement and data retention.

The *privacy verification and assurance* stage focuses on transparency. It takes as input requirements for verification and assurance that have been elicited by stakeholders involved in the operation or the use of an application. These requirements might have an impact on the design process itself (e.g. applying a given method) and/or on the technical features to implement (e.g. implementing a given monitoring capability).

The integration of the three stages in an engineering process depends on the industry ecosystem. Figure 2 shows the resulting process in a situation in which best practices have been established. Requirements for minimization, enforcement, and transparency of a given application are known, and related mechanisms are readily available as off-the-shelf building blocks. The process focuses therefore on the integration of mechanisms.

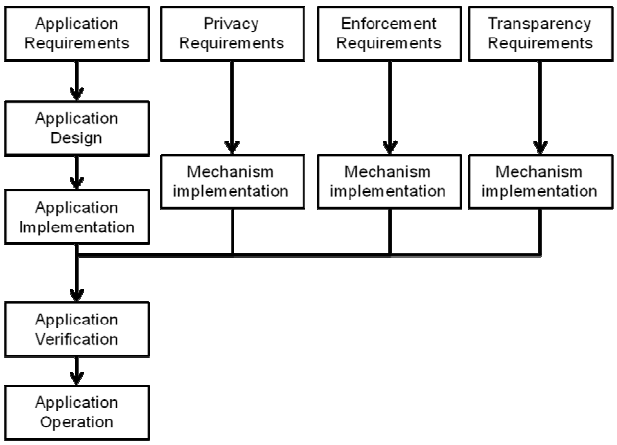

Figure 2. Privacy-by-Design Process in a Mature Ecosystem.

C. *Electronic Tolling Example*

Application requirements for electronic tolling can be described as follows: constantly record information about the vehicle route; ensure accuracy of the recorded information; bill the driver/vehicle based on the recorded route information; and keep the information for invoice verification.

A privacy-preserving solution supports the following requirements: keep the driven route private from road toll collectors, and keep route specific information only during the invoice litigation period. The result is a minimized data set consisting of the customer ID which is required to associate a vehicle with a customer account and billing information, the proof data of the driven route, and the associated cost. Associated data transformation could be based on the the optimistic payment protocol as described in [14]. Policies associated with manipulated data are as follows: detailed data concerning the vehicle route are kept and processed only inside the On-Board Equipment (OBE) of the vehicle; proof about the route driven is stored by the OBE only for a limited time that is needed for invoice verification; data sent outside the OBE only contain the customer ID and the cost for the distance that vehicle has driven the area operated by a toll charger. This data should not allow inferring data about a driver's travel. Finally this aggregated data is signed by the OBE to prevent tampering.

The privacy-aware design and implementation stage could be based on the mechanisms provided by the Privacy enforcing Run-time Architecture (PeRA) capability as developed by PRECIOSA [13][15]. In a nutshell, the PeRA provides a protected perimeter for data processing and privileged software execution. Deployed within an OBE, it ensures that recorded route information is only processed inside the protected perimeter within the OBE according to given privacy policies, i.e. raw position data is accessed only by a cost calculation application running only inside the perimeter. The application calculates the aggregated cost values that are then reported outside the perimeter and transmitted to the toll service provider. The system makes use of end-to-end transport encryption so that reports are authenticated with the OBU's credentials and are kept confidential. In addition, the privileged software is responsible for the data transformations identified in the previous stage. This allows aggregated proofs to be generated and stored inside the protected perimeter of the OBE for invoicing, instead of detailed location measurements. The PeRA can further support such proofs by ensuring the integrity of the components which process the data. After the invoicing litigation period, the PeRA automatically ensures deletion of the proof data. Furthermore, the PeRA architecture also solves an important ITS platform requirement, i.e. allowing the execution of several independent applications at the same time without interference. Applications running in an OBE outside the perimeter have no access to the raw data inside.

Finally, the privacy verification and assurance stage takes into account application requirements such as random spot checks. Furthermore, it also includes a static analysis phase

978-1-4577-0351-5/11/$26.00 ©2011 IEEE

aiming at providing a formal guarantee of privacy preservation, e.g. through the P3L (PRECIOSA privacy policy language) which provides the basis for an ontology-based analysis [16]. It could further include some common criteria evaluation [29], i.e. allowing for the verification that the implementations conform to an agreed electronic tolling protection profile. Finally, it includes conformance testing features to validate the compliance, ensuring that the implemented data transformation and enforcement features achieve what is specified. Preliminary investigation on the content of such conformance testing shows that little work has been done on this so far. Therefore some industry consensus will be needed, a matter we will discuss in section IV.

III. Impact on Technology and Architecture

The application of PbD will have a far reaching impact on the choice of technology, which in turn will have an influence on architectural aspects of the resulting implementations.

A. Technology

As discussed in the previous section requirements and technology resulting from a PbD approach may profoundly impact application technology (i.e. technology that would be used if privacy is not taken into account).

Data minimization and enforcement mechanisms are considered as Privacy Enhancing Technologies (PETs). It is a research area which constantly produces new insights. In the near future we might expect significant results both in the area of data transformation (e.g. anonymous credentials) and of enforcement (e.g. platform protected perimeters).

Transparency approaches involve features at both the process level and the operation level. Examples for such work are the TERESA FP7 project [30] and the OVERSEE FP7 project [31]. The former focuses on the use of security and dependability patterns that can later be integrated into an application development process. The latter uses platform virtualization to allow the deployment of independent applications in the same OBE. Results are expected in both areas in the near future.

B. Architecture

PbD requirements have an influence on architecture both at logical and physical level.

Minimization and enforcement impact the way data is logically structured. The consequence of minimization is that some data can no longer be collected and freely accessed. The consequence of enforcement is that all raw data (i.e. data that could be used to build up personal profiles) must be located and manipulated in a protected area of the system. Implemented mechanisms can also have a cross-layer effect. Location privacy may require the use of pseudonyms which may consequently modify the structure of the communication subsystem as shown in SeVeCom [17][18]. Similarly, monitoring capabilities designed for transparency purposes may have a transversal impact on the instrumented subsystems.

Minimization may have a drastic effect on the distributed structure. The privacy preserving electronic tolling solution described in the previous section contrasts significantly with classical approaches since all cost calculations are carried out within the vehicle OBE instead of being carried out at in a central server. Impact at the distributed structure can actually be influenced by trade-off decisions, as illustrated now.

For the sake of this example, we assume a simplified ITS infrastructure consisting of three types of computing systems, a central server (CS) operating on the ground, road side units (RSU), and an OBE in each vehicle. Deployment considerations could lead to different distributed configurations, three of which we describe here. If neither RSUs nor OBEs can afford the needed computing resources, then all calculations are done in the CS, i.e. we have an enforcement perimeter that includes the CS-RSU-OBE chain. If RSUs can afford computing resources while the OBE cannot, then the calculations are carried out on the fly by a given RSU on behalf of a number of neighboring vehicles, i.e. the enforcement perimeter includes the RSU-OBE chain. Finally, if the OBE has sufficient computing resources, then all calculations are kept within the OBE, i.e. the enforcement perimeter is confined to the OBE. From a privacy preservation viewpoint, the risks are as follows. In the first case, the CS-RSU-OBE chain implies that data concerning all vehicles have to physically be made available at the central server level. Assuming that data transmitted to the CS are anonymized data, there is a risk of future re-identification of all data that are stored within the CS data retention time. In the second case, the RSU-OBE chain implies that data concerning a number of neighboring vehicles have been created in a fixed geographic position (i.e. where a given RSU is located). This creates the risk of future re-identification of all data contained in the RSU concerning all vehicles which had an interaction with the RSU within the RSU data retention time. In the last case finally, there is the risk that data contained in a vehicle could leak out of the OBE during its retention time.

IV. Challenges for ITS

A. Addressing the Instability created by PbD

A challenge for the advent of PbD in ITS applications is the instability of the engineering process itself. As we described in the previous section applying PbD can have an impact on the resulting architecture. An ITS infrastructure involves many suppliers with established business roles and liabilities. Changing the architecture might mean changing roles. The inertia of an existing ITS value chain might become a barrier for change.

Furthermore, evolutions of PET may change the architecture during the lifetime of a deployed ITS application to introduce newer and better PETs. Such change could involve massive re-deployment costs (e.g. replacing some equipment in all vehicles or RSUs).

978-1-4577-0351-5/11/$26.00 ©2011 IEEE

B. Building a Privacy-friendly Platform

A challenge for the advent of ITS is the availability of a platform on which applications may be deployed. Making this platform privacy friendly will involve further challenges.

First of all, such a platform should have the capability to morph itself into a version that can support mechanisms for data minimization, enforcement and transparency. For instance, the support for PeRA capabilities may change the platform significantly. A trade-off between application specific features and platform generic features must be identified.

ITS platforms must also support multiple applications, possibly operated by different service providers. These applications could involve different data minimization, privacy enforcement and transparency requirements. Therefore, an OBE must be able to support different applications on behalf of different service providers. Moreover, each application must be isolated properly to meet the requirements of each individual application. Isolation is addressed by the OVERSEE FP7 project [31]. Taking into account PbD could involve additional challenges, such as the support of multiple independent enforcement perimeters.

The eSecurity group has provided an analysis of vulnerabilities in ITS applications [6], concluding that a key vulnerability is the mixing of vehicle independent electronic systems which are the responsibility of vehicle manufacturers with interactive systems (which include ITS applications). Separation between those two worlds must be enforced in the architecture of future privacy-friendly ITS platforms.

C. Reaching Consensus

To make privacy-friendly ITS a reality, consensus must be be reached among different stakeholders. Adopting a common PbD process would ensure the development of privacy-friendly ITS applications designed in a similar manner. Reaching consensus on a set of PbD requirements for a given ITS application would ensure a similar level of privacy support from all manufacturers. Reaching a consensus on resulting mechanisms would ensure interoperability. Consensus on the use of common privacy-friendly ITS platforms would decrease costs and speed up development. Finally, agreeing on roadmaps for mechanisms and platforms might lead to clear and coordinated investment calendars.

V. The Way Forward

A. Research Level

Further research must be carried out to reach a comprehensive understanding of PbD in the area of privacy modeling, privacy metrics, privacy-aware analysis and software design, privacy-enhanced policy language, privacy-aware request processing, and privacy-aware communication. More details are provided in [19].

B. Industry Level

Consensus building is needed when potential conflicts of interest arise. Such consensus was necessary in the case of pollution prevention and the IPPC directive [33], where chemical business stakeholders had to reach a consensus with environmentalist stakeholders. Consensus was established through the so-called Sevilla process [20] which involved the creation of specific working groups organized with the help of dedicated staff from the European Commission (located in Sevilla, hence the name of the process). These working groups had the objective of producing common reference documents on *Best Available Techniques* (BAT) for pollution prevention. The challenge for the consensus builders has been to combine the notion of "best" and the notion of "available". It is interesting to note that the resulting documents are merely enablers. The industry is free to use them or not. The BAT approach was mentioned by the European Data Protection Supervisor in their opinion on the ITS directive [5]. The same level of conflict of interest occurs in ITS, between stakeholders involved in creating ITS applications and stakeholders concerned with privacy.

We call for a similar approach and foresee a number of horizontal as well of vertical working groups. Horizontal working groups could focus on roadmaps (e.g. maturity of technology), interoperability (e.g. the extension of interoperability aspects to privacy-based initiatives, such as the Frame architecture [32]), and the definition of a common PbD process. Vertical groups could focus on privacy reference documents for individual ITS applications (e.g. eCall, electronic tolling). Working groups could produce several generations of documents to cope with evolution of requirements and technology.

Working groups alone will not be sufficient to cope with some industry issues. In particular, we believe that further R&D investigation on transparency mechanisms is needed. They will be critical for acceptance and deployment of privacy-preserving ITS applications. In particular we do not believe that third party certification or approaches based on reputation management alone are suitable. Rather than having third parties judging the level of privacy reached, we would advocate an approach where third parties would assess and certified the level of transparency reached, thereby allowing a vaster community of stakeholders (e.g. industry, associations, users) to use the available transparency mechanisms and make more qualified open judgments on the privacy level of a given application.

Acknowledgments

This paper mostly describes work carried out within the FP7 PRECIOSA project [26]. It also mentions results from the FP6 SEVECOM [34] and FP7 OVERSEE [31] projects. These contributions will be integrated into the FP7 PRESERVE project [35] for use in field operational test initiatives. We acknowledge the support of the European Commission DG INFSO for all these projects.

References

[1] M.Satyanarayanan. Pervasive Computing: Vision and Challenges. IEEE Personal Communications, August 2001.

[2] R.Rajkumar, I.Lee, L.Sha, J.Stankovic. Cyber-physical systems: the next computing revolution. Design Automation Conference. June 2010

[3] N.Doty, E.Wilde, “Geolocation Privacy and Application Platforms”, ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, November 2010

[4] R.Agrawal, R.Srikant: "Privacy-Preserving Data Mining", ACM SIGMOD Int'l Conf. on Management of Data, Dallas, May 2000

[5] Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe. July 2009. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

[6] eSecurity Working Group. Vulnerabilities in Electronics and Communications in Road Transport: Discussion and Recommendations. June 2010. See [24].

[7] S.Spiekermann, L.Cranor, “Privacy Engineering”, IEEE Transactions on Software Engineering, Vol. 35, Nr. 1, January/February 2009, pp. 67-82

[8] S. F. Gürses, C. Troncoso, and C. Diaz, "Engineering Privacy by Design," In Computers, Privacy & Data Protection, 2011.

[9] F.Kargl, F.Schaub, S.Dietzel. Mandatory Enforcement of Privacy Policies Using Trusted Computing Principles. Intelligent Information Privacy Management Symposium, Stanford University (AAAI 2010 Spring Symposia). March 2010.

[10] Guidelines for Privacy Aware Cooperative Application. Deliverable D11. Preciosa FP7 Project. November 2010. See [26]

[11] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel. PriPAYD: privacy friendly pay-as-you-drive insurance. Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society, WPES 2007, pages 99-107. ACM, 2007 Pripayd

[12] R.Agrawal, J.Kiernan, R.Srikant, Y.Xu: "Hippocratic Databases", 28th Int'l Conf. on Very Large Data Bases, Hong Kong, August 2002

[13] V2X Privacy Verifiable Architecture. Deliverable D7. Preciosa FP7 Project. November 2009. See [26]

[14] J.Balasch, A.Rial, C.Troncoso, C.Geuens, B.Preneel, and I.Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, pages 63-78. USENIX Association, 2010.

[15] Mechanisms for V2X Privacy. Deliverable D10. Preciosa FP7 Project. March 2010. See [26]

[16] Models and privacy ontology for V2X. Deliverable D6. Preciosa FP7 Project. November 2010. See [26]

[17] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. IEEE Communications Magazine, Vol. 46, No. 11, pp. 100-109, November 2008.

[18] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, B. Wiedersheim, E. Schoch, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure Secure Vehicular Communications: Implementation, Performance, and Research Challenges. IEEE Communications Magazine, Vol. 46, No. 11, pp. 110-118. November 2008.

[19] Research contribution to V2X privacy and roadmaps. Deliverable D16. Preciosa FP7 Project. November 2010. See [26]

[20] H.Schoenberger, European Commission. Integrated pollution prevention and control in large industrial installations on the basis of best available techniques – The Sevilla Process. Journal of Cleaner Production. Vol 17 (2009). pp1526–1529.

[21] Article 29 working group. http://ec.europa.eu/justice/policies/privacy/workinggroup

[22] eCall. http://ec.europa.eu/information_society/activities/esafety/ecall

[23] eSafety forum. http://ec.europa.eu/information_society/activities/esafety

[24] eSecurity working group. http://www.icarsupport.eu/esafety-forum/esafety-working-groups/esecurity/

[25] A.Cavoukian. Information & Privacy Commissioner Ontario, Canada. Privacy-by-design. http://www.privacybydesign.ca

[26] PRECIOSA (Privacy Enabled Capability in Co-operative Systems and Safety Applications) FP7 project..http://www.preciosa-project.org/

[27] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://oecdprivacy.org

[28] Privacy Impact Assessment. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

[29] Common criteria. http://www.commoncriteriaportal.org

[30] Teresa FP7 (Trusted Computing Engineering for Resource Constrained Embedded Systems Applications) project. http://www.teresa-project.org/

[31] Oversee (Open VEhiculaR SEcurE platform) FP7 project. https://www.oversee-project.com/

[32] Frame architecture. http://www.frame-online.net/

[33] Directive 2008/1/EC concerning Integrated Pollution Prevention and Control. 15 January 2008, http://ec.europa.eu/environment/air/pollutants/stationary/ippc/

[34] SeVeCom (Secure Vehicular Communication) FP6 project. . http://www.sevecom.org/

[35] PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) FP7 project. http://www.preserve-project.eu/

978-1-4577-0351-5/11/$26.00 ©2011 IEEE