ICT and Privacy: Barriers

Antonio Kung

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

Abstract. This paper identifies barriers for the handing of privacy issues caused by *Information and Communication Technologies* (ICT). It reports first on experience gained in addressing privacy issues in *Intelligent Transport systems* (ITS). It discusses two applications, eCall and Pay-Per-Use. It identifies barriers for privacy and suggests recommendations. These barriers are at the application level (conflict of interest, lack of consensus on protection policies), at the design level (agreement on the meaning of Privacy-by-Design, neglect of architecture impact, lack of practice) and at the implementation level (leaks created by ICT infrastructures, lack of flexibility).

Keywords: Privacy-by-Design, Minimisation, Enforcement, Transparency, PET, Architecture, PEAR.

1 Introduction

The European Commission adopted in 2010 the directive 2010/40/EU [1] in order to address the compatibility, interoperability and continuity of Intelligent Transport Systems (ITS) solutions across the EU, for areas such as traffic and travel information, eCall emergency systems, and intelligent truck parking. The directive was preceded by the adoption of an Action Plan [2] in 2008. This action plan included four application areas, (1) optimal use of road, traffic and travel data, (2) continuity of traffic and freight management, (4) road safety and security, and (4) integration of vehicle and transport infrastructure. The eSafety initiative [3] provides more information on the many projects that were undertaken. The action plan also included a specific transversal area: data protection and liability, for which a series of research projects were started: SeVeCom [4], PRECIOSA [5], EVITA [6], OVERSEE [7] and PRESERVE [8]. They addressed secure communication, privacy, protection against vehicle intrusion, secure platforms, and validation through field operational tests respectively. The eSecurity Working Group [8] involving data protection and ITS stakeholders was also created. Work is continuing as the European Commission is currently carrying out a study to assess data protection in ITS [10] while keeping the new privacy regulation [11] in perspective.

This paper reports on the insight gained from these undertakings. It will first report on experience gained in the study of two applications, eCall and Pay-Per-Use insurance, and two R&D projects, SeVeCom and PRECIOSA. It will then describe barriers to ICT which are not necessarily specific to ITS and provide recommendations for

B. Preneel and D. Ikonomou (Eds.): APF 2012, LNCS 8319, pp. 177–186, 2014.

ICT in general. These barriers are at the application level (conflict of interest, lack of consensus on protection policies), at the design level (agreement on the meaning of Privacy-by-Design, neglect of architecture impact, lack of practice) and at the implementation level (leaks created by ICT infrastructures, lack of flexibility).

2 Experience Gained from ITS

2.1 Applications

eCall is a European initiative intended to bring rapid assistance to motorists involved in a collision anywhere in the European Union. The development of solutions for eCall rapidly led to concern about the location tracking of vehicles. The Article 29 Working Group Party published a working document on eCall in 2006 [12] which recommended the possibility of switching off the eCall capability. This recommendation raised further issues that were discussed in a meeting organised by the technology subgroup of the Article 29 WG Party in 2009. During this meeting a second generation eCall product, developed in liaison with the French data protection authority (CNIL) was presented by PSA. This solution included privacy preservation features, e.g. blurring vehicle location data to avoid calculation of speed, removing physically collected data on a daily basis. The solution also coped with liability issues created by the proposed approach of providing a switch-off capability: what if a vehicle eCall capability is switched off by one person and then the vehicle is used by another person which is not aware that it is switched off. It was suggested that a systematic check be included along with a request that the driver maintain the eCall capability off. The eCall case was a wake-up call within the ITS community on the need to address location issues.

Pay-As-You-Drive Insurance is a type of automobile insurance whereby the costs of insurance are dependent upon time, distance, behaviour and location. Further to the Article 29 WG party document on eCall, the European Commission organised a workshop in privacy in ITS in 2007. During this workshop a person from the French protection agency (CNIL) presented the case of MAAF, a French insurance company which requested to deploy a Pay-As-You-Drive solution but was denied authorisation. The same year, a study was started at research level that led to the specification of a privacy friendly solution called PriPayd [13] based on an approach whereby location data was kept in the vehicle. Instead of having internet based systems collecting the data and calculating invoices, only minimum billing data are provided by the vehicle. The striking characteristics of the solution was that by focusing on the physical minimisation of data (i.e. data is not collected on the internet, but is kept in the vehicle), the architecture of an application was profoundly changed.

2.2 ITS Technology

Rather than focusing on the impact of privacy on ITS applications, SeVeCom and PRECIOSA focused on how Privacy-by-Design applied to ITS applications could impact on the underlying ICT technology.

SeVeCom was an FP6 project that ran from 2006-2009 [4, 14, 15]. It focused on security for communication systems involving cooperating vehicles (i.e. car-to-car

and car-to-infrastructure communication). It therefore focused on privacy leaks that can occur in this kind of communication.

SeVeCom made the following analysis: communication includes application data and protocol data. Application data need to be transmitted with different levels of security for integrity or confidentiality reasons. Protocol data might also need to be transmitted in a secure way since they can lead to privacy infringement. This is the case of the communication of the MAC[1] address in car-to-car communication. The car-to-car MAC address was initially devised as a fixed unique address. Similarly to fixed IP addresses, the MAC address could therefore be considered as personal data, because it could be used to track a vehicle.

SeVeCom contributed the following technology:

- a mechanism in the form of proof of concept for secure communication, with pseudonym change management to address the fixed MAC address problem,
- a contribution to flexibility in the form of an implementation structure to allow for easy integration in existing implementation protocols[2].

Future deployed ITS infrastructure could reuse the SeVeCom implementation to solve the fixed MAC address issue.

PRECIOSA was an FP7 project that ran from 2009-2010 [5]. It addressed the problem of protecting collected data in ITS applications. It therefore focused on measures for privacy leaks that can occur when collecting data, in particular in ICT deployment based on common platforms.

PRECIOSA work was heavily influenced by discussions that took place in the eSecurity Working Group [8] concerning data protection stakeholders as well as privacy enhancing technology stakeholders and the need to adopt a Privacy-by-Design approach[3]. Since the meaning of Privacy-by-Design lacked clarity, the concept was investigated by the project. PRECIOSA concluded that it involves three principles, minimisation, enforcement and transparency [17] which are defined as follows.

Minimisation is related to the collection limitation principle for privacy of the OECD guidelines [18]. Applied to Privacy-by-Design, it means that the collection of personal information should be kept to a strict minimum in the design of an application. Applied to current technology trends, it means that the design process should start with the default option that no identifiable data is collected. Moreover, whenever possible personal data should be replaced by equivalent minimised data. For instance, birthdate information can be replaced by a computing proof that a person is over eighteen. Minimisation leads to requirements on what shall not be collected, on where it is collected, and on the use of specific minimisation technology. This approach was applied in Pay-As-You-Drive insurance [13].

Enforcement is related to the security safeguards principle for privacy in the OECD guidelines, which states that personal data should be protected by reasonable security

[1] MAC stands for Medium Access Layer. The MAC address identifies a communication entity in a physical network.

[2] Based on the so-called *hooking architecture* [15].

[3] The term Privacy-by-Design was coined by Ann Cavoukian, the Ontario Data Protection Commissioner [16]. In January 25, 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. The reform integrates the concept of Privacy-by-Design [11].

safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data[4]. Applied to Privacy-by-Design, it means that an application should be designed to provide maximum protection of personal data during an operation. Applied to current technology trends, it means that the design process should start with the default option that all collected personal data should be protected by technical means. They should automatically ensure that data are accessed by the authorised parties (e.g. location data is only made available to a location based application) and that such data is automatically removed at the expiration of a retention period (e.g. at the end of the day). This approach is exemplified by Hippocratic databases [19]. PRECIOSA took this further by developing a data-centric approach for protecting personal data in a cooperative ITS environment [20]. Enforcement leads to requirements on what must be protected, on how it is protected (which leads to organization decisions), and the use of technology for protection (in order to prevent from leaks due to manual organization of protection).

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 aa well as the main purposes for their use. Furthermore, an 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. Applied to Privacy-by-Design, this means that applications should be designed and operated so that maximum transparency can be provided to stakeholders about the way privacy preservation is ensured. In particular, the design process should include specific verification procedures (e.g. open design, auditing). Applied to current technology trends, it means that the design process should start with the default option that mechanisms for verification during operation should be included. For instance mechanisms could be included to provide evidence that some location data have been removed. Transparency leads to requirements on what evidences have to be produced, on how these evidences are provided (which leads to architecture decisions), and on the use of technology for evidence provision.

PRECIOSA contributed the following technology:

- a proof of concept data-centric approach for protecting personal data in a cooperative ITS environment,
- an understanding of the meaning of Privacy-by-Design.

Future deployed ITS infrastructure could reuse the PRECIOSA implementation to ensure the right level of enforcement.

3 Barriers to ICT

While investigating the impact of privacy on ITS, barriers were identified. Many of the barriers are general in nature, and they also apply to ICT.

[4] 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 liability impact.

3.1 Application Level: Conflict of Interest

When applications values are based on the use and exploitation of user data, conflict of interest will occur. This is what is currently happening in today social networks applications, and in ITS when application stakeholders want to make use of collected location based data in order to provide value-added services. There is a risk that privacy regulation and Privacy-by-Design are considered to be an obstacle for deployment of these location-based services, leading to the weakest interpretation on how to apply Privacy-by-Design.

Solving a conflict of interest in a global manner necessitates consensus. This consensus must ensure that an application can be cost effectively developed and deployed, which is the priority of application stakeholders) while protecting personal data efficiently, which is the priority of privacy defence stakeholders. It is recommended to put in place a consensus process supported by policy makers. This was suggested by EDPS [23] who recommends the development of best available techniques through "comitology", i.e. a consensus process. This approach was applied in the case of pollution prevention techniques, through a process supported by the European Commission called the Sevilla Process [24].

3.2 Application Level: Lack of Consensus on Protection Policies

Protection policies require agreement (e.g. whether a data field should be encrypted for confidentiality?). Without such agreement, different policies can be applied, leading to situations where the level of protection reached is that of stakeholders applying the least protective policy. Consider for instance data retention policy where some stakeholders simply do not remove data. A process for agreement on policies must be available but it is currently ill-supported by current standardization processes, since the time frame for standardization is so long. A more agile and flexible consensus process is needed.

3.3 Design Level: Lack of Agreement on the Meaning of Privacy-by-Design

The term Privacy-by-Design has been used widely by policy makers, including in the new privacy regulation [11]. It is generally associated with Privacy Impact Assessments (PIAs), an instrument that has been the subject of much study [25]. But as highlighted in [21], there is a gap between the understanding of this concept by policy makers and by the ICT engineering community. A common technical understanding of Privacy-by-Design is needed as a result of standardization work. [26, 27] are examples of work contributing to this understanding. The contribution of PRECIOSA explained in section 2.2 is an attempt to shape this understanding [17]. The creation of a multidisciplinary working group working in this understanding would be needed.

3.4 Design Level: Neglect of Architecture Impact

The architectural dimension of Privacy-by-Design is currently not well highlighted. Yet almost all privacy preserving solutions devised today have a profound impact on architecture as shown in the Pay-Per-Use case [13], the road charging case [30] and

the smart meters case [31, 32]. Currently research on privacy puts more value on contributions related to crypto aspects, which overshadows the need to assess architecture impacts aspects. For instance Stanford University has a web page which lists Privacy Enhancing Technologies (PET) [33]. However, no equivalent can be found for architectures. We have also observed that the meaning of PET is often narrowed to security and crypto-based features for minimisation. We believe that a broader meaning should be used, i.e. a PET can be a mechanism for minimisation, for enforcement of policies or for transparency.

It is recommended to take a more global architectural view rather than a mechanism centric viewed as suggested by the term PET. Let us switch to *Privacy Enhancing Architectures* (PEARs)!

3.5 Design Level: Lack of Practice of Privacy-by-Design

There is currently little of practice of Privacy-by-Design. We need to create a wealth of architectures (PEARs) and of measures (PETs): Privacy enhancing technologies are not well spread. Minimisation technology is a recent development. Much research is still in progress and a wealth of new results can be expected in the near future. Furthermore, it is also expected that new threats will be discovered as applications are deployed, which will also lead to new measures. Enforcement and transparency measures are currently mostly managed through manual and organisational activities. Industry expertise is not commonly available. Little research work is available on enforcement for privacy, e.g. [19, 20] for run-time protection perimeters. Nevertheless, these efforts could leverage on well-established work on enforcement of access such as the Bell-La Padula model [28].

Another issue is that Privacy-by-Design has to be properly integrated in the development process of applications. This integration is not easy to specify because of the wide variety of engineering processes in use (e.g. automotive, railways, smart meters, etc..)

Finally, Privacy-by-Design is a topic that is not addressed in the standard education curriculum. When current students are employed in the next few years, they will have little understanding of what a Privacy-by-Design process is.

3.6 Implementation: Leaks Created by ICT Infrastructures

ICT infrastructures include technology components which use and possibly transmit system data. Such data are needed for the operation of the infrastructure. For instance a run-time platform will make use of operating data such as computing resource descriptions, or a communication stack will involve the transmission of protocol data. In current industry practices, such data can be easily monitored for conformance testing or for performance monitoring purposes. However, the monitoring capability itself creates problems. Monitoring the content of memory used by an application is obviously a problem if there is a possibility to derive personal data from it. Transmitting protocol data can also be a problem, for instance a fixed IP address is enough to identify a user. The design of recent car-to-car communication systems initially planned to

use fixed MAC[5] addresses. However, this data would be enough to track a vehicle. Even worse, simply tracking communication activity could be enough in many cases to track user activity. For example, a device that transmits data could be a proof that a user is at home.

A novel approach to the design of ICT infrastructure must be taken so that it provides suitable protection of system data and system activity. It must be protection oriented, i.e. system data must be protected against unauthorized access. Isolation features should be integrated to prevent access to system data or activity by unauthorised stakeholders.

3.7 Implementation: Lack of Flexibility of ICT Infrastructures

The deployment of ICT infrastructures currently involves heavy investments and therefore any need for unanticipated modification is difficult to take into account. In fact, it is in general impossible to modify part of an ICT infrastructure while it is operating, in particular when millions of entities are involved[6].

Evolving requirements for data protection necessitate two levels of flexibility of ICT infrastructures. First of all, *policies for protection* could evolve. For instance some data initially transmitted in the clear are now required to be transmitted confidentially. Or policies for pseudonym renewal need now to be changed in a communication protocol. The challenge is to provide support for defining, creating and changing such policies dynamically. Secondly, *privacy requirements* could change. This may be caused by the discovery of privacy leaks, or by changing societal perception. For instance the physical location of smart grid data initially collected in a remote centre could evolve and be kept at the level of a smart meter. The challenge is to provide support for defining, creating and changing architecture parameters such as the physical distribution of data. This in turn has an impact on the definition of interoperability and related standards. For instance interoperability standards for a smart meter could become obsolete as a result of an architecture change.

Currently ICT infrastructures are designed and deployed according to practices which prevent such levels of flexibility. Policies are often totally hardwired, i.e. they are meant to remain unchanged. But perhaps more worrying, current architecture patterns are defined statically and not meant to change, as this would imply modifying interfaces that are frozen and standardized. Supporting the modification of patterns therefore means modifying development and standardisation practices.

Addressing ICT infrastructure flexibility necessitates a long-term research plan to address the following neglected features: *policy as a service*, i.e. the infrastructure should provide support for the flexible deployment of new policies. This should involve a set of consistent technologies in terms of description (policy language), of generation and of deployment (reconfiguring the infrastructure accordingly);

---

[5] The fixed MAC address issue is currently taken into account in ITS standardization activities. See [22].

[6] This kind of barrier must be well anticipated. This is what happened for instance when France switched overnight from 8 digit to 10 digit phone numbers.

architecture as a service, i.e. the infrastructure should provide support for the flexible deployment of new architecture patterns. This should involve features for describing architecture changes, generating modified interoperability specifications and deploying reconfigured items; *agile interoperability*, i.e. new industry practices must be put in place to make sure that reconfigurations of architecture go in parallel with appropriate modification of interoperability specifications.

3.8 Addressing Barriers

The following table provides examples of measures that can be taken to address these described barriers. A feasibility assessment is also provided.

Type of Barrier	Barriers	Recommendation of measures to policy makers	Feasibility
Application level	Conflict of interest	Creation and support of a consensus process	Domain dependent. Could be a short term goal for some domains
	Lack of consensus on policies	Creation and support of a consensus process	
Design level	Lack of agreement on the meaning of privacy-by-design	Create a multidisciplinary working group to define an agreed engineering process.	Short term goal[7]
	Neglect of architecture impact	Switching focus from PETs to PEARs	Short term goal
	Lack of practice of privacy-by-design	Wealth of architectures (PEARS) and measures (PETS)	Short term goal
		Integration into application design processes	Long term goal
		Support in curriculum	Short term goal
Implementation level	Leaks created by ICT infrastructures	Protection oriented design of infrastructure bricks, based on e.g. isolation features	Long term goal
	Lack of flexibility of ICT infrastructures	Research on flexibility Changing standardization practices for interoperability	Long term goal

Acknowledgements. We acknowledge the support of the European Commission in the following FP6 and FP7 projects: SeVeCom, PRECIOSA, OVERSEE, PRESERVE.

References

1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:FULL:EN:PDF
2. ITS Action Plan and Directive, http://ec.europa.eu/transport/its/road/action_plan/action_plan_en.htm

[7] Many contributions on PETs already include implicit contributions on PEARS.

3. eSafety initiative, http://ec.europa.eu/information_society/activities/esafety/index_en.htm
4. SeVeCom, http://www.sevecom.org/
5. PRECIOSA, http://www.preciosa-project.org/
6. EVITA, http://www.evita-project.org
7. OVERSEE, https://www.oversee-project.com/
8. PRESERVE, http://www.preserve-project.eu/
9. eSecurity Working Group, http://www.esafetysupport.org/en/esafety_activities/esafety_working_groups/esecurity.htm
10. EC Study: Assess the security and personal data protection aspects related to the handling of data in ITS applications and services and propose measures in full compliance with Community legislation, http://ec.europa.eu/transport/its/events/2012_06_12_data_protection_en.htm
11. New privacy regulation in Europe, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
12. Article 29 Working Group Party working document on data protection and privacy implications in eCall initiative (September 26, 2006), http://ec.europa.eu/information_society/activities/esafety/doc/esafety_forum/ecall/art29wp_ecall_en.pdf
13. Troncoso, C., Danezis, G., Kosta, E., Balasch, J., Preneel, B.: PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance. IEEE Transactions on Dependable and Secure Computing (to appear), https://www.cosic.esat.kuleuven.be/publications/article-2013.pdf
14. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.-P.: SeVeCom. Secure Vehicular Communications: Design and Architecture. IEEE Communications Magazine 46(11), 100–109 (2008), http://infoscience.epfl.ch/record/129969/files/sevecom1.pdf
15. Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Wiedersheim, B., Schoch, E., Thong, T.-V., Calandriello, G., Held, A., Kung, A., Hubaux, J.-P.: SeVeCom. Secure Secure Vehicular Communications: Implementation, Performance, and Research Challenges. IEEE Communications Magazine 46(11), 110–118 (2008), http://infoscience.epfl.ch/record/129970/files/sevecom2.pdf
16. Privacy-by-Desig, http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/
17. Kung, A., Freytag, J., Kargl, F.: Privacy-by-design in ITS applications. In: 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, Lucca, Italy (June 20, 2011)
18. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://oecdprivacy.org
19. Agrawal, R., Kiernan, J., Srikant, R., Xu, Y.: Hippocratic Databases. In: 28th International Conference on Very Large Data Bases, Hong Kong (August 2002)
20. Mechanisms for V2X Privacy. Deliverable D10. Preciosa FP7 Project (March 2010), http://www.preciosa-project.org/
21. Kung, A.: From PIAs to Engineering Practices. Computer Privacy and Data Protection 2012 (2012), http://www.cpdpconferences.org/I-Q/Resources/KUNG_120127.pdf

22. ETSI ITS WG5, http://docbox.etsi.org/workshop/2011/201102_ITSWORKSHOP/06_INSIDEARCHITECTURE/TC_ITS_WG5_CADZOW_StandardizationActivities.pdf
23. Opinion of the European Data Protection Supervision on an Action Plan for the Deployment of Intelligent Transport Systems in Europe. Official Journal of the European Union (February 25, 2010), http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf
24. Schoenberger, H.: 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 17, 1526–1529 (2009)
25. Wright, D., de Hert, P. (eds.): Privacy Impact Assessment. Series: Law, Governance and Technology Series, vol. 6. Springer (2012)
26. Spiekermann, S., Cranor, L.: Privacy Engineering. IEEE Transactions on Software Engineering 35(1), 67–82 (2009)
27. Gürses, S.F., Troncoso, C., Diaz, C.: Engineering Privacy-by-Design. Computers, Privacy & Data Protection (2011)
28. Access control based on Bell-La Padula model, http://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model
29. Guidelines for Privacy Aware Cooperative Application. PRECIOSA Project Deliverable 11 (November 2010), http://www.preciosa-project.org/
30. Balasch, J., Rial, A., Troncoso, C., Geuens, C., Preneel, B., Verbauwhede, I.: PrETP: Privacy-Preserving Electronic Toll Pricing (extended version). In: 19th USENIX Security Symposium
31. Kursawe, K., Danezis, G., Kohlweiss, M.: Privacy-Friendly Aggregation for the Smart-Grid. In: Fischer-Hübner, S., Hopper, N. (eds.) PETS 2011. LNCS, vol. 6794, pp. 175–191. Springer, Heidelberg (2011)
32. Acs, G., Castelluccia, C.: I have a DREAM (DiffeRentially privatE smArt Metering). In: The 13th Information Hiding Conference (IH) (2011)
33. Stanford Center for Internet and Society PET Wiki, http://cyberlaw.stanford.edu/wiki/index.php/PET