SALT Frameworks to Tackle Surveillance and Privacy Concerns

Antonio Kung, Christophe Jouvray and Fanny Coudert
Trialog, Paris, France

Keywords: PET (Privacy Enhancing Technology), AET (Accountability Enhancing Technology), SALT (Socio-Contextual, ethicAL, Legal, Technical) Framework, Privacy-by-Design, SFMT (SALT Framework Management Tool).

Abstract: This paper elaborates on the need to take into account the different views of the stakeholders involved in the development of surveillance systems and civil society, during the design process. It first provides an overview on privacy-by-design approaches. It then identifies three principles essential to integrate privacy concerns into the design of surveillance systems. It consequently proposes a design process based on social-contextual, ethical, legal and technical frameworks (SALT) and the challenges for its creation and use. It finally provides a specification of a resulting SALT framework management tool based on modelling techniques.

1 INTRODUCTION

Surveillance and Privacy are critical societal issues today. In the wake of the Edward Snowden's revelations (http://en.wikipedia.org/wiki/Edward_Snowden), several law proposals flourished in the US Congress to increase the transparency and accountability of the use by the government of its surveillance powers (Electronic Frontier Foundation, 2013). Similarly in Europe, on 8 April 2014, the European Court of Justice annulled the Data Retention Directive that was imposing to Internet Service Providers an obligation to retain all traffic and location data generated by their communication networks for purposes of investigation, detection and prosecution of serious crime. One of the arguments advanced by the Court is that such blanket data retention obligation is likely to generate in the minds of the persons concerned the feeling that their private lives are subject of constant surveillance (CJEU, 2014). These examples show that surveillance and privacy are issues that, in a democratic society, go hand in hand and must be solved jointly. One way to do so is through *Privacy-by-Design*, a concept that is turned into a legal obligation for the development of new information systems in the Data Protection Package proposed by the European Commission in January 2012 (Reform of the Data Protection Package, http://ec.europa.eu/justice/data-protection/review/index_en.htm).

This paper elaborates on the need to develop an adequate framework for the implementation of *Privacy-by-Design* in the development of surveillance technologies and systems.

2 TODAY'S PRACTICE OF PRIVACY-BY-DESIGN

One of the big hopes in solving privacy issues stemming from the development of new technologies is the concept of *Privacy-by-Design*, a term coined by Ann Cavoukian (Privacy-by-Design, http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/). Applied to the design of *Information and Communication Technologies* (ICT) based applications, Privacy-by-Design (PbD) focuses on requirements and measures that take into account the respect of the individuals' privacy. The full integration of PbD in today applications, systems and development process is being worked out both on the management front and the engineering front. At the management level PbD is often associated with Privacy Impact Assessments (PIAs) (Wright and Hert, 20102). A PIA is defined as *a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects* (PIAF, http://www.piafproject.eu).

Kung A., Jouvray C. and Coudert F..
SALT Frameworks to Tackle Surveillance and Privacy Concerns.
DOI: 10.5220/0005444306650673
In *Proceedings of the 3rd International Conference on Model-Driven Engineering and Software Development* (SPIE-2015), pages 665-673
ISBN: 978-989-758-083-3

At the engineering level, principles discussed in (Spiekermann and Cranor, 2009); (Gürses et al., 2011); (Kung et al., 2011) are used as an input to the PRIPARE FP7 project to define a comprehensive methodology (http://pripare.eu/).

Standardisation activities are also on-going. Within ISO (ISO/IEC JTC1/SC27: http://www.jtc1sc27.din.de), standards are being prepared on PIAs[1], and on a code of practice for personally identifiable information protection[2]. Within OASIS (https://www.oasis-open.org/), two standards are available, PMRM (Privacy Management Reference Model and Methodology) (OASIS, https://www.oasis-open.org/committees/pmrm/charter.php), which explains how privacy principles are mapped onto operational requirements (e.g. agreement, security, access) and PdB-SE (Privacy by Design Documentation for Software Engineers) (OASIS, https://www.oasis-open.org/committees/pbd-se/charter.php), the goal of which is to provide privacy governance and documentation standards to software engineers. Finally, the European Commission is in the process of issuing a mandate for the establishment of European standards on PbD (http://ec.europa.eu/DocsRoom/documents/5290).

The question is, how can we support PbD in the design of a surveillance system? Is it sufficient to rely on generic PbD approaches? Do we need specific features? Do we need standardisation? The next section lists three principles that are needed in a design process integrating PbD.

3 PRINCIPLES FOR PBD FOR SURVEILLANCE

3.1 Multi-stakeholder Empowerment

The deployment of a typical surveillance system usually involves a number of stakeholders. *An authority stakeholder* (often public) would decide on the deployment of a surveillance system. *A surveillance system owner* would be responsible to deploy and operate the system. *A surveillance system designer* would be mandated to design the surveillance system.

As more sophisticated surveillance capability will be available in the future, and with the rising concerns about privacy, additional stakeholders are likely to gain influence in the deployment of surveillance systems. Compliance of the system with the legal framework will not only be subject to the scrutiny of data protection authorities but also internally to the one of data protection officers and externally to third parties certifiers/auditors. Beyond legal compliance, *public opinion* will also have to be taken into account as it conditions the public acceptance of the surveillance. Public opinion is usually voiced either indirectly by *privacy advocates* (e.g. *privacy associations*, or *privacy activists)* or directly expressed on the internet (e.g. on social networks) or through specific channels opened for engaging a dialogue with civil society (e.g. meetings with the affected community of citizens). Ethical aspects of surveillance should be given more weight to solve the most difficult issues not resolved by the legal framework.

Furthermore, the rapid evolution of technology and its profound societal impact implies that technology makers and social sciences analysts will also have a strong influence. At the technology level more sophisticated privacy enhancing technology (often called PETs) will be available, but likewise more sophisticated surveillance technology will also be available.

It follows that various forces will decide on the fate and shape of a resulting surveillance system. Such forces can be structured into three viewpoints: (1) the socio-contextual ethical viewpoint, (2) the legal viewpoint and (3) the technology viewpoint. The PARIS project (PARIS, http://www.paris-project.org/) has coined the term SALT or Socio-contextual ethicAl Legal Technical to qualify the framework.

The resulting principle is *multi-stakeholders' empowerment*, i.e. each viewpoint should be entirely taken into account in the design process.

3.2 Concerted Impact Assessment

As mentioned above, a Privacy Impact Assessment or PIA (Wright and Hert, 2012); (PIAF, http://www.piafproject.eu/) is a *process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects*. A risk analysis is carried out and if resulting privacy risks are beyond some level, measures are identified and implemented to eliminate or minimise those risks. For instance (CNIL, http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf) is a privacy risk analysis that is promoted by the French data protection authority.

Likewise, it is through an assessment of the

[1] ISO 29134
[2] ISO 29151

security risks that may exist in a given area that recommendations for surveillance measures may be taken. We could say that a security impact assessment is carried out. It identifies the impact that no measures would have on the security of the given area (security of the elements that are in the area, e.g. citizens, assets) and consequently sets out the appropriate surveillance recommendations to prevent crimes and terrorism.

Both privacy and security risks analysis should be made in a concerted way. It is well known that while surveillance measures have a negative impact on privacy, privacy measures may decrease the efficiency of surveillance measures. The only solution so far is to carry out a proportionality assessment in which the need and efficiency of the claimed surveillance measures (potential benefit) is weighted against their impact on privacy (negative impact). In other words, the surveillance and the privacy impact assessments are carried out jointly. The resulting principle is *concerted impact assessment*.

3.3 Trust through Accountability Measures

The impact on citizens' privacy of surveillance measures that look for collecting comprehensive information about potential criminals or terrorists is not being discussed. Yet, citizens are willing to give up part of their privacy to ensure a reasonable level of security. A sufficient level of trust is therefore needed between citizens and stakeholders in charge of performing surveillance duties, i.e. in the fact that the latter act within the powers granted to them. One way to create trust is to establish sufficient transparency and accountability. An overview of the actions made by today civil society organisations to monitor surveillance systems is provided by (Surveillance, http://irissproject.eu).

Beyond regulation, transparency and accountability can be made easier if accountability-by-design is applied, i.e. accountability is a requirement from the start and accountability enhancing technology (AET) are used. Examples of such technology are secure access logs, i.e. technology that ensures that all access to data are securely logged in such a way that it can be used for accountability, e.g. for later judicial actions. Four design attributes are defined in (Kung, 2014) that are important in a privacy preserving system: minimization of data, enforcement of data protection policies, accountability and flexibility (to improve the system). (Kung, 2014) also lists examples of technology used for each attributes. Three types of measures are associated with accountability: log data access, log modifications (policies, level of protection), and protect log data. With this type of technology, data transmitted for surveillance purpose to external parties but also internally would be logged.

The resulting principle is *trust through accountability measures*, i.e. all surveillance actions are associated with measures that would later be used either to prove that no privacy infringing actions have been carried out, or to prove that a privacy breach has happened.

4 A DESIGN PROCESS BASED ON SALT FRAMEWORKS

Figure 1 describes the resulting design process based on the above principles. It consists of three components: a common reference or framework that will be used by the stakeholders involved in the process; the design process itself; the designed system.

The common reference acts as a dedicated repository of knowledge dedicated to a given environment. This could be a geo-political subdivision (e.g. city, a region, a country). It combines information and knowledge concerning several references, the Socio-contextual and ethicAl reference, the Legal reference, and the Technical reference. This is the reason why it is designated as a *SALT framework*. The socio-contextual and ethical reference contains parameters that are specific to a region (e.g. France), and types of interactions (e.g. at home, at work). The legal reference would relate to a country's legislation (e.g. Spain) or a given technology (e.g. video surveillance). The technical reference includes the wealth of available technologies and practices. This would include privacy enhancing technology (PET) and associated practices. In the case of surveillance systems it would further involve surveillance technology, accountability enhancing technology (AET) and associated practices.

The design process uses the common reference to drive the design of a surveillance system design that applies privacy-by-design principles as well as accountability-by-design principles. Using the common reference provides the assurance that all the needed obligations, advised practices and technology solutions are considered and integrated. This is why it is called SALT design process.

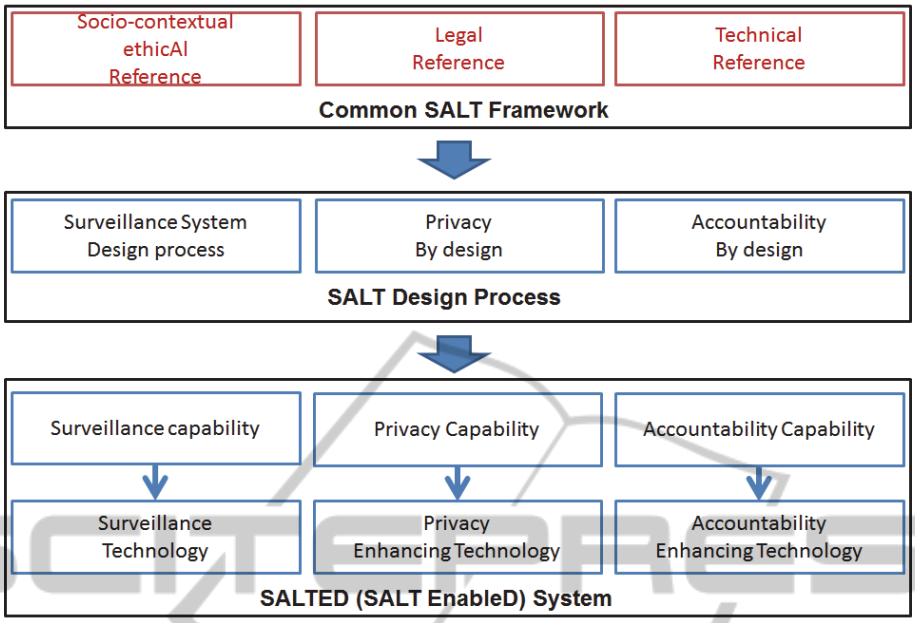

Figure 1: SALT Design Process.

Once the design process has been applied, a system is designed with privacy preservation and accountability features. This is why it is called SALT enabled or SALTED system. More information can be found in (Deliverable D2.2, http://www.paris-project.org/index.php/delivera-bles).

5 SALT FRAMEWORK CHALLENGES

There are several challenges in the use of SALT framework that must be addressed: the capture of knowledge; the need for different references; the usage of a SALT framework; and the management of a SALT framework. We briefly explain these challenges and how we address them.

5.1 SALT Framework Knowledge Capture Challenge

While the concept of a SALT framework is powerful, it is only valid if the resulting repository is comprehensive (i.e. all needed information is stored), accurate (i.e. it reflects the knowledge of the expert stakeholders) and flexible (i.e. if must cope with specific information and allow for evolution). Further, a SALT framework must be structured in order to cope with the multidisciplinary needs. Different viewpoints will be needed. For instance a stakeholder with a legal interest will need very precise access to legal references and a high level access to technical references. Likewise, engineers will need very precise technical references and high level access to legal references. The challenge is to structure information to provide different viewpoints while remaining consistent (e.g. high level views are consistent with detailed views). Another challenge is to cope with terminology issues. Lawyers would be at a loss if they were exposed to engineering phraseology, and the same would apply to engineers reading legal text.

5.2 Multiple SALT Frameworks Challenge

There can be many SALT frameworks. A surveillance system designed in France would have to follow the obligations set out by the French legal framework and the recommendations of public bodies such as the CNIL, the French Data Protection Authority (http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/declaration-videosurveillance/), while a CCTV camera installed in the UK would have to follow the UK legal framework and the recommendation of ICO, the UK Data Protection Authority (https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/). Such obligations would be part of a national common reference created for use in France and UK respectively. In practice there

could be many socio-contextual and ethical as well as legal references. While technology references could be common, it is likely that variations will exist as some technologies could be more important in some contexts (e.g accountability features would be important in Europe).

Further SALT frameworks could also include proprietary reference information. The position taken by PARIS is that the success of a SALT framework depends on the success of a multidisciplinary practice ecosystem. Several scenarios are possible. One of them could be the following: a public authority in a country decides to build a SALT framework and require surveillance system designers to use it. Surveillance system designers would use it as the starting public point, possibly enriching it with their corporate extended references. These extensions might not have to be made public for competitive advantages reasons.

5.3 SALT Framework Usage Challenge

One of the challenges of this whole design process is to agree on the way a SALT framework would be used and its value. Many discussions took place in the PARIS project on this issue with some stakeholders being concerned that relevant design decisions would be taken automatically, while other stakeholders being concerned that maximum automation would be needed to cope with error prone aspects. The following was decided in the PARIS project: interactions between a designer and SALT frameworks would be based on two interactions paradigms, the browsing paradigm and the questionnaire paradigm. Browsing would be convenient when the designer knows the items it wishes to browse. For instance, (s)he could look for a particular set of PETs, AETs or surveillance technology. Browsing would have less interest in the early stages of a SALT framework, i.e. when not many references have been stored, or when designers are not yet familiar with the design process. By contrast, Questionnaires would be more useful at that stage because they would provide guidance of complex design aspects or just when designers are not yet familiar. They would become cumbersome and tedious when used repeatedly, so they should have several structures, one with sequential access when users are not familiar with the content and one with direct access when users are already familiar with the questionnaire. Consequently, the structure of a questionnaire is important, and it must be easy to change. In other words, knowledge on a questionnaire structure is an integral part of a SALT framework.

5.4 SALT Framework Management Challenge

The management of a SALT framework is an underestimated challenge. This is because the initial version of a repository is most often created by the very same researchers and engineers who design the repository itself. They can do it easily and they focus on the implementation of the repository not on its content. There are two problems to tackle. First, editing and adding content to the SALT framework must be a mainstream activity based on quality production tools. Secondly, the governance of the SALT framework content must be addressed. How do we decide that some information can be integrated in a framework? Here are two examples of problematic governance schemes: an approach where every contribution is accepted could easily lead to a vast amount of reference information that are hard to use; an approach where each reference is duly validated and certified would create a bottleneck as the time it would take to create an entry in a framework could be too long. The PARIS project has decided to address these challenges by developing a specific editing tool. The requirements for such tool are listed in the next section. The governance of reference context would be based on transparent peer reviews. For instance, the creation of a technology entry concerning a PET would be provided by expert A and reviewed by experts B, C and D.

6 SALT FRAMEWORK TOOLS REQUIREMENTS

In order to address such requirements, a number of use cases were defined (see (Deliverable D2.2, http://www.paris-project.org/index.php/deliverables) for some examples). They broadly showed two types of requirements, those that will be useful to experts in charge of creating and maintaining a SALT framework, and those that will be useful to experts designing privacy preserving surveillance systems. We consequently need to manage two types of tools: tools for SALT Framework experts and tools for surveillance systems designers. We cover them in sequence.

6.1 Requirements for SALT Framework Experts

The requirements are threefold: *reference management, terminology management and questionnaire management.*

Reference management allows for the creation, editing, rating and version management of references, reference structures and viewpoints. If a SALT framework expert wishes to include a reference to the European legislation, (s)he includes a reference in the form of an abstract, a historical context, and a PDF file containing the text of the European legislation. (S)He also amends the existing questionnaires to take into account the new legislation. The abstract is later amended with an additional comment highlighting a specific aspect of the questionnaire. The link from the questionnaire to the comment is also integrated in the framework. In order to ensure increasingly better questionnaires, rating of questionnaires is also supported, at two levels: by peer experts and by users (i.e. designers of surveillance systems based on the SALT framework).

Terminology management allows for the creation, edition, rating and version management of taxonomy and terms. It would enable consistent use in questionnaires. An example of feature could be equivalence of terms and subclass dependency, i.e. a questionnaire can use a synonym or a refined term. A change in a terminology would trigger detection of changes in questionnaires (and possibly edition of the questionnaires). It would also trigger version management, i.e. it would be possible to run the amended part of the questionnaire only. If a technology expert creates a taxonomy on surveillance technologies, (s)he uses the SALT framework edition tool to store the taxonomy. The result is subsequently used by further experts to store entries on surveillance technologies. Some years later when hundreds of surveillance technologies have been stored, a new class of surveillance technology imposes a change in the taxonomy. The initial expert wishes to change the taxonomy, without compromising the already entered entries. For instance socio-contextual, ethical, legal and technology experts have combined their knowledge to design one or several questionnaires. The questionnaires structures are also stored in the framework. The questionnaires consist of free text carefully crafted by the experts, except that surveillance technologies terminology is based on the taxonomy. The result of changing the surveillance taxonomy has an impact on the questionnaire. But the expert is presented with the options of changing automatically the questionnaire (when term A is just replaced by term B), or of being displayed individual occurrences (when term A is replaced by two other terms).

Questionnaire management allows for the creation, edition, rating and version management of questionnaires. A question could be changed, refined into several questions. The sequence of questions could be changed, and dependencies between highlighted could be annotated. A change in a questionnaire would trigger version management, i.e. it would be possible to run the amended part of the questionnaire only. The third example focuses on the structure of questionnaires: a SALT framework expert creates a questionnaire which is used by designers of specific surveillance systems based on biometric systems in country A. The questionnaire is used during six months by an initially small number of designers. Feedback is used by SALT framework to improve the questionnaire. The sequencing of some questions are changed. Some questions are refined into more precise questions. The questionnaire is then used satisfactorily during a couple of years until some new regulation procedures are put in place. The questionnaire is changed accordingly with the expert determining the list of previous questions that need not be answered. A version management capability allows for the generation of two types of sessions, a new design session when the new questionnaire is entirely run, and a redesign session when designed systems using the previous questionnaire must be verified.

6.2 Requirements for Designers

Here the requirements are twofold: *Design management and Governance management.* We illustrate them through two examples of scenarios involving surveillance system designers using a questionnaire in a SALT framework.

Design management allows for the management of design sessions with design options. Flexible access, e.g. direct access to questionnaires is possible (e.g. direct access to a question). Access to previous designs is also possible to help for reuse. It also allows for the generation of design documentation (e.g. a PIA document). The designer creates a design session and runs the various questionnaires prepared in the SALT framework. He selects some parameters providing indication on the size of the system being designed. He knows that the entire design lifecycle will take several months. Consequently he creates a design session that

contains incomplete and sometimes preliminary answers to questions. Initially he is not familiar with the questionnaire structure but he is provided with a high-level structure presentation of the questionnaire that he can easily match with its system design process. Later he is familiar with the questionnaire structure and uses direct access to specific questions. He can also consider different design options and weigh their privacy impact, i.e. the questionnaire session manager can handle several options in parallel.

Governance management allows the qualification of answers and the involvement of the whole design teams (including lawyers, privacy managers, managers, designers) when some decisions need more governance. It also allows for the access to a design dashboard and the creation of a logbook including in particular accountability statements. The second example focuses on the use of the tool to validate and review a designer's decision: designers can qualify their answer according to their design certainty (e.g. designer has committed to an answer and can justify it, designer has several design options that is he is analysing, designer needs further discussions with other stakeholders in his organisation). He is provided with a design dashboard allowing him to see the design status. His design is also accessible by the corporate members involved in design and its validation. At the end of his analysis he is left with two design options which need management review. Managers access the design session and make a decision. The rationale for the decision is stored and kept for traceability and accountability.

6.3 A Tooling Approach based on Model-Driven Engineering Techniques

An initial set of tool requirements for SALT framework experts was defined in (Deliverable D3.1, http://www.paris-project.org/index.php/deli-verables). The tool, called SALT framework management tool (SFMT), relies on the use of models and model driven engineering techniques (http://en.wikipedia.org/wiki/Model-driven_enginee-ring), an approach at the forefront of software engineering. The main benefit of model driven engineering is that it allows for the modelling of any type of knowledge, its representation into suitable digital form, and the subsequent provision of associated tools. Here is one example: geographic maps designed with model driven engineering techniques would consist of *meta-models* and *models*. Meta-models would describe a map structure (e.g. roads, lights), include properties (e.g. one way road, toll, speed limit), and constraints (e.g. a temporary construction will block the road). The meta-model would then be instantiated into a model with a set of data concerning e.g. Belgium. A driver could then use a navigation tool that gets updated with dynamic information such as temporary road constructions, traffic jams and so forth.

SFMT is structured around the need to support four phases: the *SALT knowledge capture phase*, when experts enter in a SALT knowledge repository references, terminology, questionnaires; the *SALT knowledge analysis and representation*, when specific knowledge on references, terminology and questionnaires are selected to be represented as models; the *SALT knowledge repository phase*, when the knowledge is stored; the *SALT knowledge application phase*, when specific tools are created for use by surveillance systems designers. Figure 2 depicts the four phases.

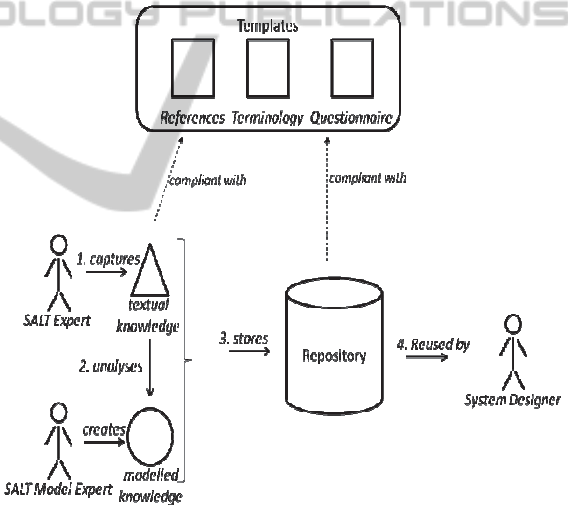

Figure 2: SALT Knowledge Process.

6.4 Models Needed to Support SALT Framework Experts

Many discussions took place in the PARIS project to identify which type of knowledge needed to be modelled. It was agreed that modelling techniques should not be used to systematically capture the semantics of referenced information (e.g. a legal text). Rather they would be useful to capture the semantics of structures for multidisciplinary practice. Consequently, models have been identified for the following needs: Concerning reference management, *reference viewpoint structures* will

provide viewpoint models for each type of stakeholder (e.g. the technology viewpoint for a legal reference is an adapted abstract associated with the reference). Concerning terminology management, *taxonomies* will provide dependency models that can be used to create flexible questionnaires. Concerning questionnaire management, *questionnaires' structure* will provide question grouping and sequencing capability. *Relationships between references, taxonomy and questionnaires* will provide consistency in a questionnaire with references and terminology.

PARIS also anticipates that other types of knowledge could be modelled, for instance related to technical considerations leading to decisions on PETs. Those additional models, and associated engineering tools can easily be added in the future to a SALT framework repository already based on models.

6.5 Towards Models Checking

One of the potential benefit of models to represent SALT framework knowledge is model checking. For instance SALT modelled references would be compliant to a specific format with metadata added concerning authors, date, or purpose. Constraints written with a specific language called Object Constraint Language (OCL) could then be added, for instance on data retention for a video camera.

PARIS has developed a specific tool called PAERIS (Deliverable D4.3, http://paris-project.org/index.php/deliverables) which checks that constraints are valid in a developed surveillance system model (figure 3)

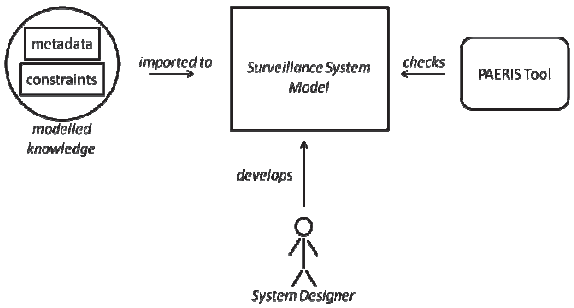

Figure 3: Model Checking for Surveillance System Design.

7 CONCLUSIONS

This paper has presented the approach proposed in the PARIS project to integrate surveillance and privacy issues into a privacy-by-design process, based on the use of the concept of SALT frameworks and an associated SALT Framework Management Tool (SFMT). The PARIS project is currently implementing a SFMT and applying it to two use cases, a video surveillance lifecycle management use case (Deliverable D5.1, http://www.paris-project.org/index.php/deliverables) and a biometric surveillance use case (Deliverable D6.1, http://www.paris-project.org/index.php/deliverables). It is also implementing a prototype model checking verification tool, PAERIS.

This article has shown that in the field of surveillance, the PbD process should give specific weight to multi-stakeholders empowerment, to mechanisms that enable to carry out the proportionality assessment (such as concerted impact assessment) and finally to accountability and transparency tools. The SALT framework developed within the PARIS project builds on these three pillars. It has also been shown that while the PbD process can rely on general principles, it is paramount to specify these principles to the dedicated environment to which they should be applied. Finally, it is too soon to assess the need for specific features or standards, as this will depend on the needs of the SALT framework ecosystem.

ACKNOWLEDGEMENTS

This paper was made possible thanks to the funding and work performed for the PARIS project (PrivAcy pReserving Infrastructure for Surveillance). This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312504. We would also like to thank Ann Cavoukian who suggested the use of the term *contextual* in the SALT acronym.

REFERENCES

http://en.wikipedia.org/wiki/Edward_Snowden.

See for an overview, Electronic Frontier Foundation, EFF's Cheat Sheet to Congress' NSA Spying Bills, https://www.eff.org/fr/deeplinks/2013/08/effs-cheat, 11 September 2013.

CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and

Others. Judgment (Grand Chamber) of 8 April 2014, §37, http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

Reform of the Data Protection Package, http://ec.europa.eu/justice/data-protection/review/index_en.htm.

Privacy-by-Design. http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/

Wright, David; de Hert, Paul (Eds.). *Privacy Impact Assessment*. Series: Law, Governance and Technology Series, Vol. 6, Springer. 2012.

PIAF: Privacy Impact Assessment Framework. http://www.piafproject.eu.

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

S. F. Gürses, C. Troncoso, and C. Diaz. *Engineering Privacy-by-Design*. Computers, Privacy & Data Protection, 2011.

A.Kung, J.Freytag, F.Kargl. *Privacy-by-design in ITS applications*. 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, June 20, 2011, Lucca, Italy.

http://pripare.eu/

ISO/IEC JTC1/SC27: http://www.jtc1sc27.din.de.

OASIS. Organization for the Advancement of Structured Information. https://www.oasis-open.org/

OASIS Privacy Management Reference Model (PMRM) Technical Committee. https://www.oasis-open.org/committees/pmrm/charter.php.

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) Technical Committee. https://www.oasis-open.org/committees/pbd-se/charter.php.

http://ec.europa.eu/DocsRoom/documents/5290.

PARIS: PrivAcy pReserving Infrastructure for Surveillance. http://www.paris-project.org/

CNIL methodology for privacy risk management. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf.

Surveillance, fighting crime and violence. Deliverable D1.1, IRISS Project. February 2012. http://irissproject.eu.

Antonio Kung. *PEARs: Privacy Enhancing ARchitectures*. Annual Privacy Forum, May 21-22, 2014, Athens, Greece. Proceedings APF14 "Privacy Technologies and Policy". Springer Verlag.

Deliverable D2.2 Structure and Dynamics of SALT Frameworks http://www.paris-project.org/index.php/deliverables.

http://en.wikipedia.org/wiki/Architectural_pattern.

http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/declaration-videosurveillance/

https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

Deliverable D3.1 SALT Framework Management Tool Requirements http://www.paris-project.org/index.php/deliverables.

http://en.wikipedia.org/wiki/Model-driven_engineering.

Deliverable D5.1 Video Surveillance Lifecycle Management Use Case Description http://www.paris-project.org/index.php/deliverables.

Deliverable D6.1 Biometrics Use Case Description http://www.paris-project.org/index.php/deliverables.

Deliverable D4.3 SALT Compliant Processes Guidelines for Use Cases - http://paris-project.org/index.php/deliverables.