INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Team LICIT

Legal Issues in Communication and Information Technologies

Grenoble - Rhône-Alpes

Theme : knowledge-and-data-representation-and-management

Table of contents

1. Team

Research Scientist

Daniel Le Métayer [Team Leader, Senior Researcher, INRIA, HdR]

PhD Students

Sophie Guicherd [with University Pierre Mendès-France]
Eduardo Mazza [with VERIMAG]

Post-Doctoral Fellows

Julien Le Clainche [to July 2010]
Manuel Maarek [to September 2010]
Guillaume Piolle [to August 2010]
Romuald Thion [to August 2010]

Administrative Assistants

Elisabeth Borel [to July 2010]
Françoise De Coninck [since September 2010]

2. Overall Objectives

2.1. Introduction

The main objective of LICIT is to undertake new research activities on the interactions between ICT and the law. The motivations for this new initiative are manifold. First and foremost, the rapid evolution of the technological landscape and the impact of ICT on the everyday life of citizens (including their private lives) raise new challenges which cannot be tackled by a purely technological approach [26]. For example, the protection of privacy rights on the Internet or in pervasive computing environments is by definition multidimensional and requires expertise from disciplines such as social sciences, economics, ethics, law and computer science [28]. Other examples of the ever-growing intermingling of ICT and law include electronic commerce, digital rights management (DRM), social networks, forensics, cybercrime, e-government, and e-justice. As far as research is concerned however, there are still very few links between the ICT and law communities. This situation is unfortunate considering the importance of the interests (both societal and economical) at stake. In addition, at a time of growing mistrust of citizens towards technology, more attention should be paid to the implications of research results on society.

Starting from this observation, the goal of LICIT is to contribute, in partnership with research groups in law, to the development of new approaches and methods for a better integration of technical and legal instruments.

In practice, the interactions between ICT and law take various forms and go in both directions [23]:

- The ICT "objects" are, as any other objects, "objects of law": on one hand, there is no reason why new technologies and services should escape the realm of law; on the other hand, it may be the case that existing regulations need to be adapted to take into account the advent of new, unforeseen technological developments (e.g. certain provisions of privacy regulations become inapplicable in a pervasive computing context, intellectual property laws are challenged by the new distribution modes of electronic contents). Understanding precisely when this is the case and how regulations should evolve to cope with the new reality may be a complex "technico-legal" issue with potential impacts on both disciplines.
- ICT can also provide new enforcement mechanisms and tools for the benefit of the law. For example, DRM technologies are supposed to "implement" legal provisions and contractual commitments, Privacy Enhancing Technologies (PET) help reduce privacy threats, certified tools can be provided to support electronic signature, computer logs can be used as evidence in courts, etc. At a different level, data mining or knowledge management systems can be applied to the extraction of relevant legal cases or the formalization of legal reasoning.

Generally speaking, legal and technical means should complement each other to reduce risks and to increase citizens' and consumers' trust in ICT: on one side, laws (or contracts) can provide assurances which are out of reach of technical means (or cope with situations where technical means would be defeated); on the other side, technology can help enforce legal and contractual commitments. This synergy should not be taken for granted however, and if legal issues (and more generally, the consequences of the technologies on society) are not considered from the outset, technological decisions made during the design phase may very well hamper or make impossible the enforcement of legal rights.

In the longer term, further thought needs to be devoted to the potential conflicts between, on one side, rapidly evolving technologies and, on the other side, bodies of regulations which, in essence and for the sake of "legal security", require a form of stability. This complex issue is related to the problem of finding the right level of abstraction in regulations - or strike the right balance between very general principles (which remain stable but offer little indication as far as practical application is concerned, and can thus lead to another form of legal insecurity) and precise provisions whose application may be less prone to interpretation but are bound to become quickly outdated.

The means used by LICIT to reach its objectives are twofold:

1. Research actions: to investigate specific research topics following an interdisciplinary approach in order to better integrate legal and technical instruments. This research work emphasizes the use of formal methods as a link between the ICT and regulations.
2. Networking actions: to favour the emergence of an "ICT and law" research community and to enhance the interest of ICT researchers in this emerging field.

The outputs of the first line of actions are research results whereas the networking actions take the form of joint events (seminars, conferences), joint projects and position papers.

2.2. Highlights of the year

The main results of the year concern both the aforementioned research and networking objectives:

- Definition of a formal framework for the specification of liability in software systems [12].
- Definition of formal criteria to design and evaluate log architectures for legal evidence [13].
- Co-organization of the conference on legal issues in software contracts and the impact of cloud computing and free software (Paris, 3 December)[1]. This conference, which was organized in the context of the LISE project, has attracted more than 200 participants.
- Co-organization of the CPDP Conference and panel on "the right to be forgotten"[2]. CPDP, which is now established as the main privacy conference in Europe, attracts every year a wider and more multidisciplinary audience (more than 200 participants in 2010).
- Co-organization of the first national workshop on privacy protection APVP 2010 (Annecy, 26-27 May 2010) [3].

Central to the research themes of LICIT, we have also edited a volume of collected work on "ICT and law: opportunities, challenges and limitations" [20] published by Bruylant this year.

3. Scientific Foundations

3.1. Context

[1] http://juriscom.net/actu/visu.php?ID=1263
[2] http://www.cpdpconferences.org
[3] http://licit.inrialpes.fr/apvp2010/

As set forth in Section 2.1, LICIT is by nature not only interdisciplinary but also transversal in the sense that a wide variety of computer science areas are potentially relevant to its activities (including security, formal methods, verification, automated reasoning, natural language processing, software engineering). Encompassing this variety of competences within the team itself is obviously out of reach: the approach followed in LICIT is rather to establish partnerships with research groups (in ICT and law) providing complementary backgrounds in order to ensure that the highest level of expertise is available to reach its objectives. As far as the legal background is concerned, the most relevant domains are individual rights (privacy right, personal data protection, free speech, etc.), contract law, legal evidence, intellectual property and legistics.

In this section, we focus on the computer science area which plays a central role in LICIT, namely formal methods, which serve as a link between ICT and law. We explain its significance in the context of LICIT in the first subsection before outlining the relevant techniques in the second subsection.

3.2. Formal methods as a link between ICT and law

Beyond their many differences, ICT and law share a strong emphasis on formalism. This commonality is not without reason: in both cases formalism is a way to avoid ambiguity and to provide the required level of rigour, transparency, and security. As an illustration, L. Fuller in his book "The morality of law" [22] puts forward the following distinctive features of a legal system: (1) set of rules (2) without contradiction (3) understandable (4) applicable (5) predictable (6) publicized and (7) legitimate. Even though they were obviously not proposed with such a comparison in mind, it is interesting to note that, among these features, the first five are also often used in computer science to characterize a good software specification.

As far as software is concerned, the fact that both disciplines refer to the word "code" is not insignificant and the explorations of the commonalities can be very fruitful (and not only from a theoretical perspective). Indeed, there are many situations where the frontier between the two notions seems to be blurring[4]. Just to take a few examples:

- Software contracts typically incorporate references to technical requirements or specifications which can be used, for example, to decide upon acceptance of the software by the customer or validity of an error correction request. In case of litigation, such specifications can also be used by the judges since they form part of the contract executed by the parties. In this perspective, the contract can thus be seen as an extension of the technical specification including further requirements such as use rights, delivery schedule, warranty, and liability.
- Several languages have been proposed to express privacy policies (e.g. P3P by the W3C Consortium and EPAL by IBM); they are used by some commercial sites and can be handled by popular browsers such as Mozilla Firefox or Internet Explorer. The policies published by these sites can be used both by software code - checked by browsers or enforced by Privacy Enhancing Technologies (PET) - and by judges, possibly interpreting them as commitments on the privacy policy of the company.
- The DRM technologies are supposed to implement legal provisions and contractual commitments about the use of digital content such as music or video.
- More and more transactions are performed on the basis of electronic contracts (SLA: Service Level Agreements for Web and grid services, electronic software licenses, e-commerce contracts, etc.).

In fact, the convergence has developed so much that legal experts have expressed worries that "machine code" might more and more frequently replace "legal code", with detrimental effects on consumers. This topic has stirred up a series of discussions and publications in the legal community [24], [25], [27] and is bound to remain active for quite a long time. Indeed, the implementation of contractual commitments by computer code raises a number of issues such as the lack of flexibility of automated tools, the potential inconsistency between computer code and legal code, the potential errors or flaws in computer code itself or the respective roles of human beings and computers in the process.

[4] Lawrence Lessig refers to East Coast Code and West Coast Code to denote respectively law and software code [25]

The position taken in LICIT is that the first step for a fruitful and useful exploration of the relationships between legal and software code is the definition of a formal framework for expressing the notions at hand, understanding them without ambiguity, and eventually relating or combining them.

3.3. Relevant techniques

The formal methods relevant to LICIT include (1) specification methods and (2) validation methods.

1. Specifications are models or abstract representations of IT systems and their properties which can be used to define their expected behaviour without ambiguity. Specifications can also serve as a basis for various kinds of analyses and tools such as consistency analysis, validation, evaluation, certification, and animation. Specifications can play a role at different phases of the life cycle of a system : before, during or after its design and development. Different specification frameworks have been proposed, which can be roughly classified into semi-formal methods and formal methods. Semi-formal methods provide a well-defined syntax for the models (or "views" of the models) while the underlying semantics remain informal; in contrast, formal methods rely on a mathematical framework which is used to define the semantics of the models. The benefit of semi-formal methods is the definition of a shared body of notions, presentation rules and graphical tools which improve the communication and mutual understanding between the actors involved in the life-cycle of a system (designer, architect, development teams, evaluators, etc.). However, because of their lack of mathematical semantics, they do not necessarily guarantee the absence of ambiguity and they are not supported by formal verification tools. A standard example of semi-formal framework is UML. In contrast, formal methods such as Coq or B come with interactive theorem provers which help users verifying critical properties of their models. In addition, they provide ways to establish a formal link between a model and its implementation (through program extraction in Coq and refinement in B). Both formal and semi-formal methods are relevant to LICIT, especially specification techniques based on "execution traces" where the expected behaviour of a system is defined in terms of properties of its sequences of operations. As far as logical frameworks are concerned, temporal logics (which make it possible to express properties on the future or the past) and deontic logics (which involve obligation and permission operators) are of prime importance in specifying legal rules.
2. Validation consists in checking a system to ensure that it behaves as expected. The most ambitious validation methods involve a formal specification of the system (using one of the aforementioned formalisms) and a proof (usually interactive) that the actual implementation complies with the specification. An alternative approach is to use the formal specification to derive test suites in a systematic way based on well-defined coverage criteria. The validation can also consist of checking simpler properties (typically well-foundedness properties such as type correctness, absence of buffer overflow or implementation of specific security properties) using automatic tools: these tools are called "type checkers" when the properties to be checked are expressed as types and "program analysers" when they are defined in terms of abstract domains. The main benefit of this category of tools is their automation; their limitation is the restricted expressive power of their language of properties. For LICIT, *a posteriori* verifications are as relevant as *a priori* verifications: *a posteriori* checks are necessary when *a priori* verifications are either insufficient or not feasible, which is the case in particular for obligations which cannot be enforced by technical means.

To conclude this subsection, we stress the fact that the separations into categories (semi-formal versus formal, type inference versus program analysis, testing versus verification) have been used for the sake of the presentation (and because they originated from different research communities) but the frontiers between them tend to blur: for example certain frameworks include semi-formal and formal techniques, graphical representations such as state diagrams can be endowed with formal semantics, types can be defined in terms of abstract domains, program analysers can themselves be checked by theorem provers, etc.

4. Application Domains

4.1. Industrial applications

The application areas which are directly concerned by LICIT are varied, including

- Internet services, e-commerce, pervasive computing, cloud computing, profiling, behavioural targeting, location based services, smart cards...(especially w.r.t. liability and privacy protection)
- Software licensing, IT contracts (especially w.r.t. liability and intellectual property rights)
- Digital content (audio, video, information, etc.) distribution and protection, Digital Right Management (especially w.r.t. liability and intellectual property right protection)
- Forensics and cybercrime (especially w.r.t. liability and digital evidence)

4.2. Current industrial cooperations

The PERSOPOLIS project involves a collaboration with players of the smart card industry, including OCS (Oberthur Card Systems), TRUSTED LOGIC and CEV.

5. New Results

5.1. Liability issues in software engineering

Participants: Daniel Le Métayer, Manuel Maarek, Eduardo Mazza.

Software contracts usually include strong liability limitations or even exemptions of the providers for damages caused by their products. This situation does not favour the development of high quality software because software editors do not have sufficient economic incentives to apply stringent development and verification methods. Indeed, experience shows that products tend to be of higher quality and more secure when the actors in position to influence their development are also the actors bearing the liability for their defects. The usual argument to justify this lack of liability is the fact that software products are too complex and versatile objects whose expected features (and potential defects) cannot be characterised precisely, and which thus cannot be treated as traditional (tangible) goods. Taking up this challenge is one of our objectives : we study liability issues both from the legal and the technical points of view with the aim to put forward a formal framework to (1) define liability in a precise and unambiguous way and (2) establish such liability in case of incident.

Obviously, specifying all liabilities in a formal framework is neither possible nor desirable. Usually, the parties wish to express as precisely as possible certain aspects which are of prime importance for them and prefer to state other aspects less precisely (either because it is impossible to foresee at contracting time all the events that may occur or because they do not want to be bound by overly precise commitments). Taking this requirement into account, our architecture provides different levels of services which can be used by the parties depending on the economic stakes and the timing constraints for the drafting of the contract [12], [5]:

1. The first level is a systematic (but informal) definition of liabilities.
2. The second level is the formal definition of liabilities. This formal definition itself can be more or less detailed and encompasses only a part of the liability rules defined informally. In addition, it does not require a complete specification of the software but only the properties relevant for the targeted liability rules.
3. The third level is the implementation of a log infrastructure or the enhancement of existing logging facilities to ensure that all the information required to establish liabilities will be available if a claim is raised and will be trustable to be used as evidence for the case.
4. The fourth level is the implementation of a log analyser to assist human experts in the otherwise tedious and error-prone log inspection task.

Each level contributes to further reducing the uncertainties with respect to liabilities, and the parties can decide to choose the level commensurate with the risks involved with potential failures of the system.

In order to provide a precise characterization of liability, we have introduced a concept of "logical causality" [11]. Causality has been studied for a long time in computer science, but with quite different perspectives and goals. In the distributed systems community, causality is seen essentially as a temporal property. In [11], we have defined several variants of logical causality allowing us to express the fact that an event e_2 (e.g. a failure) would not have occurred if another event e_1 had not occurred ("necessary causality") or the fact that e_2 could not have been avoided as soon as e_1 had occurred ("sufficient causality"). We have shown that these causality properties are decidable and proposed trace analysis procedures to establish them.

As far as the log architecture is concerned, a key design choice is the distribution of the log files themselves. Indeed, recording log entries on a device controlled by an actor who may be involved in a claim for which this log would be used as evidence may not be acceptable for the other parties. In [13], we have introduced a framework for the specification of log architectures and proposed criteria to characterize "acceptable log architectures". These criteria depend on the functional architecture of the system itself and the potential claims between the parties. They can be used to check that a log architecture is appropriate for a given set of potential claims and to suggest improvements to derive an acceptable log architecture from a non-acceptable log architecture. On the formal side, we have shown that, for a given threat model, the logs produced by acceptable log architectures can be trusted as evidence for the determination of liabilities: technically speaking, any conclusive evaluation of a claim based on these logs produces the same verdict as the evaluation of the claim based on the sequence of real events.

As far as the log analysis itself is concerned, we have proposed a formal specification of the analyser using the B method in [15] and we have shown the correctness of an incremental analysis process. This result makes it possible to build on the output of a first analysis to improve it by considering additional logs or further properties.

The overall approach has been applied to several representative case studies: an electronic signature application on a mobile phone [5], [12], a distributed hotel booking service [13] and a cruise control system [11].

5.2. Privacy policies

Participants: Julien Le Clainche, Daniel Le Métayer, Guillaume Piolle, Romuald Thion.

Despite apparently strong legal protections, many citizens feel that information technologies have invaded so much of their lives that they no longer have suitable guarantees about their privacy. As a matter of fact, many aspects of new information technologies render privacy protection difficult to put into practice. A lot of data communications already take place nowadays on the Internet without the users' notice and the situation is going to get worse with the advent of "ambient intelligence" or "pervasive computing" [28]. One of the most challenging privacy issues in this context is the compliance with the "informed consent" principle, which is a cornerstone of most data protection regulations. For example, Article 7 of the EU Directive 95/46/EC states that "personal data may be processed only if the data subject has unambiguously given his consent" (unless waiver conditions are satisfied, such as the protection of the vital interests of the subject). In addition, this consent must be informed in the sense that the controller must provide sufficient information to the data subject, including "the purposes of the processing for which the data are intended". We have studied the notion of consent from the legal point of view, identified its limitations and proposed avenues for clarification and enhancement of the rights of the individuals [9].

On the technical side, privacy by design is often praised as an essential step towards a better privacy protection: in a world where privacy is increasingly jeopardized by new information and communication technologies, the growing view is that part of the remedy should come from the technologies themselves. One must admit however that the take-up of privacy by design is still rather limited so far. We have reviewed this gap between a toolset of available technologies and the still unrealized promises of privacy by design and suggested a range of actions to enter into a virtuous cycle for a wider adoption of privacy by design [10].

One way to apply the principles of privacy by design to the aforementioned issue of "informed consent" is to provide a framework allowing the subjects to express their wishes in terms of privacy policies. However privacy is a very subtle notion and the definition, implementation and practical use of privacy policies raise a number of challenges. LICIT has tackled these issues from complementary perspectives in 2010, from logics to languages and applications:

A logical framework for the expression of privacy policies

A major challenge for the formalization of privacy policies is the integration of deontic and temporal operators [7]. Deontic operators are required because privacy policies are typically expressed in terms of obligations and interdictions. Temporal operators are necessary because obligations and interdictions usually come with deadlines: for example, the controller must inform the data subject before forwarding his data to a third party or must delete the data within a given period of time. On the theoretical side, the limitations of Standard Deontic Logic (SDL) have constantly been pointed out, almost since its introduction. However, no other unified mathematical formalization of this logic has been proposed so far. Instead, many specialized logics have been put forward, each aimed at addressing one particular issue. To adddress this challenge, we have proposed a normal modal deontic logic based on a dyadic operator, similar in structure to the temporal "until" [16]. By bringing significant expressiveness to the logic, this operator makes it possible to define both a monadic desirability operator similar to the SDL obligation and the expression of the relative level of desirability of target formulae. The interpretation of this logic on a linear structure of worlds ordered by desirability makes its semantics more intuitive and concrete than the SDL deontic accessibility relation. We have also shown that the core modality of the logic allows us to represent well-known paradoxes of deontic logic in a more precise way, which does not lead to inconsistencies [16].

Privacy policy languages

In practice, the implementation of privacy policies involves two complementary aspects: the expression of the subject's wishes and the enforcement of the rules on the controller's side. As far as the subject is concerned, a model of "privacy aware agent" has been proposed to provide assistance in the definition of data protection rules. This agent has the ability to analyze and reason about normative contexts [6][5]. On the controller's side, we have proposed a language called FLAVOR (Formal Language for A posteriori Verification Of legal Rules) for the expression of obligations to be fulfilled by organizations. Indeed, organizations have to comply with a growing number of legal rules stemming from law, regulations, corporate policies or contractual agreements. Generally speaking, the actions to be monitored can be checked either *a priori* or *a posteriori*. *A priori* checks are stronger in the sense that they make it possible to ensure that no breach will occur. However, they are too constraining, if not inapplicable, in many situations. Even when they could be implemented, *a priori* checks are not desirable in situations in which it could be legitimate to bypass the rules. For instance, it is necessary to provide emergency procedures to access personal health records when human lifes are at stake, even if the medical practitioner on duty does not have sufficient permissions. The essential features provided by FLAVOR are the possibility to express "contrary to duty" obligations (substitute obligations to be fulfilled in case of breach of the primary obligation), obligations with deadlines and contextual obligations. We have defined a strength ordering between obligations and illustrated the language with typical privacy policy rules.

Privacy policies for healthcare records

Healthcare is one of the most demanding areas with respect to privacy policies and subject consent. First there is a strong pressure to implement electronic healthcare records for a variety of reasons: data availability, quality of care, cost reduction, etc. But the management of healthcare records is quite challenging because healthcare data is considered as sensitive from a legal point of view (with stronger constraints on collection and use) and such records can potentially be accessed by a large number of actors with different privileges (doctors, surgeons, physicians, nurses, etc.). Appropriate means should be provided to allow the patient to define his privacy policy with the required level of detail and confidence. In collaboration with the SMIS project team, we have defined EBAC, an event based access control model which can be used by the patient to mask healthcare records in his folder [19]. The model is based on the concepts of events, episodes and

[5] [6] and [7] are follows-up of a thesis prepared in the LIG laboratory (MAGMA team).

trust relations. Each healthcare record is associated with an event and each event belongs to an episode. An episode is a logically related set of events such as “abortion” or “wisdom tooth extraction”. The trust relation defines, for each episode, what each actor can do and see from the other actors’ actions. To this end, events are qualified as “shared” or “exclusive” and read and write privileges depend on the qualification of the events. The semantics of the EBAC model has been defined in a relational framework and it has been implemented in the DBMS (Database Management System) system of the SMIS project team in the context of the DMSP (Shared Medical Social Folder) project of the Yvelines district council [18], [19].

6. Contracts and Grants with Industry

6.1. Software liability

LICIT is involved in an industrial collaboration with TRUSTED LOGIC in the framework of a “Research Valorisation Agreement” on legal issues in software engineering.

7. Other Grants and Activities

7.1. Regional actions

Participants: Daniel Le Métayer, Sophie Guicherd.

The CIBLE programme of Région Rhône-Alpes funds a collaborative project involving LICIT, the Valorisation Service of the INRIA Grenoble Rhône-Alpes and the research group GRDS (“Research Group in Law and Science”) of the Law Faculty of Grenoble (University Pierre Mendès-France). The main objective of this project is to study, from a dual - academic and industrial - perspective the legal issues pursuant to software license agreements, especially liability issues. This project funds a doctoral position (Sophie Guicherd).

7.2. National actions

7.2.1. Lise (ANR)

Participants: Daniel Le Métayer, Eduardo Mazza, Manuel Maarek.

The LISE [6] project started in 2008 and is funded by the ANR SESUR programme. LISE is coordinated by LICIT and invloves the AMAZONES and POP ART INRIA project-teams, the Law Faculty of Versailles Saint-Quentin, the Law Faculty of Caen, VERIMAG and SUPELEC.

One of the motivations of the LISE project is the fact that, as observed by several authors, software quality and patterns of security frauds are directly related to legal liability patterns. But the precise definition of the expected functionalities of software systems is quite a challenge, not to mention the use of such definition as a basis for a liability agreement. Taking up this challenge is precisely the objective of LISE. To achieve this goal, the project studies liability issues both from the legal and the technical points of view with the aim to put forward methods (1) to define liability in a precise and unambiguous way and (2) to establish liability in case of disagreement [12], [5].

7.2.2. Fluor (ANR)

Participants: Daniel Le Métayer, Guillaume Piolle.

The FLUOR [7] project started in 2008 and is funded by the ANR SESUR programme. FLUOR is coordinated by ENSTB and involves the CNRS (IODE), INRIA (LICIT), the LIUPPA (University of Pau), SWID and the University of Polynésie Française.

[6] http://licit.inrialpes.fr/lise/
[7] http://fluor.no-ip.fr/

The FLUOR project aims to protect corporate documents circulating within companies. More precisely, the objective of the project is to unify information flow models and usage control models and to analyse the legal issues raised by the use of these documents. Emphasis will be put by LICIT on the specification of obligations within organizations and the associated risk analysis.

7.2.3. Persopolis (Competitivity poles Systematic and TES)

Participants: Daniel Le Métayer, Julien Le Clainche.

PERSOPOLIS (2008-2010) is a project funded by the Competitivity poles SYSTEMATIC and TES. The coordinator is OCS (Oberthur Card Systems) and the other partners of the project are CEV, ENSI Caen, IAE Caen, the Law Faculty of Caen, INRIA (LICIT), NBSTECH and TRUSTED LOGIC.

The smart card life cycle includes, before delivery to the end-user, a personalization phase which consists in loading into the card data which is specific to the user (typically name, credentials, cetificates...). This personalization phase, which is highly critical, is generally conducted in the secured premises of the card manufacturer or subcontracted to a third party ("personalizer") offering high security guarantees. In order to favour the deployment of service cards managed by local authorities (e.g. city council, social services, employment agencies...) it is necessary to reconsider this centralized personalization process while maintaining the required security guarantees. The objective of the PERSOPOLIS project is to define the technical and legal requirements for the personalization of smart cards in such "open" contexts. Emphasis is put on the management of personal data and the associated liability issues.

7.2.4. Collaborations inside Inria

LICIT collaborates with the AMAZONES and POP ART project-teams in the context of LISE and with the SMIS project-team on the design of privacy policies for healthcare files.

7.2.5. Cooperations with other laboratories

LICIT collaborates with the following laboratories:

Research groups in computer science:

- SSIR ("Security of Information Systems and Networks") - SUPELEC (LISE project).
- VERIMAG- INPG Grenoble (LISE project).
- SISTEM- ENSI Caen (PERSOPOLIS project).
- CIME - IAE Caen (PERSOPOLIS project).
- LIUPPA - University of Pau (FLUOR project).
- SERES, PRATIC, LUSSI - ENSTB (FLUOR project).
- Terre-Océan - University of Polynésie Française (FLUOR project).

Research groups in law:

- GRDS ("Research Group in Law and Science") - Law Faculty of Grenoble, University Pierre Mendès-France (CIBLE project).
- DANTE ("Business and New Technologies Law") - Law Faculty of Versailles Saint-Quentin (LISE project).
- PRINT("Intellectual Property") - Law Faculty of Caen (LISE and PERSOPOLIS projects).
- IODE (European Regulation and Human Rights) - CNRS (FLUOR project).

7.3. International Actions

LICIT participates in the activities of the NESSI TSD WG ("Network European Software and Services Initiative - Trust, Security and Dependability Working Group").

8. Dissemination

8.1. Scientific community

As part of the networking activities put forward in Section 2.1, LICIT has organized or co-organized the following events:

- Workshop on legal issues of multi-service smart card deployment (Caen, 7 January). The other organizer was ENSI Caen. This open workshop was organized in the context of the PERSOPOLIS project.
- Annual Conference on Computers, Privacy and Data Protection CPDP 2010 (Brussels, 28-29 January 2010)[8]. The other organizers are the Free University of Brussels (VUB), the University of Tilburg, the University of Namur and the Fraunhaufer Institute. CPDP, which is now established as the main privacy conference in Europe, attracts every year a wider and more multidisciplinary audience (more than 200 participants in 2010).
- First national workshop on privacy protection APVP 2010 (Annecy, 26-27 May 2010)[9]. The other organizers were the PLANETE project-team and LAAS (Toulouse).
- Workshops on legal issues in software engineering (Grenoble, 1 June and 24 June). The other organizer was the university Pierre Mendès-France (Grenoble). These open workshops were organized in the context of the regional CIBLE project.
- Conference on legal issues in software contracts and the impact of cloud computing and free software (Paris, 3 December) [10]. The other organizers were the DANTE laboratory (University of Versailles Saint-Quentin) and the AFDIT (Association Française du Droit de l'Informatique et de la Télécommunication). This conference, which was organized in the context of the LISE project, has attracted more than 200 participants.

Daniel Le Métayer was a member of the scientific committees of :

- The sixth International Workshop on Security and Trust Management STM 2010.
- The Annual Conference on Computers, Privacy and Data Protection CPDP 2010.
- The Annual Conference on Security in Network Architectures and Information Systems SAR-SSI 2010.

and gave the following invited talks:

- Namur, 20th anniversary of the CITA laboratory: *Vie privée et libertés: articulation des protections techniques et juridiques* in partnership with Yves Poullet (CRID Namur).
- Berlin, PRECIOSA workshop on Privacy in ITS Applications : *Formal methods for privacy.*
- Paris, MFDL workshop: *Liability issues in software engineering: a formal approach.*

As far as institutional relationships are concerned, Daniel Le Métayer was invited to express his views in the context of a hearing hold by the CNIL on the future of privacy protection and the definition of personal data.

8.2. Teaching

8.2.1. Courses

Daniel Le Métayer and Guillaume Piolle gave a tutorial on privacy at the ADBS workshop in Biarritz.

[8] http://www.cpdpconferences.org
[9] http://licit.inrialpes.fr/apvp2010/
[10] http://juriscom.net/actu/visu.php?ID=1263

Daniel Le Métayer also gave a tutorial on privacy by design at the University of Lyon 1 and a talk on ethical issues related to privacy at the university Joseph Fourier (Grenoble).

8.2.2. Advising

- Eduardo Mazza, co-advised by Daniel Le Métayer (with Marie-Laure Potet, VERIMAG), PhD in computer science, INPG.
- Sophie Guicherd, co-advised by Daniel Le Métayer (with Etienne Vergès, GRDS Law Faculty of Grenoble), PhD in law, Pierre Mendès-France University.

9. Bibliography

Major publications by the team in recent years

[1] D. LE MÉTAYER (editor). *Les technologies au service des droits, opportunités, défis, limites*, Bruylant, Cahiers du CRID No 32, 2010.

[2] D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. FRENOT, V. VIET TRIEM TONG, N. CREPEAU, R. HARDOUIN. *Liability in software engineering: overview of the LISE approach and application on a case study*, in "International Conference on Software Engineering, ICSE'2010", ACM/IEEE, 2010, p. 135-144.

[3] D. LE MÉTAYER, E. MAZZA, M.-L. POTET. *Designing log architectures for legal evidence*, in "8th International Conference on Software Engineering and Formal Methods, SEFM'2010", IEEE, 2010, p. 156-165.

[4] D. LE MÉTAYER, S. MONTELEONE. *Automated consent through privacy agents : legal requirements and technical architecture*, in "The Computer Law and Security Review, Elsevier", 2009, vol. 25(2).

Publications of the year

Articles in International Peer-Reviewed Journal

[5] D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. FRENOT, V. VIET TRIEM TONG, N. CREPEAU, R. HARDOUIN. *Liability issues in software engineering. The use of formal methods to reduce legal uncertainties*, in "Communications of the ACM", 2011, journal version of the ICSE conference paper, to appear in CACM Research Highlights.

[6] G. PIOLLE, Y. DEMAZEAU. *Déléguer la protection des données personnelles à des agents cognitifs*, in "Revue d'Intelligence Artificielle", 2010, p. 357-390.

[7] G. PIOLLE, Y. DEMAZEAU. *Representing privacy regulations with deontico-temporal operators*, in "Web Intelligence and Agent Systems: an International Journal (WIAS)", 2010, to appear.

Invited Conferences

[8] T. ALLARD, N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, R. THION. *Concilier ubiquité et sécurité des données médicales*, in "Les technologies au service des droits, opportunités, défis, limites", Bruylant, Cahiers du CRID No 32, 2010, p. 173-207.

[9] J. LE CLAINCHE. *Consentement et traitement de données à caractère personnel*, in "Les technologies au service des droits, opportunités, défis, limites", Bruylant, Cahiers du CRID No 32, 2010, p. 135-171.

[10] D. LE MÉTAYER. *Privacy by design: a matter of choice*, in "Data Protection in a Profiled World", S. GUTWIRTH, Y. POULLET, P. DE HERT (editors), Springer Verlag, 2010, p. 323-334.

International Peer-Reviewed Conference/Proceedings

[11] G. GOESSLER, J.-B. RACLET, D. LE MÉTAYER. *Causality Analysis in Contract Violation*, in "Proceedings of the International Conference on Runtime Verification (RV' 2010)", LNCS, Springer Verlag, 2010, vol. 6418, p. 270-284.

[12] D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. FRENOT, V. VIET TRIEM TONG, N. CREPEAU, R. HARDOUIN. *Liability in software engineering: overview of the LISE approach and application on a case study*, in "International Conference on Software Engineering, ICSE'2010", ACM/IEEE, 2010, p. 135-144.

[13] D. LE MÉTAYER, E. MAZZA, M.-L. POTET. *Designing log architectures for legal evidence*, in "8th International Conference on Software Engineering and Formal Methods, SEFM'2010", IEEE, 2010, p. 156-165.

[14] M. MAAREK. *On the extraction of decisions and contributions from summaries of Legal IT Contract Cases*, in "Proceedings of the LREC 2010 Workshop on Semantic Processing of Legal Texts (SPLeT-2010)", 2010, http://www.lrec-conf.org/proceedings/lrec2010/workshops/W23.pdf.

[15] E. MAZZA, M.-L. POTET, D. LE MÉTAYER. *A formal framework for specifying and analyzing logs as electronic evidence*, in "3rd Brazilian Symposium on Formal Methods, SBMF'2010", LNCS, Springer Verlag, 2010, vol. 6527.

[16] G. PIOLLE. *A dyadic operator for the gradation of desirability*, in "Proceedings of the 10th International Conference on Deontic Logic in Computer Science (DEON'10)", LNAI, Springer Verlag, 2010, vol. 6181, p. 33-49.

National Peer-Reviewed Conference/Proceedings

[17] D. LE MÉTAYER, G. PIOLLE. *Droits et obligations à l'ère numérique: protection de la vie privée*, in "Séminaire INRIA - L'usager Numérique", ADBS Editions, 2010, p. 66-88.

Scientific Books (or Scientific Book chapters)

[18] T. ALLARD, N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, R. THION. *Seamless Access to Healthcare Folders with Strong Privacy Guarantees*, in "Healthcare Delivery Reform and New Technologies: Organizational Initiatives", IGI Global Publishing, 2010, to appear.

[19] T. ALLARD, N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, R. THION. *Trustworthiness of Pervasive Healthcare Folders*, in "Pervasive and Smart Technologies for Healthcare: Ubiquitous Methodologies and Tools", IGI Global Publishing, 2010, p. 172-196.

Books or Proceedings Editing

[20] D. LE MÉTAYER (editor). *Les technologies au service des droits, opportunités, défis, limites*, Bruylant, Cahiers du CRID No 32, 2010.

Scientific Popularization

[21] D. LE MÉTAYER. *Au service des citoyens*, in "Textes et Documents pour la Classe", 2010.

References in notes

[22] L. L. FULLER. *The morality of law*, Yale University Press, 1964.

[23] D. LE MÉTAYER, A. ROUVROY. *STIC et droit : défis, conflits et complémentarités*, in "Interstices", November 2008, http://interstices.info/jcms/c_34521/stic-et-droit-defis-conflits-et-complementarites.

[24] L. LESSIG. *The future of ideas: the fate of the commons in a connected world*, Random House, 2001.

[25] L. LESSIG. *Code and other laws of cyberspace, Version 2.0*, Basic Books, 2007.

[26] Y. POULLET. *The Directive 95/46/EC: ten years after*, in "Computer Law and Security Report", 2006, vol. 22, p. 206–217.

[27] J. REIDENBERG. *Lex informatica: the formulation of information policy rules through technology*, in "Texas Law Review", 1998, vol. 76, n^{o} 3.

[28] A. ROUVROY. *Privacy, data protection and the unprecedented challenges of ambient intelligence*, in "Studies in Ethics, Law and Technology, Berkley Electronic Press", 2008.