Computer Assisted Consent for Personal Data Processing

Daniel Le Métayer
Shara Monteleone

INRIA Grenoble Rhône-Alpes
Daniel.Le-Metayer/Shara.Monteleone@inrialpes.fr

Abstract. The changes imposed by new information technologies, especially pervasive computing and the Internet, require a deep reflection on the fundamental values underlying privacy and the best way to achieve their protection. The explicit consent of the data subject, which is a cornerstone of most data protection regulations, is a typical example of requirement which is difficult to put into practice in the new world of "pervasive computing" where many data communications necessarily occur without the users' notice. In this paper, we study the legal implications of the use of "Privacy Agents" to make privacy right protection more effective. We consider successively three aspects of consent – its nature, its essential features (qualities and defects) and its formal requirements, and we draw the lessons of this legal analysis for the design of valid Privacy Agents. To conclude, we suggest an implementation of these requirements developed in PRIAM[1], a multidisciplinary project involving lawyers and computer scientists.

Reference: Proceedings of the *3d LSPI Conference on Legal Security and Privacy Issues in IT (LSPI'2009)*, pp. 29-41.

1. Why Computer Assisted Consent ?

Privacy is a complex and multi-faceted notion, both from the social and from the legal point of view and it has been interpreted in various ways depending on times, cultures and individual perceptions (Solove, 2008). Notwithstanding such differences, it is widely agreed that the values underlying privacy pertain to fundamental human rights (Rouvroy, 2008) and many regulations, instruments and recommendations have been introduced to protect them[2]. Despite apparently strong legal protections, many citizens feel that technologies – especially information technologies – have invaded so many aspects of their

[1] PRIAM: "PRivacy Issues in AMbient intelligence", http://priam.citi.insa-lyon.fr/.

[2] Just to take a few examples: the European Convention on Human Rights, the Charter of the Fundamental Rights of the European Union, the European Directives 95/46/EC and 2002/58/EC; the US 1974 Privacy Act and the Health Insurance Portability and the Accountability Act (HIPAA); the Australian Privacy Act; the Japan Personal Information Protection Act; OECD Privacy Guidelines; UN Guidelines Concerning Personalized Computer Files, etc.

lives that they no longer have suitable guarantees about their privacy. This has given rise to two different kinds of attitudes. Some people are inclined to consider that this loss of privacy is the price to pay for new facilities, while others strongly oppose the idea of having to relinquish one of their fundamental rights in return for inessential services, and prefer to snub these services altogether. Neither of these attitudes can be qualified as satisfactory or sustainable in the long term. In the same way as the growing use of photography at the end of the 19th century prompted S. Warren and L. Brandeis seminal paper (Warren & Brandeis, 1890) we believe that the changes imposed by new information technologies, especially pervasive computing and the Internet, require a deep reflection on the fundamental values underlying privacy and the best way to achieve their protection (Bennet, 1992; Poullet & Dinant, 2006; Poullet, 2006a; Poullet, 2006b; Kleve & De Mulder, 2007, Rouvroy, 2008). We also believe that such reassessment should be a multidisciplinary endeavour because privacy can neither be apprehended nor guaranteed by exclusively legal, social or technical approaches, in particular in the context of the fast development of new information technologies (Cohen, 2003; Poullet, 2006b; Kosta, Zibuschka, Scherner, Dumortier, 2008).

We illustrate our position with the explicit consent of the data subject, which is a cornerstone of most data protection regulations (Veldhuisen, 2007). For example, Article 7 of the EU Directive 95/46/EC[3] 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*". But many aspects of new information technologies render privacy protection – and especially informed consent – difficult to put into practice (Bygrave, 2001; Poullet 2006a; Friedewald, Vildjiounaite, Punie, & Wright, 2007; Rouvroy 2008). Many 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". These expressions refer to environments where individuals are surrounded by small devices with capabilities for computing, communicating and reasoning. Such devices include sensors, actuators, RFID tags, mobile phones, communicating personal digital assistants (PDAs), etc. They communicate through various wireless protocols such as Bluetooth, WiFi, WLAN, GPRS, etc. The strong marketing argument for pervasive computing proponents is the possibility for human beings to evolve in a dream environment that automatically adapts to their (supposed) wishes: for example, the front door automatically opens when the home owner comes close and his RFID badge gets detected, or the car adjusts to the preferences of the driver (wheel and rear-view mirror positions, internal temperature, radio channel, etc.). But the key features of pervasive computing that make such feats possible, namely invisible communications and profiling, also raise a lot of concern with respect to privacy. Coming back to the "informed consent", imposing that the user of pervasive systems gives his consent before each communication of personal data would largely defeat the purpose of providing these systems in the first place. This would lead to a situation where individuals would just have the choice between refusing the new services or renouncing to their privacy rights.

[3] Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995.

Our intent in presenting this apparent discrepancy between new technologies and privacy regulations is not to be defeatist though. The natural question for the computer scientist is then: what about using the technology itself to cure the problems caused by the technology? In other words, if privacy rights are jeopardized by the highest level of automation provided by pervasive computing, it is also possible to increase the level of automation on the side of the defence of these rights. This idea leads to the notion of “Privacy Agent”, a dedicated software which would act as a “surrogate” of the subject and manage on his behalf his personal data. The subject could define his privacy requirements once for all, with all information and assistance required, and then rely on his Privacy Agent to implement these requirements faithfully. But this possibility also triggers a number of new questions from the legal side (Stuurman & Wijnands 2001; Cranor & Reidenberg, 2002): To what extent should a consent delivered via a software agent be considered as legally valid? Are the current regulations flexible enough to accept such kind of delegation to an automated system? Can the Privacy Agent be “intelligent” enough to deal with all possible situations ? Should subjects really rely on their Privacy Agent and what would be the consequences of any error (bug, misunderstanding, etc.) in the process?

The goal of this paper is to contribute to the legal analysis of these questions and put forward technical and legal constraints that should be imposed on a Privacy Agent to be used as a valid medium for the consent of the data subject. To this aim, we consider successively three aspects which have to be clarified to properly adress the implementation of consent by Privacy Agents: we start with a study of the legal nature of consent (unilateral versus contractual act) in Section 2. Then we proceed with its essential features in Section 3 (qualities and defects) and its formal requirements in Section 4. In each of these sections, we focus mostly on privacy and data protection regulations and recommendations (official texts, mostly European, as well as jurisprudence and doctrine) and put them, as necessary, in the broader perspective of civil law. In Section 5 we draw the lessons to be learned from this legal analysis for the design of Privacy Agents and we suggest in Section 6 an implementation of these requirements, as proposed in the PRIAM project.

2. Consent : Unilateral Act or Contract ?

The first issue to address before considering the development of Privacy Agents concerns the very nature of consent. Indeed, the word “consent” can have two different meanings in civil law : in some cases, it conveys the idea of an agreement between at least two persons (reflecting the etymology *cum sentire*); in other cases it is used in the sense of a single manifestation of will. The essential role of the free personal will is the legacy of the “subjectivist” theory of the last century. According to this theory, legal obligations strictly depend on the consent as act of will. This point of view has inspired the “consensualism” movement, which has promoted the “autonomy of will” and had a strong influence on the legal systems of civil law tradition: in these systems, the exchange of consents between the parties is essential for the validity of legal acts, the form requirement being the exception (Forray, 2007).

In the context of data protection regulations, the nature of consent (contractual versus unilateral) has fueled some debates in the last decade (Bibas, 1994; Mell, 1996; Messinetti, 1998; Litman, 2000; Schwartz, 2004; Sica & Stanzione, 2005). Advocates of the first view see the relationship between the data subject and the data controller as a contract. This position is often associated with the idea that subjects have property rights on their personal data, which, due to their scarce nature, become assets in the information society and, therefore, possible objects of economic transactions. Evidence would come from the fact that data are often disclosed as a compensation, or a requirement, for services, and they are thus convertible into money (Bibas, 1994). The right of the subject to oppose to further processing of his personal data would prove the continuity of the relationship between the controller and the subject (Zeno Zencovich, 1997). Other developments in this direction include (Schwartz, 2004) which proposes a model of "propertized personal information" (specifically with respect to the U.S. regulation) and (Mell, 1996) which observes the variety of interests in personal data (interests of the individuals, interests of the government, public interest, commercial interests) and argues that property law, which has long been used to balance competing interests, can provide a basis for a better privacy protection.

Supporters of the second view (consent as unilateral act) see the consent as a form of authorization and analyze data protection not in terms of property, but in terms of freedoms (Poullet, 1991; Messinetti, 1998; Sica & Stanzione, 2005). The fundamental value grounding data protection laws is the respect of individual autonomy (Rouvroy, 2008, Rouvroy & Poullet, 2008): the subject's consent thus becomes a form of control on his personal data.

The unilateral act theory is the most widely accepted today (at least in Europe) and it is also the most protective for data subjects. In particular, this theory is more consistent with the fact that consent is neither always necessary (derogations), nor always sufficient (for example, the processing of sensitive data requires in addition the authorization of the data protection authority). In addition, the exercise of the rights of the subject (access, modification, etc.) is a legal obligation of the controller (rather than a contractual obligation). In particular, the right to object for "legitimate grounds" or for marketing purposes is more difficult to reconcile with the contractual view[4]. Moreover, the Directive 95/46/EC asks for the specific consent of the subject (which means, according to most interpretations, an expression of will separated from other contractual clauses[5]), which pleads in favour of the theory of unilateral act: the fact that the request for consent is sometimes included into the body of a commercial contract (typically in general conditions) is not an acknowledgment of the contractual nature of the consent[6].

The system of sanctions and remedies set forth in European data protection regulations provides even stronger arguments in favour of the theory of unilateral act:

(1) Most European national laws provide administrative or criminal sanctions. This is a distinctive feature of a system of protection of society rather than individual interests which are the realm of contracts.

[4] The expression "legitimate grounds" covers situations which are not reducible to the controller's acts, for examples situations related to the subject only, such as change of name, of political or religious convictions, etc.

[5] See the indications provided in the Opinion 5/2004, § 3.2., by the Art 29 Data Protection Working Party.

[6] For example (Bianca & Busnelli, 2007) observes that the freedom to conclude a contract with a bank is sometimes confused with the freedom to give one's consent for personal data processing. Indeed, one may argue that the customer's consent for personal data processing is not valid when it is incorporated into a commercial contract if the subject cannot express such consent (for personal data processing) separately from his consent to the contract itself (unless the processing of such personal data is required to execute the contract).

(2) In order to start legal proceedings, the existence of the damage (typical of the civil responsibility) is not required, the breach of the law by the controller being sufficient[7].

(3) In case of invalid consent, the subject does not need to enter into a complex and expensive action of annulment (as required in case of defective consent for a contract): he can just send a request to the national data protection authority to stop the illicit processing[8].

(4) Last but not least, the sanctions can be applied (according to European national laws) on the initiative of the data protection authority (*ex officio*), without any action of the subject himself: this contrasts with the private autonomy, typical of the contractual system. This choice is motivated by the consideration, made by the legislator, of the unbalanced positions of the subject and the controller (the latter usually being in a dominant position).

To conclude this section, let us mention that the prominent role of the data protection authorities in European regulations is consistent with the view that certain fundamental rights cannot be left to the contractual autonomy of the individuals (Sica & Stanzione, 2005). Coming back to the nature of consent, we can thus take the position that, even if it is not an absolute criterion for lawful personal data processing (because of the legal exceptions and the additional authorizations which can be required from data protection authorities), the consent should be interpreted as a manifestation of individual will of the subject rather than as a contractual relationship between the subject and the controller. The impacts of this interpretation on the design of Privacy Agents are presented in Section 5.

3. Consent : Qualities and Defects

The next question regarding consent concerns the definition of its essential features, both on the positive side (qualities) and the negative side (defects). As far as qualities are concerned, the Directive 95/46/EC states that the consent must be (a) *freely* given, (b) *specific*, (c) *informed* and *unambiguous*:

(a) According to the Art 29 Data Protection Working Party[9], *free* means that the subject has had the opportunity to make a genuine choice and to evaluate the consequences of this choice[10]. For example, the consent cannot be considered as free if it is delivered (e.g. for marketing purposes) in the general conditions of a commercial contract (Bianca & Busnelli, 2007). The consent must also be without pressure or bullying: in circumstances in which the subject is in a position of weakness or dependency, such as e.g. in employer–employee

[7] Civil actions for damages remain a possibility, but in case of damages that are direct consequences of the processing (see Art 23 of the Directive 95/46/EC).

[8] For example the decision of the French CNIL n° 2007-352 of the 22th November 2007 imposes a fine of 5 000 euros against a marketing company for unsollicited communications after several notices enjoining this company to delete personal data as requested by their subjects. This decision is available at http://www.cnil.fr/index.php?id=2435.

[9] Art 29 Data Protection Working Party, which is an independent European advisory body on privacy and data protection, set up under art 29 of Directive 95/45/EC.

[10] See Art 29 Working Party, Opinion n. 114/2005 of 25 November 2005, § 2.1.: “Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a *fait accompli* cannot be considered to be valid”.

relationships (Fragale Filho & Jeffery, 2003), he must have a real opportunity to withhold his consent without suffering any harm.

(b) According to the Art 29 Data Protection Working Party, *specific* means that the consent cannot be granted for a generic processing but should refer to well delimited purposes and aims: different scopes require different (separate) manifestations of consent. It is generally agreed however that a specific consent can refer to categories of processing. For example, Directive 2002/58/EC[11] (art 13) allows unsolicited electronic communications, even without the subject's consent, in the context of an offer of products or services similar to products or services already provided to the subject[12]. This provision is significant in the perspective of Privacy Agents because it introduces the principle that the consent of the subject does not necessarily need to occur just before each single disclosure of data.

(c) The first condition for *unambiguous* consent is the "opt-in" requirement which is reaffirmed by the Art 29 Data Protection Working Party (tacit consent is not acceptable). Another necessary condition is the fulfilment by the controller of the obligation of information (identity, nature of the collected data, purpose of the processing, third parties that could get access to the data, etc.) in order to ensure that the consent of the subject is *aware*. Most European laws do not provide any precise constraint or details on the information to be provided though, and it turns out that in practice data controllers often provide only vague information (or no information at all)[13]. As argued in Section 5, it is also possible to design Privacy Agents that enforce a minimum level of information[14].

Even though the above definitions of the requirements for valid consent, as provided by the data protection regulations, prevail upon the more general rules of the civil law, the traditional categories of defect of consent (mistake, violence or duress, willful misrepresentation)[15] still have residual application. The notion of "mistake", or misunderstanding of essential aspects of the consent, is especially significant in the context of Privacy Agents, at least for two reasons: first, it is well known that software may contain bugs, which means that a Privacy Agent could behave differently from the expectations of the subject. In addition, misunderstanding can also occur during the interaction between the subject and his Privacy Agent. According to civil law, such mistakes could be sufficient to

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L 201, 31/07/2002.

[12] C.f. Art 29 Working Party, Opinion n. 5/2004, § 3.5: "The purpose principle (compatible use, fair processing) should help in this regard [...] similarity could be judged in particular from the objective perspective (reasonable expectations) of the recipient, rather than from the perspective of the sender [of emails]".

[13] See the Flesh Eurobarometer Survey on Data Protection in the EU, n. 226, 2008, about the need expressed by controllers of a better definition and harmonization at European level of the information obligations.

[14] (Schuck, 1994) also argues that new technologies can be used to better enforce the information obligation.

[15] According to the theory of the defects of consent, any mistake in the process of formation of the will, or any act of violence or fraud used to obtain a consent cause its invalidity; to be able to invalidate the consent, the mistake should be determining for the personal decision: the subject would not have provided his consent if he had known the truth; the violence (physical or moral) and the wilful misrepresentation affect the essence of the consent, making it defective (Forray, 2006).

make the consent null and void unless it is possible to resort to the “appearance principle” and consider that the subject has used the Privacy Agent knowingly (also aware of the risk of bugs) and has thus taken the responsibility for the consent. According the “appearance principle”, a party creating trust and reliance in the mind of the other parties may be legally bound by the consequences of legal acts concluded on the basis of such trust (Dahiyat, 2006). In the context of data protection, this principle makes legal the collection and processing of personal data by a controller based on interactions with the Privacy Agent of the subject (provided that the controller has complied with the requirements of the subject, as expressed by his Privacy Agent), even if the behaviour of this Privacy Agent didn’t reflect the true wishes of the subject. In such a situation, the subject can take other actions: first, he can forbid further processing of his data on the basis of “legitimate ground”; he can also turn against the supplier of the Privacy Agent to get appropriate indemnifications or compensations (provided however that he has executed with this supplier a sufficiently protective contract).We come back to this issue in Section 5.

4. Consent : Formal Requirements

In the previous sections we have studied the nature of consent and its essential features. The last aspect which is of prime importance to determine the conditions for the validity of Privacy Agents is the legal requirements on the form of the consent. The Directive 95/46/EC requires the *explicit* consent for the processing of sensitive data, leaving the implementation modalities to the national laws. Looking at national transpositions of the Directive, we observe, for example, that the French law does not mention a specific form for the consent in case of ordinary data but requires an *express* consent for sensitive data: both the doctrine and the jurisprudence tend to interpret express consent as *written* consent (Gentot, 2002). In the Italian Law, the consent for ordinary data must be “documented in writing”, it being understood that the consent document does not need to be created by the subject (it can also be recorded by the controller). For the processing of sensitive data, the Italian Law also requires a “written consent of the subject” (in addition to the authorization of the data protection authority).

The written consent for the processing of sensitive data is usually interpreted as a *signed* consent (Bianca, 2007; Sica & Stanzione, 2005). The differences between the ways to express the consent for ordinary and for sensitive data can also be analyzed in the light of the traditional legal distinction between written documents which are required *ad validitatem* or *ad probationem* (Forray, 2007; Joly-Passant, 2006). Documents required *ad validitatem* constitute a necessary condition for the existence of the act itself. Documents required *ad probationem* can be used as evidence in case of dispute, leaving the possibility to prove the existence of the act by other means. For the processing of ordinary data, the main opinion is that, when the law[16] requires a specific form, its function is *ad probationem* (Bianca, 2007) and the electronic form is admissible[17]. On the other hand, regarding

[16] Like in the Italian law.

[17] The Directive 1999/93/EC has introduced the legal equivalence between electronic and traditional documents. Therefore, the support and technology used can only affect the probative values of the documents.

sensitive data, it is widely admitted that the signed consent is required *ad validitatem*: if this requirement is not fulfilled, the consent is considered null and the processing is unlawful[18].

In conclusion, it seems that no formal requirement proves a stumbling block to the delivery of consent through Privacy Agents. However, if the possibility of consent expressed electronically for the processing of ordinary data is generally accepted without strong technical requirements[19], the same cannot be said for sensitive data. This does not preclude the use of electronic consent in such cases though, but this would require the use of an “advanced electronic signature” in the sense of the Directive 1999/93/EC[20], which puts much stronger requirements on the implementation and use of Privacy Agents.

5. Requirements for Valid Privacy Agents

In the light of the legal analysis of the consent presented in the previous sections we can now reconsider the validity of “automated” consent through Privacy Agents and come back to the issues raised in the introduction. The notion of “agent” has been used in a number of privacy related projects during the last decade (Borking, 2000; Langheinrich, 2002; ISTPA, 2002; Pearson, 2002; Cissée & Albayrak, 2007) with different meanings and objectives. For the purpose of this paper, a Privacy Agent can be defined as a software offering two essential functionalities: (1) a User Interface to interact with the subject (for example to allow him to define his “privacy policy”) and (2) a Data Manager controlling the disclosure of personal data. First, as suggested in Section 3 and Section 4, no specific legal provision (at least in European regulations) excludes the possibility of consent through automated tools[21]. However the legal analysis of consent, of its qualities, defects and formal requirements all have a strong impact on the design of valid Privacy Agents, both on their User Interface and Data Manager component.

As far as the nature of consent is concerned, the choice of the “unilateral act” theory imposes that the Data Manager of the Privacy Agent is exclusively dedicated to the management of consent, which precludes, for example, technical solutions integrating a negotiation phase or delivering the consent as part of a more general agreement (e.g. on a package of services). In other words, the Data Manager should play the role of “privacy monitor” akin to the well-known “security monitors” which encapsulate in a single component all key security functions of a system (and only these functions, so as to keep this component minimal). In addition, in order to implement the opt-in principle, the Data Manager should be designed in such a way that data disclosure is prohibited by default and is allowed only in the cases (and contexts) explicitly specified by the subject. The Data Manager can also enforce the information obligation by checking the content of the messages sent by the controller prior to disclosure or by sending information requests to the controller.

[18] As an example of document which cannot be accepted as equivalent to a signed consent, (Bianca & Busnelli, 2007) refers to a questionnaire containing references to sensitive data.

[19] In Art 29 Working Party 5/2004, issue 3.2, the use of boxes to be ticked by the data subject is recommended as an indication of the subject’s consent.

[20] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013, 19/01/2000.

[21] We must admit, however, as discussed in (Bygrave, 2000), the paucity of case law in the area of data protection.

In order to ensure that the consent is specific, the User Interface of the Privacy Agent must be rich enough to allow the subject to express his wishes as precisely as possible (for example the authorized purposes, the precise categories of data, the contexts in which such data can be disclosed, the authorized third parties, etc.). In addition, in order avoid ambiguities, the system must provide a way to solve any divergence of interpretation concerning the consent. Indeed, one of the criticisms raised against existing privacy frameworks such as P3P (W3C, 2002) was their lack of clarity and the divergent (or even misleading) representations of privacy policies by user agents (Cranor & Reidenberg, 2002). Beyond legal considerations, the existence of a precise definition of privacy statements would also help increasing the trust of the individuals.

The most significant defect of consent to be considered in the context of automated tools is the "mistake", which, as stated in Section 3, could be sufficient to make the consent null and void unless it is possible to resort to the "appearance principle". To go in this direction, we believe that the use of Privacy Agents should be seen as a *shift of consent* of the subject: not a consent for the processing of his personal data by a third party, but a *consent* to use the Privacy Agent to *consent* on his behalf to the processing of his personal data ("super-consent"). This view has two major consequences:

(1) If the consent to use the Privacy Agent is valid, then the appearance principle should apply and controllers should not be threatened by subjects arguing that the consent delivered by their Privacy Agent is not valid. In the case of bug in the implementation of a Privacy Agent, misleading documentation or User Interface, subjects should rather turn against their Privacy Agent providers to get appropriate indemnifications or compensations[22].

(2) The contractual agreement between the Privacy Agent provider and the subject must clearly state the commitments of the provider and the expected behaviour of the Privacy Agent. In addition, precise procedures should be put in place to ensure that liabilities can be established in case of misbehaviour of the Privacy Agent (typically based on log data). Such procedures should be usable in case of litigation so that Privacy Agent providers have a real incentive to take all measures to deliver correct software. Ideally automatic audits should also be conducted on a regular basis to further strengthen the overall trust in the system.

The above considerations cover the legal requirements for the processing of non sensitive data. Technically speaking, several options are possible with respect to sensitive data. As set forth in Section 4, one possibility is to associate the Privacy Agent with an electronic signature, but this would make the system significantly more complex. Let us stress however that the unilateral interpretation of consent discussed in Section 2 requires a single signature (by the subject) rather than a double signature (by the subject and the controller). Another possibility is to rely on the Privacy Agent for non sensitive data only, and require the express consent of the subject (possibly through other means) for sensitive data. The Privacy Agent could still play the role of filter and send a warning to the subject upon receipt of a request for the disclosure of sensitive data.

[22] We consider implicitly here that no "legal personality" is granted to software agents, which cannot be liable as such, even though this issue is debated among lawyers (Stuurman & Wijnands, 2001; Finocchiaro, 2003; Dahiyat, 2006; Jurewitz, 2006).

6. Conclusion: Privacy Agents in Practice

In order to show that the requirements identified in this paper are not purely abstract considerations and can really be implemented, we sketch in this section the Privacy Agent architecture put forward in the PRIAM project. Actually, several kinds of Privacy Agents have been proposed in PRIAM, including:

- Subject Agents (as discussed in this paper) which are installed on a device attached to the subjects (for example their mobile phones) and control all disclosures of their personal data (whether stored on the same device or delivered through other means such as RFID tags or sensors).
- Controller Agents which are installed on the sites of the controllers and manage the access and use of the personal data collected by the controllers. Controller Agents implement the commitments of the controllers and ensure that all requirements set by the subjects are met (retention delay, access right, modification right, etc.).
- Auditor Agents which are launched by certified authorities and interact with Controller Agents to check their execution traces.

As far as the legal framework is concerned, the roles of the different actors involved in the process have been defined precisely (including the roles of the subjects, of the controllers, of the Privacy Agent providers and the personal data authority) and contract models have been proposed to formalize the commitments of the Privacy Agent provider with respect to the subjects and to the controllers. In order to minimize the risks of misunderstanding, a simple privacy language has been devised. This language is a restricted (pattern based) natural language dedicated to the expression of privacy policies (the requirements of the subject on one side and the commitments of the controller on the other side). Subjects (respectively controllers) can interact with their agents through a user-friendly interface and double-check a natural text description of their privacy requirements (respectively privacy commitments) before accepting them. In order to avoid ambiguities in the expression of privacy policies, a mathematical semantics of the privacy language has been defined. This mathematical semantics characterizes precisely the expected behaviour of the Privacy Agents (based on the privacy policies defined by their users) in terms of *authorized execution traces.* In addition, as recommended in the previous section, all privacy related actions are recorded into log files which can be audited automatically by Auditor Agents (to check that they are consistent with the authorized execution traces) and can also be used as evidence in case of legal dispute.

Two significant design choices have been made in PRIAM: *minimality* and *separation of issues*:

- The project has focused on the needs arising from the legal analysis and proposed the minimal technical setting to reach its goal. *Minimality* is a pre-requisite in this context, both with respect to the natural language used to communicate with the users (to minimize the risks of misunderstanding by a subject or controller) and with respect to the mathematical model (to minimize the risk of misunderstanding or rejection of the elements of proof by legal experts in case of litigation).
- The *separation of issues* reflects the legal position of isolating privacy from economical issues: according to this view, personal data are not considered

as assets for bargaining but values to be protected independently of any other consideration. As a result, Subject Agents behave as ``Privacy Monitors" in charge of controlling all disclosures of data, but strictly limited to this role.

More details on the technical issues can be found in (Le Métayer, 2008). As a concluding remark, we would like to emphasize the need for a pragmatic approach to privacy protection. As far as consent is concerned, we should consider objectively the two options facing us:

1. Either we refrain from resorting to Privacy Agents and stick to the rule that subjects should give their consent before each single disclosure of personal data; the likely result will be that, overwhelmed by repeated requests for consent, individuals will end up accepting systematically and thus giving up any privacy protection.

2. Or we accept the risk of delegating our consent to a Privacy Agent which meets strong legal and technical requirements, even though we are aware of the fact that software may contain bugs and the risk of mistake is not null.

At the end of the day, the choice is a matter of risk analysis, and the main conclusion of our study is that risks are greater if we choose the first option: if the technical and legal frameworks are designed with the utmost care, Privacy Agents can efficiently contribute to improve the protection of our privacy rights. In addition to the methods and tools proposed by the computer science community for the design of trustable software (and their verification), we believe that the emergence of certification mechanisms could be instrumental to the development of valid and widely accepted Privacy Agents (Cranor & Reidenberg, 2002)[23].

Acknowledgements: This work has been funded by the INRIA Collaborative Research Action PRIAM (PRivacy Issues in AMbient intelligence).

References

1. Bennet, C. J. (1992). Regulating Privacy, Cornell University Press, New York, Ithaca.
2. Bianca, C.M. & Busnelli, F. (2007). La protezione dei dati personali, Padova: Cedam.
3. Bibas, S. (1994). A contractual approach to Data Privacy, Harvard J. Law & Pub. Pol, 591.
4. Bygrave, L.A. (2000) Where have all the judges gone ? Reflections on judicial involvement in developing data protection law, Privacy Law & Policy Reporter, 2000, volume 7, 11-14, 33-36.
5. Bygrave, L.A. (2001) Electronic Agents and Privacy: a Cyberspace Odyssey 2001, International Journal of Law and Information Technology, volume 9, (Issue 3), 275-294.

[23] This position is consistent with the European Commission First Report on the Implementation of the Data Protection Directive 95/46/EC, COM (2003) 265 of the 15th of May 2003, which promotes the use of Privacy Enhancing Technologies and encourages the development of certification schemes. The Communication from the Commission to the European Parliament and the Council of the 7th of March 2007 COM (2007) 87 reiterates the promotion of Privacy Enhancing Technologies.

6. Borking, J. J. (2000) Privacy Incorporated Software Agent (PISA): proposal for building a privacy guardian for the electronic age, Proceedings of the conference “Anonymity 2000”, Springer Verlag, LNCS 2009, 130-140.
7. Cissée, R. & Albayrak, S. (2007) An Agent-Based Approach for Privacy-Preserving Recommender Systems, Proceedings of the AAMAS Conference, ACM.
8. Cohen, J. E. (2003) "DRM and Privacy" . Berkeley Technological Law Journal, Vol. 18, p. 575-617.
9. Cranor, L. & Reidenberg, JR. (2002) Can user agents accurately represent privacy notices? From http://ssrn.com/abstract=328860
10. Dahiyat, E.A.R. (2006). Intelligent agents and intentionality: should we begin to think outside the box? Computer Law and security Report, volume 22 (Issue 6), 472-480.
11. Finocchiaro, G. (2003). The conclusion of the electronic contract through software agents. A false problem? Brief considerations. Computer and security Report, volume 19 (Issue 1), 20-24
12. Forray, V. (2007). Le consensualisme dans la théorie générale du contrat, Paris: Librarie généraoe de droit et de jurisprudence (LGDJ).
13. Fragale Filho, R. & Jeffery, M. (2003) Information technology and workers’ privacy: notice and consent, Comparative Labour Law and Policy Journal, volume 23, 4, 551-568.
14. Friedewald, M., Vildjiounaite, E., Punie, Y. & Wright, D. (2007). Privacy, identity and security in ambient intelligence: a scenario analysis, Telematics and Informatics, 24, 1.
15. Gentot, M. (2002). La protection des donnes personnelles à la croisée des chemins. La protection de la vie privée dans la société d’information, Volume I, Paris: Presses Universitaires de France.
16. ISTPA (2002), ISTPA (International Security Trust and Privacy Alliance) privacy framework, Version 1.1, Technical Report.
17. Joly-Passant, E. (2006). L’ecrit confronté aux nouvelles technologies, Paris: Librarie généraoe de droit et de jurisprudence (LGDJ).
18. Jurewitz, A. (2006) Report on Legal Issues of software agents, Legal IST, from http://193.72.209.176/projects/P1086/D14%20Legal%20issues%20in%20Software%20Agents%20Final.pdf.
19. Kleve, P. & De Mulder, R. (2007), Privacy protection and the right to information: in search of a new balance. Computer Law and security Report, volume 24 (Issue 3), 223-232.
20. Kosta, E., Zibuschka, J., Scherner, T., Dumortier, J. (2008) Legal considerations on privacy-enhancing Location based Services using PRIME technology, Computer Law and Security Report, Volume 24, 139-146.
21. Langheinrich, M. (2002), A privacy awareness system for ubiquitous computing environments, Proceedings of the Ubicomp Conference, Springer Verlag LNCS 2498, 237-245.
22. Le Métayer, D. (2008). A formal privacy management framework. http://pop-art.inrialpes.fr/people/lemetayer/
23. Litman, J. (2000). Information Privacy/Information Property, 52 Standford. L.R.
24. Mell, P. (1996) Seeking shade in a land of perpetual sunlight: Privacy as Property in the electronic wilderness, Berkley technical Law Journal, volume 11 (issue 1);
25. Messinetti, D. (1998). Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali, Rivista critica di diritto provato, Napoli, Jovene.
26. Pearson, S. (2002) Trusted Agents that Enhance User privacy by self-profiling, HP Laboratoies 196, from http://www.hpl.hp.com/techreports/2002/HPL-2002-196.html
27. Poullet, Y. (1991). Le fondement du droit à la protection des données nominatives: proprietés ou libertés, Nouvelles technologies et propriété, Montreal, Thémis.

28. Poullet, Y. & Dinant, J. M. (2006) The Internet and private life in Europe: Risks and aspirations The Internet and private life in Europe: Risks and aspirations. New dimension in Privacy Law, 60-90, Cambridge University Press.
29. Poullet, Y. (2006a). ICT and co-regulation: towards a new regulatory approach? Starting points for ICT regulation, Information Technology & Law series, Volume 9, 247-259.
30. Poullet, Y. (2006b). The Directive 95/46/EC: ten years after, Computer Law and Security Report (Issue 22), 206-217.
31. Rossler, B. (2005). The value of privacy, Polity Press, Cambridge.
32. Rouvroy, A. (2008). Privacy, data protection and the unprecedented challenges of ambient intelligence, Studies in Ethics, Law and Technology, Berkley Electronic Press
33. Rouvroy, A. & Poullet, Y. (2008) The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy, Springer Verlag.
34. Schuck, P.H. (1994). Rethinking Informed Consent, 103 Yale L. J.
35. Schwartz, P. M. (2004) Property, Privacy, and Personal Data. Harvard Law Review, Vol. 117, Volume 7, p. 2055
36. Sica, S. & Stanzione, P. (2005). La nuova disciplina della privacy, Torino: Giappichelli.
37. Solove, D. (2004). The digital person, Technology and privacy in an Information Age, Harvard University Press
38. Stuurman, K. & Wijnands, H. (2001). Intelligent agents: a curse or a blessing? A survey of the legal aspects of the application of intelligent sofware systems, Computer Law and security Report, volume 17, (Issue 2), 92-100.
39. Veldhuisen, A. & Kohras, M. et. al. (2007) Analysis of privacy principles: making privacy operational, ISTPA International Security Trust and Privacy Alliance, Technical Report.
40. Zeno Zencovich, V. (1997). Il consenso informato e la autodeterminazione informativa nella prima decisione del Garante, Milano: Corriere Giuridico.
41. Warren, S. & Brandeis, L. (1890). The right to privacy, Harvard Law Review, 193-220.
42. W3C Consortium (2002) Platform for Privacy Preferences P3P, W3C Recommendation, www.w3.org.

Opinions of consultative bodies and surveys

43. Article 29 Data Protection Working Party, Opinion 5/2004, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf
44. Article 29 Data Protection Working Party, Opinion 114/2005, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.
45. Article 29 Data Protection Working Party, Opinion 2/2008, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf.
46. European Commission, Communication to the European Parlament and the Council on the follow-up of the Work programme for better implementation of the Data Protection directive, COM (2007) 87 final of 7th March 2007, from http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf
47. Flash Eurobarometer Survey on Data Protection in the EU, 226, Controllers' perceptions (2008), from http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf