Addressing Temporal Aspects of Privacy-Related Norms

Guillaume Piolle, Yves Demazeau

Addressing Temporal Aspects of Privacy-Related Norms

Guillaume Piolle[1] and **Yves Demazeau**[2]

Abstract. Agents interacting in open environments such as Internet are often in charge of personal information. In order to protect the privacy of human users, such agents have to be aware of the normative context regarding personal data protection (applicable laws and other regulations). These privacy-related norms usually refer to deadlines and durations. To represent these regulations, we introduce the Deontic Logic for Privacy; this logic represents privacy-related obligations while providing the required temporal expressiveness.

1 INTRODUCTION

Any personal agent designed to evolve in an environment like Internet and to assist a human user with her online activities should then be aware of privacy issues and regulations, in order to protect the user's personal information. These regulations appear as laws, contracts, company policies, user requirements... Six dimensions have been identified that can be used to analyze regulations dealing with personal data protection [7, 6]. These are *user information*, *user consent*, *data update*, *justification of data collection and usage*, *data retention* and *data forwarding*.

Many privacy-enhancing technologies, protocols and architectures try to address parts of the issue [4]. The Platform for Privacy Preferences (P3P), for instance, aims to deal with the first two dimensions, by providing websites with means to communicate on their privacy policies [9]. However, none is able to provide a cognitive agent with means to reason on the regulations themselves, so that it could adapt to the context of a transaction in a dynamic and autonomous fashion.

In this paper, we propose a logic designed in order to specifically represent privacy-related regulations concerned with all six dimensions. This Deontic Logic for Privacy (DLP) is able to deal with obligations regarding personal data processing and its temporal organization. We explain why specific operators are needed to represent dated norms, we identify the requirements for expressing obligations with deadlines, we build such an operator on the base of existing propositions and we put it in the context of privacy norms.

2 THE DLP LOGIC

When dealing with privacy management, norms are often linked with notions of delays, deadlines, precedence between actions; an explicit representation of time would then provide valuable reasoning means. Much work has been done on temporal deontic logics in general [1], but to the best of our knowledge none of them deals with privacy-related norms in a specific way. A prominent temporal feature of privacy regulations is the notion of deadline. We will examine how existing proposals can be of use in privacy-based reasoning, but we must first introduce a common formalism to compare them. This is why, in the light of this background, we present here the DLP language, a temporal deontic logic able to represent specific privacy-related norms, and in particular the deadlines associated to them.

DLP is a language where the SDL obligation modality Ob is freely mixed with LTL operators. The well-formed formulae φ of the DLP language are defined as follows, where p is a proposition from a language $\mathcal{L}_{DLP}$ to be specified later:

$$\begin{aligned}\varphi = \; & p \mid \varphi \text{ “}\vee\text{” } \varphi \mid \text{“}\neg\text{” } \varphi \mid \text{“}Ob\text{” } \varphi \\ & \mid \varphi \text{ “}\mathcal{U}\text{” } \varphi \mid \varphi \text{ “}\mathcal{S}\text{” } \varphi \,;\end{aligned} \tag{1}$$

We have chosen the $\mathcal{U}$ $\mathcal{S}$ temporal language ($\mathcal{U}$ and $\mathcal{S}$ being the strict versions of "until" and "since" connectives) for its expressiveness, but we will use the common abbreviations F, G, H, P. We also define $\mathcal{U}^-$ and F^- as the loose versions of $\mathcal{U}$ and F including the present. The X^i operators, based on a "neXt" operator X and its counterpart in the past X^{-1}, can be used to travel step-wise along a time flow. The DLP logic is interpreted over bidimensional Kripke-like structures, where a world is defined by its *history* h (the linear flow of time it belongs) and a *date* t_i in the time flow. The temporal accessibility relation relates a world in a history to its successor in the same history, and the deontic accessibility relation relates a world to all its acceptable deontic alternatives (in all histories).

3 OBLIGATIONS WITH DEADLINES

We have said that in order to express privacy-related norms, we need the notion of deadlines, to which obligations will be attached. Indeed, it is often argued that obligations without deadlines are void [3]: one can not fulfill them, and yet never be in violation of a norm (since one can always postpone and pretend the obligation will be fulfilled later). In order to deal with deadlines, we introduce specialized constants in our language, which we call *dated propositions*. They are noted $\{\delta_i\}_{i\in\mathbb{N}}$, δ_i being true only at date t_i.

Our aim here is to build an operator $Ob(\varphi, \delta)$ expressing the obligation for φ to be true before the date represented by δ (*i.e.* before the propositional date δ becomes true). We have identified six requirements that an operator in our formalism should meet in order to bear the right meaning in privacy-related norms:

1. Failed obligations should be dropped after the deadline;
2. Violations should be made punctual, not persistent in time;
3. Deadlines that are not dated propositions have no meaning;
4. Obligations on $\bot$ should be impossible to fulfill;
5. Obligations on $\top$ should be trivially respected;

[1] Université Joseph Fourier, Laboratoire d'Informatique de Grenoble, France, email: guillaume.piolle@imag.fr

[2] CNRS, Laboratoire d'Informatique de Grenoble, France, email: yves.demazeau@imag.fr

6. It should be impossible to express obligations with past deadlines;
7. The operator must comply with the propagation principle [2], saying that an obligation must be maintained until the deadline is reached or the obligation is fulfilled;
8. The operator must comply with the monotony principle [2], saying that an obligation with a given deadline implies an obligation with a further deadline.

Some work has been done already on obligations with deadlines; our first six requirements regard choice points already discussed by Dignum *et al* [5]. However, our conclusions slightly differs from theirs, for instance on the fact that they take violation as a state rather than as an event. In their own work, they introduces an operator that defines an obligation jointly with its violation. Because of their strictly temporal definition, dated obligations can then be derived whenever they seem to be respected, which is a significant drawback for us. From another point of view, it is not monotonic and deadlines with a value of $\top$ can be defined, resulting in an immediate obligation. Brunel *et al* [2] extend a temporal deontic logic with explicit quantification on time, in order to reason on delays rather than on deadlines. For that reason, it cannot be directly expressed in DLP. Furthermore, it is not monotonic.

The operator proposed by Demolombe *et al* [3], although not expressed in temporal deontic logic, can be translated. It satisfies some kind of semi-monotony, ensuring the property provided that the obligation is not violated. This key property makes it our best candidate. The operator matches most of our other requirements, but needs to be adapted to dated propositions in order to comply with the third and sixth points. We integrate these conditions to a DLP translation of the original proposition, and end up with the dated operator $Ob(\varphi, \delta)$ (2). The authors propose a persistent violation for their operator; we transform it into a punctual one (3) in order to match our second requirement. One can see that semi-monotony has a nice side-effect: it prevents us from deriving multiple violations for the same initial obligation, while still ensuring monotony if the obligation is fulfilled.

$$Ob(\varphi, \delta) \stackrel{def}{=} \begin{cases} F(\delta \wedge G\neg\delta \wedge H\neg\delta) \\ Ob(F^{-}(\varphi \wedge F\delta))\, \mathcal{U}^{-}\ (\varphi \vee \delta) \end{cases} \tag{2}$$

$$\text{viol}(\varphi) \stackrel{def}{=} \delta \wedge P(Ob(\varphi, \delta) \wedge \neg\varphi\, \mathcal{U}^{-}\delta) \tag{3}$$

4 APPLICATION TO PRIVACY NORMS

Our deontic and temporal formalism can be used to express privacy-related norms by its application on a base language $\mathcal{L}_{DLP}$. $\mathcal{L}_{DLP}$ is based on predicates related to the six dimensions of personal data protection mentionned in the introduction. Argument domains are finite or countable sets, so we end up with a countable set of propositional terms. $\mathcal{L}_{DLP}$ includes for instance a predicate *perform* representing the actual process involving personal information, a predicate *consent* representing the user's authorization, a predicate *forget* representing data deletion[3]...

As an application, let us see how the an example regulation about data retention (*One must not keep somebody else's credit card number more than one week after a transaction*) translates into DLP (4). It is an interesting example since it involves antecedence and a deadline. Formally, it says that whenever an agent A performs a process of type `transaction` to which is attached an information of type `creditCardNum` owned by an agent B (and not by agent A), if δ represents a date one week in the future, then there is a dated obligation that A should forget this information before the deadline δ.

$$\begin{array}{l} \textit{perform}(\text{A}, \text{ID}) \wedge \textit{owner}(\text{ID}, \texttt{creditCardNum}, \text{B}) \\ \wedge\neg\textit{owner}(\text{ID}, \texttt{creditCardNum}, \text{A}) \\ \wedge\ \textit{actiontype}(\text{ID}, \texttt{transaction}) \wedge X^{7*24}\delta \\ \quad \rightarrow Ob(\textit{forget}(\text{A}, \text{ID}, \texttt{creditCardNum}), \delta) \end{array} \tag{4}$$

5 CONCLUSION AND FUTURE WORK

We have proposed the DLP language, based on temporal deontic logic, to represent privacy-related norms. DLP is expressive enough to represent obligations with deadlines, as well as other (more classical) temporal notions, in an acceptable way. DLP is based on a propositional language specifically oriented towards personal data processing. Some work remains to be done on this logic, including a better basis for the temporal operators of the language. Currently, it is based on the $\mathcal{U}, \mathcal{S}$ logic, which is very general but somewhat too expressive. Indeed, we must then question inclusion of "since" in the logic, since we do not seem to need it, and it has already been argued that adding it to an until-based logic is not trivial from the point of view of complexity [8]. An automated procedure is to be proposed to generate DLP formulae on the basis of information exctracted from P3P policies [9]. DLP, along with these associated tools, are then to be integrated in a privacy-aware cognitive agent that should be able to model and reason on its privacy-related normative context.

ACKNOWLEDGEMENTS

This research has been supported by the Rhône-Alpes region Web Intelligence project. We would also like to thank Andreas Herzig and Philippe Balbiani for their valuable comments on our work.

REFERENCES

[1] Lennart Åqvist, 'Combinations of tense and deontic modalities', in *7th International Workshop on Deontic Logic in Computer Science (DEON 2004)*, eds., Alessio Lomuscio and Donald Nute, volume 3065 of *LNCS*, pp. 3–28, Madeira, Portugal, (2004). Springer.

[2] Julien Brunel, Jean-Paul Bodeveix, and Mamoun Filali, 'A state/event temporal deontic logic', in *Eighth International Workshop on Deontic Logic in Computer Science (DEON'06)*, number 4048 in LNCS, (2006).

[3] Robert Demolombe, 'Formalisation de l'obligation de faire avec délais', in *Troisièmes journées francophones des modèles formels de l'interaction (MFI'05)*, Caen, France, (2005).

[4] Yves Deswarte and Carlos Aguilar-Melchor, 'Current and future privacy enhancing technologies for the internet.', *Annales des Télécommunications*, **61**(3-4), 399–417, (2006).

[5] Frank Dignum, Jan Broersen, Virginia Dignum, and John-Jules Meyer, 'Meeting the deadline: Why, when and how', in *Third International Workshop on Formal Approaches to Agent-Based Systems (FAABS'04)*, eds., Michael G. Hinchey, James L. Rash, Walt Truszkowski, and Christopher Rouff, pp. 30–40, (2004). Springer Verlag.

[6] Guillaume Piolle and Yves Demazeau, 'Une logique pour raisonner sur la protection des données personnelles', in *16e congrès francophone AFRIF-AFIA sur la Reconnaissance de Formes et l'Intelligence Artificielle (RFIA'08)*, Amiens, France, (2008). AFRIF-AFIA.

[7] Guillaume Piolle, Yves Demazeau, and Jean Caelen, 'Privacy management in user-centred multi-agent systems', in *7th Annual International Workshop "Engineering Societies in the Agents World" (ESAW 2006)*, eds., Gregory O'Hare, Michael O'Grady, Oguz Dikenelli, and Alessandro Ricci, pp. 354–367, Dublin, Ireland, (2006). Springer Verlag.

[8] Mark Reynolds, 'The complexity of the temporal logic with until over general linear time', *Journal of Computer and System Sciences*, **66**(2), 393–426, (2003).

[9] World Wide Web Consortium. Platform for Privacy Preferences specification 1.1. `http://www.w3.org/P3P/`.

[3] Due to page limitations, we are not able to include the full specifications of $\mathcal{L}_{DLP}$ here.