TOWARDS A CONCEPTUAL FRAMEWORK FOR DIGITAL DOSSIER MANAGEMENT IN CRIMINAL PROCEEDINGS

Martin Apistola, Martijn Warnier, Frances Brazier, Anja Oskamp
VU University Amsterdam
De Boelelaan 1105 Amsterdam
The Netherlands
m.apistola@rechten.vu.nl, warnier@cs.vu.nl, frances@cs.vu.nl, a.oskamp@rechten.vu.nl

ABSTRACT
The use of digital dossiers by the Public Prosecution and Courts is an example of how technology will change today's law practice. The potential has been experienced in pilot projects in Amsterdam and Rotterdam. The legal, organisational and technological requirements, however, are numerous: sensitive data is acquired from distributed sources; consistency and completeness need to be guaranteed. This paper proposes a conceptual framework for digital dossier management, based on the use of dedicated software agents. To this purpose a number of underlying taxonomies are introduced: for the data, the dossier management processes, software agents and distributed environments.

KEY WORDS
Legal document processing, digital dossier, criminal proceedings, agent technology, taxonomies.

1. Introduction

The use of digital dossiers by the Public Prosecution and Courts is an example of how technology changes today's law practice [1]. Digital dossiers, prepared by the Public Prosecutor, are shared by the judge(s), the Public Prosecutor, the Defence and the clerks involved. (Note that their notes are not necessarily shared; each of these parties decides whether and with whom to share his/her notes). Currently the digital dossier is based on paper versions of relevant files: these files are scanned and stored as pdf-files in the digital dossier [2]. A web-based user interface allows a user to access the digital dossier. In the future the digital dossier will also contain XML (parsable) content and include multi-media material (sound, images and video).

Digital dossiers are challenging because of the many requirements: legal, technological and organisational. Not only do the dossiers contain much sensitive data but they are also part of a large-scale distributed environment. In this environment different data sources are distributed both physically and across organizations that need to work together within fixed boundaries set by the law to manage a dossier.

Agent technology is a promising technology for large-scale distributed environments and supports modularity, security and scalability in these environments. Dedicated software agents make it possible to clearly separate tasks, responsibilities and integration of new functionalities.

This paper proposes a conceptual framework, based on a taxonomy of core elements of digital dossier management viz. data in the dossier and dossier management processes, but also taxonomies of software agents and distributed environments [3]. The conceptual framework indicates which types of software agents can support which kinds of data, dossier management processes and distributed environments. Different parts of the taxonomy can be used independently or combined in different situations for different purposes. The focus in this paper is on the role of agent technology in relation to dossier management processes and data and on agent technology in relation to distributed environments.

The paper is structured as follows. Section 2 sketches a scenario that briefly explains the context of Dutch criminal proceedings. This scenario is used to illustrate the application of the taxonomies for digital dossier management. Section 3 presents taxonomies for digital dossier management: data in the digital dossier, dossier management processes, software agents and distributed environments. Section 4, the core of the paper, presents a conceptual framework for digital dossier management, relating agents to data, dossier management processes and distributed environments. Section 5 briefly indicates how the taxonomies and conceptual framework can be used by organizations in criminal proceedings and ends with a discussion and conclusions.

2. Scenario

In Dutch criminal proceedings numerous organizations are involved. Criminal proceedings start with a criminal

investigation, usually followed by a trial, a verdict and the execution of a sentence. An example of the Dutch criminal proceedings for a juvenile repeat offender is described below. This same scenario has previously been presented in [2]. This scenario is sketched to briefly explain the context of Dutch criminal proceedings and to illustrate the application of the taxonomies for digital dossier management in the following sections.

A police officer arrests a juvenile suspect for vandalism and escorts him to the police station where an assistant prosecutor questions the suspect. The Police opens a new dossier which contains a summary of the offence for which the suspect is being charged, the date and location of the incident, number of suspects, personal data of the victim, the official police report, and other relevant data. The personal data the suspect has provided is cross-referenced with the municipal database. (Note that in the Netherlands each municipality stores such data for each resident). The Police also queries local repeat offender databases to discover whether this suspect is a known repeat offender.

Because a minor suspect is involved, the Police issues a request to other organizations for juvenile offenders. These organizations provide relevant data about the minor's background. All of this data is added to the dossier. After collecting this data, the Police and the Assistant Prosecutor inform the Public Prosecutor of the case and transfer the dossier. The Public Prosecutor decides whether to press charges or, to pursue an alternative if other (minor) punishment is deemed more suitable. This decision is based both on the current case and the (criminal) history of the suspect. A dedicated Judicial Documentation Database is used to retrieve data on the criminal past of the suspect. Typically, at this point, the Public Prosecutor will again consult Municipal Databases and local Juvenile Repeat Offender Systems. All data is cross-referenced with the case dossier and information is updated when needed.

The Public Prosecutor decides to bring the case to Court. The next mandatory step involves informing the Child Welfare Council of the case. In the Dutch context the Child Welfare Council has the task to investigate the crimes of minors. In addition to the criminal offences of the minor, the family situation and other relevant social factors are taken into account. This results in a motivated advice for suitable punishment of the suspect. This advice is added to the dossier. The prosecutor then summons the suspect and a lawyer is assigned to the juvenile suspect. Adding the summons to the dossier finalizes the dossier at this point. A copy of the dossier is sent to the Court and to the lawyer of the suspect. To check the correctness of the dossier, the presiding judge may query judicial history and other judicial documentation in the Judicial Documentation Database as well as information from Municipal and other databases. At the court session all parties involved use the information in the dossier. The Public Prosecutor demands a suitable sentence, the lawyer presents the defence and ultimately the judge comes to a verdict. The suspect is sentenced and all data regarding the court session is added to the dossier. The dossier itself is filed in Judicial Documentation Database for future reference.

3. Taxonomies

In this section the core elements of digital dossier management are presented: data in the dossier, dossier management processes, software agents and distributed environments. These taxonomies represent one possible classification scheme for each of these elements.

3.1 Data in the Dossier

Digital dossiers contain both sensitive and less sensitive data. Sensitive data may cause damage when illegally used or used in the wrong context. Law usually protects this data. Such sensitive data can only be stored and processed for a specific purpose and task. In the scenario described in the previous section the Police is only allowed to store personal data of suspects that is strictly necessary for its task of tracking down juvenile suspects. Sensitive data can and must only be provided, and processed, by persons and organisations mentioned by law. Less sensitive data is data that may be made available to the general public. Data on, for example, specific legislation that was used in the juvenile scenario can be made available on the Internet for use in similar cases.

The specific data stored in a digital dossier depends on the offence involved. Standard templates can be defined for each type of offence.

3.2 Dossier Management Processes

Important dossier management processes are completeness and consistency checking, controlling access, organizing the dossier, user interaction and physical data protection measures such as back-up procedures.

- **Completeness check [2]:**
  - Determining for which type of offence which data is mandatory;
  - Checking if all the mandatory data is in the dossier.

- **Consistency check [2]:**
  - Checking whether the data for a dossier is consistent with all other data in the dossier;
  - Checking reasonable entries and possible values in data fields.

- **Access control:**
  - Granting rights with regard to the dossier based on specific security policies [1];
  - Checking role based access [4]: who may change existing data in the dossier and create new dossiers;
  - Limiting the access of individuals by checking whether their identity is on a list associated with the dossier [5];
  - Adding meta-data to the dossier on specific human or software agents that may change, read, delete or add information to a dossier.

- **Organizing the dossier:**
  - Adding the right meta-data to the dossier such as the name, author(s) and status of the dossier and its documents;
  - Indexing information in the dossier;
  - Deploying effective retrieval techniques.

- **User interaction:**
  - Inventory aspects of the interface of the digital dossier that define its behaviour;
  - Inventory of user's goals, expectations, behaviours, and needs;
  - Making the dossier's user interface respond to the user's experience.

- **Physical data protection - back ups:**
  - Making an image of the entire dossier or parts of the dossier;
  - Replacing the digital dossier or one or more files without influencing the rest of the dossier while doing so;
  - Comparing old versions of dossiers or parts of dossiers with current versions of dossiers.

3.3 Agent Technology

Software agents are software systems that are (to some degree) autonomous and pro-active, have the ability to communicate with other agents and to react to their environment [6]. They may, in addition, be mobile – able to migrate from one physical location to another, and be able to learn from their interactions with other agents and their environment.

Agent technology provides a means to distribute responsibilities and tasks across the many interacting distributed autonomous systems in criminal proceedings. This makes it possible and easier, compared to the current situation to, for example, find out who took the decision to not make specific information available to the lawyer, according to what rule and on what law are those rules based.

Dedicated software agents can, for example, also be designed to perform the task of guarding consistency of data both within a source, and between sources within the digital dossier, and notifying appropriate (human) parties when needed. With respect to completeness, dedicated agents can monitor the availability of necessary documents in the digital dossier. For instance, a trial cannot start if a copy of the original police report is not in the digital dossier.

Agent technology also offers the possibility for a gradual construction. Initially it is possible to develop agents for relative simple tasks. Subsequently, the complexity of these tasks can gradually be increased. Legal professionals in criminal proceedings can experience their potential. Agents can be developed according to the specific wishes of their users. In the context of criminal proceedings specific and dedicated agents can be developed with the level of security required by their users and can be authorized by their users to only access specific sources.

As a relatively closed environment, the context of the criminal proceedings is a good starting point to gradually explore the use of intelligent agents and their interaction with users in this environment. In the long run, by gradually adding new functionality, responsibilities, suitable security techniques and thereby building trust amongst human users, these agents can be deployed in more open environments such as the Internet for specific types of information.

The following categorization of agent technology represents the functionality needed in, and suited for the domain of criminal proceedings [6]:

- **Authorized authenticated mobile agents:** Authorized authenticated mobile agents are standard equipped with rights to access specific sources. They can identify themselves and they can be linked to their human owner. It is possible to verify whether these agents are who they claim to be. Authorized authenticated mobile agents are equipped with the right credentials. They interact with other agents (and possibly humans) in an agent-communication language. Authorized authenticated mobile agents do not simply act in response to their environment; they are able to exhibit goal-directed behaviour by taking the initiative (i.e. they are pro-active). They take the initiative rather than acting simply in response to their environment [7]. Authorized authenticated mobile agents operate without the direct guidance and intervention of humans or others, and have some level of control over their actions and internal state [7]. They are situated within an environment, can sense the environment, can act on it, over time, in pursuit of their own agenda and so as to effect what it senses in the future [8]. Authorized authenticated mobile agents migrate between organizations.

- **Unauthorized anonymous mobile agents:** Unauthorized anonymous mobile agents cannot

always identify themselves and cannot always be linked to their human owner. They are not automatically equipped with the right credentials. It is possible though to authenticate them by providing them with credentials of, for example, a third party. They interact with other agents (and possibly humans) in an agent-communication language. Unauthorized anonymous mobile agents do not simply act in response to their environment; they are able to exhibit goal-directed behaviour by taking the initiative. They take the initiative rather than acting simply in response to their environment [7]. Unauthorized anonymous mobile agents operate without the direct guidance and intervention of humans or others, and have some kind of control over their actions and internal state [7]. An unauthorized anonymous mobile agent is situated within an environment, senses that environment and acts on it, over time, in pursuit of its own agenda and so as to effect what it senses in the future [8]. Unauthorized anonymous mobile agents can migrate between organizations.

- **Authorized authenticated static agents:** Authorized authenticated static agents can identify themselves and can be linked to their human owner. It is possible to verify whether these agents are who they claim to be. They are standard equipped access rights to specific sources and posses the right credentials. Each organization has complete control of all of its own authorized authenticated static agents. Authorized authenticated static agents perceive their environment, and respond in a timely fashion to changes that occur in the environment [7]. They interact with other agents (and possibly humans) in an agent-communication language.

- **Unauthorized anonymous static agents:** Unauthorized anonymous static agents cannot always identify themselves and cannot always be linked with their user. In case of unauthorized anonymous static agents, organisations administer their own agents. Unauthorized anonymous static agents are not automatically equipped with the right credentials. It is possible though to authenticate them by providing them with credentials of, for example, a third party. Each organization has complete control of all running agents. Unauthorized anonymous static agents perceive their environment, and respond in a timely fashion to changes that occur in the environment [7]. They interact with other agents (and possibly humans) via in an agent-communication language.

3.4 Environments

The digital dossier is part of closed environments, semi-open environments and open environments.

- **Closed environment:** data is only made available to authorized parties within the organisation.

- **Semi-open environment:** data is made available to authorized parties outside of the organisation.

- **Open environment:** data is available to external organisations.

4. A Conceptual Framework for Dossier Management

The potential roles of the different types of agent and environments distinguished in Section 3, in dossier management processes is depicted in Table 1. This table indicates the extent to which the different agents can be expected to support dossier management processes and how well the different agents can be expected to support the various environments:

\+ = Support is available
+/- = Needs some support and
\- = Offers insufficient support

The resulting framework can be used by organizations in criminal proceedings as a starting point and should be refined for specific situations.

Table 1

	Agent Technology			
	Authorized authenticated mobile agents	Unauthorized anonymous mobile agents	Authorized authenticated static agents	Unauthorized Anonymous static agents
Data and dossier management processes				
Check completeness and consistency of sensitive data in the dossier	+/-	+/-	+	-
Check completeness and consistency of less sensitive data in the dossier	+	-	+	-
Back-up	+	+	+/-	+/-
Access control	+	+	+/-	+/-
Organization of the dossier	+/-	+/-	+	+
User interaction	+	+/-	+	+/-
Environments				
Closed environment	+	-	+	+/-
Semi-open environment	+	+/-	+	+/-
Open environment	+	+	+	+

- **Check Completeness and Consistency of Sensitive and Less Sensitive Data in the Dossier:** Completeness and consistency checks of both sensitive and insensitive data can best be assigned to authorized authenticated static agents as on basis of

their authentication and authorization they can be trusted more to act accordingly. This is also true for authorized authenticated mobile agents, although then logging needs to be well regulated for both types of data. Assigning completeness and consistency checks to both types of unauthorized anonymous agents is not advisable, as it is unclear to which organisation responsibility has been delegated.

- **Back-up:** In case of backing-up sensitive and valuable data authentication and authorization are important requirements. Stakeholders need information on or experience with the way agents have successfully back-upped data in the past. Having unauthorized anonymous agents backing-up data is a risk as information about their past actions is not always known and so their future back-up actions are hard to predict. Authorized authenticated mobile agents support the requirement of authentication. Unauthorized anonymous static agents support the requirement of authentication when provided with the right credentials of, for example, a trusted third party.

- **Access Control:** Authentication plays a major role in access control. Authorized authenticated mobile and static agents support this requirement. Unauthorized anonymous agents may, but they will need to provide credentials.

- **Organization of the Dossier:** Agents need to react to changes in their direct environment concerning preferred ways of organizing dossiers. Authorized authenticated static agents meet this requirement the best followed by unauthorized anonymous static agents. Pro-activity is needed to investigate the environment of the dossier and take the initiative in inventory preferences to organize dossiers.

- **User Interaction:** Agents decide for themselves how they interact with human agents, including their owner. Coordination of user interaction between different agents may be needed, requiring additional knowledge to this purpose. There is little difference between the ability of static and mobile agents to communicate with human agents. Interaction with unauthorized anonymous agents may not always be opportune depending on the content.

- **Closed Environment:** A requirement in a closed environment is that the users are able to authenticate agents in that environment. Authorized authenticated static agents and unauthorized anonymous static agents (when equipped with credentials) meet this requirement. Parties in closed environments must know each other in order to access, exchange and process data. Authorized authenticated mobile and static agents meet this requirement in opposite to unauthorized anonymous mobile and static agents, unless they have the right credentials.

- **Semi-open Environment:** In the semi-open environment of criminal proceedings autonomy plays a role that can be supported by authorized authenticated mobile agents and unauthorized anonymous mobile agents. Each organization can have agents that decide for themselves what data to exchange and with whom. In case of sensitive data exchange at least some intervention by human agents remains important. Authorized authenticated static agents and unauthorized anonymous static agents support this requirement. In all cases agents must be relied upon that they can decide for themselves to send specific data to the right organization in criminal proceedings. Authorized authenticated static agents and unauthorized anonymous static agents have the advantage in this environment that their users can control them locally. There are also parties in this environment though that do not necessarily have to control agents locally. In this case authorized authenticated mobile agents and unauthorized anonymous mobile agents are of use. In the semi-open environment of criminal proceedings most parties know each other. In such an environment authorized authenticated mobile agents and authorized authenticated static agents seem to be preferable, especially when exchanging sensitive data. Unauthorized anonymous mobile agents and unauthorized anonymous static agents can be used though to retrieve and exchange the less sensitive data in this environment.

- **Open Environment:** Agents in an open environment do not necessarily need to be controlled by the users in this environment and can have much autonomy in this environment. In some cases authorized authenticated and unauthorized anonymous mobile agents are suited while in other cases authorized authenticated static agents and unauthorized anonymous static agents are suited.

The next section discusses how the framework might be used to assist organizations in criminal proceedings.

5. Discussion and Conclusions

This paper proposes a conceptual framework based on taxonomies for digital dossier management, viz. data in the dossier, dossier management processes, agents and environments.

Taxonomies of the core elements of dossier management can help organizations in criminal proceedings to clarify their needs regarding distributed information processing. This is important, because of the central role dossiers play in criminal proceedings. The. This paper describes how taxonomies for dossier management can be used in criminal proceedings. In future research the taxonomies

need to be further elaborated upon. The various entries of the table should be refined, and where appropriate divided into subcategories. Obviously, the relation between data in the dossier, data management processes and environments also needs to be described.

The conceptual framework, based on the taxonomies, indicates which type of agents may preferably be used to support which kinds of data, processes and environments. Agent technology can support more than one dossier management process, but there is no overview in criminal proceedings of what dossier management processes are important to each organization. It is, however, clear that agent technology should not be used randomly to support dossier management processes. By organizing dossier management processes of organizations in criminal proceedings it becomes clearer which dossier management processes are important to them.

The paper also provides organizations in criminal proceedings a general overview of various means of agent technology support. By making clear distinctions between forms of agent technology support, it becomes easier for organizations in criminal proceedings to select the right type of support.

Acknowledgements

This research is supported by the NLnet Foundation (http://www.nlnet.nl) and is conducted as part of the ACCESS-project (http://www.iids.org/access) funded by the NWO Token program.

References

[1] M. Warnier, F. Brazier, M. Apistola & A. Oskamp. Secure Distributed Dossier Management in the Legal Domain, *Proc. 2nd IEEE International Workshop on Dependability and Security in e-Government*, 2007.

[2] M. Warnier, F. Brazier, M. Apistola & A. Oskamp. Towards Automatic Identification of Completeness and Consistency in Digital Dossiers. *Proc. 11th International Conference on Artificial Intelligence and Law*, ACM Press, 2007.

[3] M. Apistola & A.R. Lodder, Law firms and IT. Towards optimal knowledge management, *Journal of Information, Law and Technology*, (2), 2005.

[4] R. Sandhu, E. Coyne, H. Feinstein, C. Youman, Role-Based Access Control Models. *Computer*, 29(2), 1996, 38–47.

[5] C. Kaufman, R. Perlman & M. Speciner, *Network security, private communication in a public world* (Prentice Hall, 2002).

[6] N.R. Jennings & M. Wooldridge. Intelligent agents: Theory and practice, *Knowledge Engineering Review*, 1995.

[7] H.S. Nwana. Software agents: An overview, *Knowledge Engineering Review*, 11(3):1–40, September 1996.

[8] A. Graesser & S. Franklin. Is it an agent, or just a program?. A taxonomy for autonomous agents, *Proc. 3rd International Workshop on Agent Theories, Architectures, and Languages*, 1996.