MyMemory: an ontology for privacy protection in external digital memories

Completed Research

Bianca Rodrigues Teixeira
Federal University of the State of Rio de Janeiro
bianca.teixeira@uniriotec.br

Flavia Maria Santoro
Federal University of the State of Rio de Janeiro
flavia.santoro@uniriotec.br

Fernanda Araujo Baião
Federal University of the State of Rio de Janeiro
fernanda.baiao@uniriotec.br

Abstract

Every day, over one billion people actively use some social network or social media, sharing opinions, describing facts they believe, and detailing moments of their lives online. In some way, we are digitizing part of our lives and, thus, creating an external collective digital memory in which the issue of privacy is central. We propose to address the privacy issue of digital memories by applying conceptual modeling and semantic web technologies. For that, we built MyMemory, an ontology for the broad concept of digital memory that includes the concept and associated rules to address private memory associated to the context in which it was produced.

Keywords

Digital memory, privacy, ontology.

Introduction

In the past few years, technology has experienced some major advancements; but as a result, some important consequences could be observed in daily life. For example, every day, over one billion people actively use some social network or social media (like Facebook¹), sharing opinions, describing facts they believe, and detailing moments of their lives online (Facebook reports, 2015); and all this data has been stored and can be revisited on demand. In some way, we are digitizing part of our lives and, thus, creating an external collective digital memory in which the issue of privacy is central, especially for the Information Systems (IS) research area. Acquisiti and Gross (2008) performed a study and found that a minimal percentage of Facebook users change the default privacy settings. Nevertheless, information posted online has been used with many purposes that could be considered as invasion of privacy.

According to The Guardian², a growing number of companies observe the behavior of its employees in social networks, through diverse surveillance devices and even private messaging apps, both for hiring and throughout their employment relationship. However, what they want to know has little to do with work. They are really searching for religious and political positioning, connections with organized crowds, embarrassing content photos and manifestations of intolerance or prejudice. Eavesdropping systems specialize in monitoring workplace chats such as Slack³ and Yammer⁴ to identify, among other issues, “intentional and unintentional harassment, threats, intimidation”. The report states that “connecting the dots between a person’s work life and personal life can lead to uncomfortable territory”, as the example cited by one insider at a consulting firm that aims to prevent fraud among bankers by watching their Facebook pages. The scenario is a trader who had just changed his relationship status from married to

¹ www.facebook.com.br
² https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology
³ https://slack.com
⁴ https://www.yammer.com/
divorced, the expense of which “could put that person under pressure to commit fraud or steal”.

Research on this topic provides evidence of the privacy issue. Developments in workplace surveillance technologies have made it easier for employers to track, monitor, and access employees’ online activities (Ciocchetti, 2011; O’Connor, 2016). Zou (2017) states that the quantity and extent of data generated and shared on social networks have become a precious resource for employers to monitor work performance and look into employee misconducts. In this sense, policies and protection laws have been discussed and delivered. However, we argue that it should be also addressed in the context of IS development.

We propose to address the privacy issue of digital memories by applying conceptual modelling and semantic web technologies. For that, we specified, codified and illustrated the use of an ontology for the broad concept of digital memory that includes the concept of private memory associated to the context in which it was produced. MyMemory Ontology was built as an extension of the work described in Rodrigues et al. (2017). The main use of the ontology is to automatically detect situations in which the owner of a certain piece of memory would not wish to share it with a particular entity. Our ontology encompasses logic axioms to support inferring whether the entity that wants to access the owner’s memory should have access or not to that memory. Therefore, we rely on inferences to protect the user’s privacy.

This paper is structured as follows. Section 2 presents background knowledge: a brief concept of memory, privacy and ontologies; Section 3 describes MyMemory, the formal definition of the ontology; Section 4, discusses it in the light of an application scenario; and, Section 5 concludes the paper and presents future perspectives of this research.

Research Background

Memory

Le Goff (1990), a French historian, claims that memory relates to an individual and psychological event which allows humans to update past impressions or information they previously had. Megill (2004) defines memory as “... an image of the past constructed by a subjectivity in the present.” The operations related to memory – the acts of remembering and forgetting – undergo an ontological shift with a possibility of also representing and recording both thoughts and speech established within social groups as an extension of itself, through the modeling, construction, and organization of external memories.

Rodrigues et al. (2017) state that collective memories result from the interactions between individuals, the past and present reality. Individuals are the providers of their own memories, which are collected and manipulated. The processes of collective memory production are diverse and transformed over time according to the social experience and the technological devices of that context. So, the creation of digital memories occurs through various processes, through social networks on the web, applications, surveillance cameras in public and private space, closed systems, content production, GPS, cookies, digital traces, among many others. The production of the memory operates in “real-time” or “online” both in individual and in collective layer. Thus, digital memory can provide relationships between individual and collective memories, and might subvert ontological experiences, such as the processes of remembering and forgetting, as well as cultural, social, economic, political, historical, and other issues.

Privacy of the Digital Memory

According to Solove (2008), an expert in privacy law, for ages people have debated issues of privacy, ranging from gossip to surveillance. “Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations.”

Privacy on social networks is a complex concept which involves major challenges since many studies indicate that the existing privacy systems as well as their designs must be improved to better address threats and meet users’ expectations (Raad and Chbeir, 2013). For these authors, privacy has been related to network anonymization, privacy preservation, and access control; however, these conventional techniques have several disadvantages and network users lack appropriate means to efficiently control and protect their published data. Thus, the risk of revealing personal and sensitive information is critical.
Krishnamurthy and Wills (2008) investigated the issue of privacy affirming that users are encouraged to share a variety of personal identity-related information, including physical, mental, cultural, and social attributes; and they frequently believe that such information is accessible to their friends on that social network. However, the set of entities that can have access to private information is large and diverse: third-party advertisers and data aggregators, members in the social network who are not friends of the user, and external applications. For these authors, traditional privacy protection policies are not efficient, because limiting access to just friends or those in a network is not fine-grained enough. They proposed to match what information a user makes available with what is needed by other users and applications, comparing to techniques to protect privacy leakage to third-party domains for traditional Web sites. We argue that only policies are not enough, systems should automatically recognize a possible privacy invasion. The technology should make unattainable for that users’ private moments to be violated.

**Ontology**

The word “ontology” has been largely used in the literature with different meanings in different communities. In the Philosophical sense, "Ontology" accounts for the branch of philosophy which deals with the nature and structure of "reality", focusing on the nature and structure of things per se and their description in terms of general categories and relations independently of any further considerations or their actual existence. In a computational sense, on the other hand, an ontology refers to an information object (computational artifact) typically used as a means to formally model the structure of a system (i.e., the relevant entities and relations that emerge from its observation, and which are useful to our purposes) (Guarino et al, 2009). Still according to Guarino et al. (2009), the backbone of an ontology consists of a taxonomy of concepts: "For appropriate usage, ontologies need to fulfill a further function, namely facilitating the communication between the human and the machine – referring to terminology specified in the ontology – or even for facilitating inter-machine and inter-human communication".

In this latter (more pragmatic) computational sense, an ontology has been commonly (and yet still informally) defined as a "formal, explicit specification of a shared conceptualization" (Studer et al., 1998). Particularly in the context of Semantic Web, an ontology is referred to as a description of a domain theory for the explicit representation of the semantics of the data (Gontier, 2015), providing formal conceptualizations. The final goal of a computational ontology is to become a model in its domain. As a computational artifact, it is composed of several elements, such as classes, object properties (relationships between classes), data properties (or attributes), axioms (which define logical rules that generate inferences) and individuals (instances of classes). It is commonly specified using the UML\textsuperscript{5} language and codified in OWL\textsuperscript{6} language, on top of editing tools such as Protégé\textsuperscript{7}.

Rodrigues et al. (2017) proposed a preliminary ontological model to represent only the concept of external digital contemporary memory; however, it was not concerned with discussions about the use of such memories, not even with privacy concerns about it. The objective of the present work is to build an ontology about the domain of memory, extending the ontology from Rodrigues et al. (2017) so as to address privacy issues of an individual’s piece of memory. Next section presents this domain ontology.

**MyMemory Ontology**

In Social Networks, we observe that people's digital memories are composed of photos, videos and textual posts captured by one of the participants of the event. MyMemory Ontology intends to establish a formal and broad concept for it. We are interested in securing individual memories, identifying the context of one particular piece of memory, and moreover, in establishing boundaries able to distinguish what should be public and what should be private (Teixeira et al., 2017). In this sense, we extended the ontology of Rodrigues et al. (2017) to include new classes and relationships to help secure somebody’s pieces of memories based on a current Situation, focusing on the concept of Individual Memory.

Figure 1 graphically represents the ontology organized in a UML Class Diagram. The general idea is that a **Person** may own several **IndividualMemories**. Each **IndividualMemory** occurs (isSetIn) in a

---

\textsuperscript{5} http://www.omg.org/spec/UML/About-UML/

\textsuperscript{6} https://www.w3.org/OWL/

\textsuperscript{7} http://protegeproject.github.io/
Location under a particular Situation (more specifically, an IndividualMemory plays the role of a Focus that characterizes a specific Situation, or a state of affairs in reality). A Situation can be explained by (is composed by) a set of ContextualElements. An IndividualMemory might also be related to an EmotionalState that belongs to its owner’s PsychologicalCondition (Happy, Nervous and Hesitant are examples of specific subtypes of PsychologicalCondition). EmotionalState of a Person is a composition of its PsychologicalConditions (for example, Peter may be feeling both anxious and happy about his scheduled date with Mary). An EmotionalState of someone may be classified as either being a RelaxedState or a StressfulState, based on his/her PsychologicalConditions. The subclasses of EmotionalState identify how the memory’s owner feels, which will contribute to decide whether a particular memory should be shared or not. So, although we have defined only Relaxed and Stressful states, there can be more. Also, a Person may want to access an IndividualMemory of a different owner.

We take Focus as the IndividualMemory currently under analysis regarding privacy issues. A Situation characterizes a Focus. For the same piece of memory (IndividualMemory) being analyzed, there may be several Focuses and Situations. Situation is composed of ContextualElements, which are the details about circumstances under which the IndividualMemory was produced (for example, the first kiss she had with her former boyfriend). A set of rules state three possible ContextualElements.

![Figure 1 - Visualization of the concepts of the MyMemory Ontology](image)

Table 1 defines the object properties present in the ontology. Each object property has a domain and a range of values, as well as its inverse property. Domain is the class in which the property is defined, while range is the class to which the property points to (for example, all the objects from class EmotionalState possess a property named "belongs to", pointing to the Person that experiences it; that is, an EmotionalState belongs to a Person). The inverseOf stands for the inverse property of its counterpart property, that is, another property with domain and range inverted from the original property ("experiences" stands for the inverse of "belongsTo", meaning the Person that experiences the EmotionalState). If any two properties a and b are disjoint, it means that no individual x can be connected to individual y through both a and b properties at the same time.

There is only one Data Property, which is "meaning". It is a property for the Location class and it is a string. It creates semantic for a certain location (for example, "at Mary's house" or "at the zoo"). Moreover, the proposed ontology encompasses 13 rules that specify the semantics of the ontology concepts more precisely. The rules represent the core of our ontology regarding its intended use, i.e., the characterization of customizable situations in which a memory should automatically be kept private from some entity that wants to have access to it. Each rule is presented as follows, both in a textual description and in Semantic Web Rule Language® (SWRL). SWRL is a language that can be used to express rules based on description...

---

8 https://www.w3.org/Submission/SWRL/
logics, combining OWL DL or OWL Lite with a subset of the Rule Markup Language.

<table>
<thead>
<tr>
<th>Object Property</th>
<th>Domain</th>
<th>Range</th>
<th>Inverse Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>belongsTo</td>
<td>EmotionalState</td>
<td>Person experiences</td>
<td>experiences</td>
</tr>
<tr>
<td>characterizes</td>
<td>Situation</td>
<td>Focus</td>
<td>isCharacterizedBy</td>
</tr>
<tr>
<td>experiences</td>
<td>Person</td>
<td>EmotionalState</td>
<td>belongsTo</td>
</tr>
<tr>
<td>feels</td>
<td>Person</td>
<td>PsychologicalCondition</td>
<td>isFeltBy</td>
</tr>
<tr>
<td>hasPart</td>
<td>Person</td>
<td>PsychologicalCondition</td>
<td>part of</td>
</tr>
<tr>
<td>isCharacterizedBy</td>
<td></td>
<td></td>
<td>characters</td>
</tr>
<tr>
<td>isFeltBy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>isLocatedIn</td>
<td>City</td>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>isOwnerOf</td>
<td>Person</td>
<td>IndividualMemory</td>
<td>isOwnedBy</td>
</tr>
<tr>
<td>isSetIn</td>
<td>IndividualMemory</td>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>isTryingToBeAccessedBy</td>
<td></td>
<td></td>
<td>wantsToAccess</td>
</tr>
<tr>
<td>partOf</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>relatedTo</td>
<td>EmotionalState</td>
<td>IndividualMemory or Person</td>
<td></td>
</tr>
<tr>
<td>wantsToAccess</td>
<td>Person</td>
<td>IndividualMemory</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 - Object properties of the MyMemory Ontology

**Rule 1 (Defining Person as a contextual element):** In case a person would like to access a certain memory, then that person is a contextual element.

Person(?p), wantsToAccess(?p, ?iM), IndividualMemory(?iM) → ContextualElement(?p)

**Rule 2 (Defining Location as a contextual element):** In case a memory is set in a certain location, then that location is a contextual element.

IndividualMemory(?iM), Location(?l), isSetIn(?iM, ?l) → ContextualElement(?l)

**Rule 3 (Owner can access his/her memory):** In case a person would like to access a certain memory and is the owner of that memory, then the person can access the memory.

Person(?p), IndividualMemory(?m), wantsToAccess(?p, ?m), isOwnerOf(?p, ?m) → canAccess(?p, ?m)

**Rule 4 (Defining Person as not owner of a memory):** In case a person p1 would like to access a memory m1, a person p2 owns m1 and p1 and p2 are different people, then p1 is not the owner of m1 (since a memory can have only one owner).

Person(?owner), IndividualMemory(?iM), Person(?requester), wantsToAccess(?requester, ?iM), isOwnerOf(?owner, ?iM), DifferentFrom (?owner, ?requester) → isNotOwnerOf(?requester, ?iM)

**Rule 5 (Defining Person as part of a Situation):** In case a situation characterizes a memory and that memory is trying to be accessed by a person, then that person, as a contextual element, should be part of the same situation.

Situation(?s), characterizes(?s, ?iM), IndividualMemory(?iM), Person(?p), wantsToAccess(?p, ?iM) → hasPart(?s, ?p)

**Rule 6 (Defining Location as part of a Situation):** In case a situation characterizes a memory and that memory is set in a particular location, then that location should be part of the situation (as a contextual element).

Situation(?s), characterizes(?s, ?iM), IndividualMemory(?iM), Location(?l), isSetIn(?iM, ?l) → hasPart(?s, ?l)

**Rule 7 (Defining EmotionalState as part of a Situation):** In case a situation characterizes a memory and that memory is related to an emotional state (see rule below), then the same situation contains the emotional state as a contextual element.

The emotional state of the owner of the memory is directly related to the memory that is being requested. If the owner doesn’t want to show his/her memory, the emotional state will be a stressful or an angry state, and if the owner has no problem in sharing his/her memory, he/she will feel relaxed.
Rule 8 (Defining an EmotionalState as a contextual element, defining its feelings and defining its relationship with a person and with a memory): In case a person feels a psychological condition and he/she is the owner of a memory that somebody else is trying to access, and if the owner has an emotional state, then this means the emotional state is affected by the fact that someone else wants access to his/her memory. So, the emotional state is reclassified as a contextual element and it contains the psychological condition the user is feeling at that time. Also, the emotional state is related to the person that wants to access to the owner's memory and is related to the memory itself.

Person(?p), PsychologicalCondition(?pC), feels(?p, ?pC), EmotionalState(?eS), IndividualMemory(?iM), isOwnerOf(?p, ?iM), Person(?p2), wantsToAccess(?p2, ?iM), belongsTo(?eS, ?p) → ContextualElement(?eS), hasPart(?eS, ?pC), relatedTo(?eS, ?p2), relatedTo(?eS, ?iM)

Rule 9 (Classifying EmotionalState as stressful): In case an emotional state contains the psychological condition Nervous, then it is reclassified as a stressful state.

EmotionalState(?eS), Nervous(?n), hasPart(?eS, ?n) → StressfulState(?eS)

Rule 10 (Classifying EmotionalState as stressful 2): In case an emotional state contains the psychological condition Hesitant, then it is reclassified as a stressful state.

EmotionalState(?eS), Hesitant(?h), hasPart(?eS, ?h) → StressfulState(?eS)

Rule 11 (Classifying EmotionalState as relaxed): In case an emotional state contains the psychological condition Happy, then it is reclassified as a relaxed state.

EmotionalState(?eS), Happy(?h), hasPart(?eS, ?h) → RelaxedState(?eS)

Rule 12 (Memory can be accessed if owner feels relaxed): There is a situation that currently characterizes the memory that is trying to be accessed by a person. If the situation is composed of a relaxed emotional state, meaning, if the owner feels relaxed about someone trying to access their memory, then the person that wants access can access the memory.

IndividualMemory(?iM), Situation(?s), RelaxedState(?rS), hasPart(?s, ?rS), characterizes(?s, ?iM), Person(?p), wantsToAccess(?p, ?iM), relatedTo(?rS, ?p) → canAccess(?p, ?iM)

Rule 13 (Memory cannot be accessed if owner feels stressed and if someone else is requesting it): There is a situation that currently characterizes the memory that is trying to be accessed by a person that is not the owner of the memory. If the situation is composed of a stressful emotional state, meaning, if the owner feels stressed about someone else trying to access their memory, then the person that wants access cannot access the memory.

IndividualMemory(?iM), isNotOwnerOf(?p, ?iM), wantsToAccess(?p, ?iM), relatedTo(?sS, ?p), hasPart(?s, ?sS), Person(?p), characterizes(?s, ?iM), Situation(?s), StressfulState(?sS) → cannotAccess(?p, ?iM)

Next section describes a scenario in which the ontology determines the possibility of an entity to access someone’s memory.

Application Scenario

In this section, we present a preliminary evaluation of the application of the ontology proposed. We provide an instantiation of the ontology, simulating one scenario among the possible worlds.

Scenario description

An employer (John) wants to access his employee’s (Lisa’s) memory, that is a video in which she is with her former lover (Jonas), who is also an employee of the same company. We assume that John should not have access to this memory, because Lisa would not feel comfortable with it. However, Lisa is not aware of how to protect that piece of memory (or the artifacts representing it), since it could be easily spread over the Social Network. The system should then understand the situation and automatically protect that piece of memory. The ontology would support it by means of its rules.

Ontology instantiation
To characterize the situation, we have created ten individuals in Protégé, as seen on Table 3.

<table>
<thead>
<tr>
<th>Individual Name</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lisa</td>
<td>Person</td>
</tr>
<tr>
<td>John</td>
<td>Person</td>
</tr>
<tr>
<td>LisasMemoryWithJonas</td>
<td>IndividualMemory</td>
</tr>
<tr>
<td>EmotionalState1</td>
<td>EmotionalState</td>
</tr>
<tr>
<td>Hesitant</td>
<td>PsychologicalCondition</td>
</tr>
<tr>
<td>Nervous</td>
<td>PsychologicalCondition</td>
</tr>
<tr>
<td>Location1</td>
<td>Location</td>
</tr>
<tr>
<td>Bristol</td>
<td>City</td>
</tr>
<tr>
<td>England</td>
<td>Country</td>
</tr>
<tr>
<td>Situation1</td>
<td>Situation</td>
</tr>
</tbody>
</table>

Table 3 - Individuals and their respective classes for the application scenario

Each individual in Table 3 has its own set of object properties described in Table 4. Note that some individuals do not have any object properties defined. Situation1 defines the current circumstance in which LisasMemoryWithJonas is required. This way, it is composed of some contextual elements, which are: how the owner is feeling, who is requesting the memory, and where the memory was 'recorded'. However, these properties are not defined manually, they are inferred based on definitions in Table 4.

<table>
<thead>
<tr>
<th>Object property (domain, range)</th>
</tr>
</thead>
<tbody>
<tr>
<td>feels(Lisa, Nervous)</td>
</tr>
<tr>
<td>feels(Lisa, Hesitant)</td>
</tr>
<tr>
<td>isOwnerOf(Lisa, LisasMemoryWithJonas)</td>
</tr>
<tr>
<td>experiences(Lisa, EmotionalState1)</td>
</tr>
<tr>
<td>wantsToAccess(John, LisasMemoryWithJonas)</td>
</tr>
<tr>
<td>isIn(LisasMemoryWithJonas, Location1)</td>
</tr>
<tr>
<td>hasPart(Location1, Bristol)</td>
</tr>
<tr>
<td>isLocatedIn(Bristol, England)</td>
</tr>
<tr>
<td>characterizes(Situation1, LisasMemoryWithJonas)</td>
</tr>
</tbody>
</table>

Table 4 - Object properties for the application scenario

**Ontology use**

We argue that the system is able to detect the individuals from Table 3 and their object properties from Table 4 automatically. It is able to understand that Lisa feels nervous and hesitant and that John wants to see that particular piece of memory of her with Jonas. The piece of memory is composed of video and audio, so it contains information about her (her habits, friends, etc.). Based on the rules and on ontology, many other properties and concepts could be inferred, and they help determine whether John should be able or not to access Lisa's memory. Therefore, the implementation of the ontology should support making inferences about the user memories. In Protégé, once we synchronize a reasoner, it shows all the inferences that have been computed. The new Object Properties inferred are: feltBy(Nervous, Lisa), partOf(Nervous, EmotionalState1), feltBy(Hesitant, Lisa), partOf(Hesitant, EmotionalState1), hasPart(EmotionalState1, Nervous), hasPart(EmotionalState1, Hesitant), belongsTo(EmotionalState1, Lisa), relatedTo(EmotionalState1, John), relatedTo(EmotionalState1, LisasMemoryWithJonas), partOf(EmotionalState1, Situation1), partOf(Bristol, Location1), partOf(Location1, Situation1), hasPart(Situation1, Location1), hasPart(Situation1, EmotionalState1), hasPart(Situation1, John), isOwnedBy(LisasMemoryWithJonas, Lisa), isCharacterizedBy(LisasMemoryWithJonas, Situation1), isTryingToBeAccessedBy(LisasMemoryWithJonas, John), cannotBeAccessedBy(LisasMemoryWithJonas, John), partOf(John, Situation1), isNotOwnerOf(John, LisasMemoryWithJonas), cannotAccess(John, LisasMemoryWithJonas).

Some object properties were inferred based on the **inverseOf** property. "feltBy" was inferred because of the "feel" property, since they are inverse. Similarly, "isTryingToBeAccessedBy" is the inverse of...
"wantsToAccess", which was defined manually, as "isOwnedBy", which is the inverse of "isOwnerOf". Also, "isCharacterizedBy" is the inverse of "characterizes", as well as "belongsTo(EmotionalState1, Lisa)" and "experiences(Lisa, EmotionalState1)". The property "hasPart(Location1, Bristol)" has been manually added, so "partOf(Bristol, Location1)" was inferred. Other uses of "partOf" and "hasPart" in Table 5 are also inferences, since neither were manually added.

"hasPart(EmotionalState1, Nervous)", "hasPart(EmotionalState1, Hesitant)", "relatedTo(EmotionalState1, John)" and "relatedTo(EmotionalState1, LisasMemoryWithJonas)" have been inferred based on Rule 8, which states that "In case a person feels a psychological condition and he/she is the owner of a memory that somebody else is trying to access, and if the owner of the memory has an emotional state, then this means the emotional state is affected by the fact that someone else wants access to his/her memory. So, the emotional state is reclassified as a contextual element and it contains the psychological condition the user is feeling at that time. Also, the emotional state is related to the person that wants access to the owner's memory and is related to the memory itself." Breaking it down in parts, we have Lisa, who feels Nervous/Hesitant. Besides, we have the property "isOwnerOf(Lisa, LisasMemoryWithJonas)". We have Jonas, who "wantsToAccess(Jonas, LisasMemoryWithJonas)". The property "experiences(Lisa, EmotionalState1)" states that Lisa has an emotional state. Because of these properties, EmotionalState1 is classified as a ContextualElement and the property "hasPart(EmotionalState1, Hesitant/Nervous)" is defined. Also, the properties "relatedTo(EmotionalState1, Jonas)" and "relatedTo(EmotionalState1, LisasMemoryWithJonas)" were inferred. "partOf(Nervous/Hesitant, EmotionalState1)" was inferred because of inverseOf qualities.

The properties "hasPart(Situation1, EmotionalState1)" has been inferred based on Rule 8 and on Rule 7. Rule 7 states that: "In case a situation characterizes a memory and that memory is related to an emotional state (see rule 8), then the same situation contains the emotional state as a contextual element". The property "characterizes(Situation1, LisasMemoryWithJonas)" was previously defined and, based on the inferences mentioned, we have "relatedTo(EmotionalState1, LisasMemoryWithJonas)". So, the property "hasPart(Situation1, EmotionalState1)" links the situation with the emotional state since they both are related to the same memory. Inversely, "partOf(EmotionalState1, Situation1)" was also inferred.

The properties "hasPart(Situation1, Location1)" and "hasPart(Situation1, John)" have been inferred in a similar manner. Rule 6 and Rule 5 have caused them. Rule 5 states that: "In case a situation characterizes a memory and that memory is trying to be accessed by a person, then that person, as a contextual element, should be part of the same situation". The properties "characterizes(Situation1, LisasMemoryWithJonas)" and "wantsToAccess(John, LisasMemoryWithJonas)" apply to the rule above. Also, Rule 1 casts John as a ContextualElement, as it states: "In case a person would like to access a certain memory, then that person is a contextual element."

Similarly, Rule 6 states that: "In case a situation characterizes a memory and that memory is set in a particular location, then that location should be part of the situation (as a contextual element)". The properties "characterizes(Situation1, LisasMemoryWithJonas)" and "isSetIn(LisasMemoryWithJonas, Location1)" apply to the rule above, causing the property "hasPart(Situation1, Location1)". As the previous example, Location1 is also classified as a contextual element, based on Rule 6: "In case a memory is set in a certain location, then that location is a contextual element." Because of inversion, properties "partOf(Location1, Situation1)" and "partOf(John, Situation1)" have also been inferred.

The property "isNotOwnerOf(John, LisasMemoryWithJonas)" has been inferred based on Rule 4: "In case a person p1 would like to access a memory m1, a person p2 owns m1 and p1 and p2 are different people, then p1 is not the owner of m1 (since a memory can have only one owner)." We have defined "wantsToAccess(John, LisasMemoryWithJonas)" and "isOwnerOf(Lisa, LisasMemoryWithJonas)". It was manually set in Protégé that Lisa and John are different individuals. Because of these three items, "isNotOwnerOf(John, LisasMemoryWithJonas)" is inferred.

Lastly, there are "cannotAccess(John, LisasMemoryWithJonas)" and "cannotBeAccessedBy(LisasMemoryWithJonas, John)", which are inverse properties. For these inferences, a few rules were used. The main is Rule 13: "There is a situation that currently characterizes the memory that is trying to be accessed by a person that is not the owner of the memory. If the situation is composed of a stressful emotional state, meaning, if the owner feels stressed about someone else trying to access their memory, then the person that wants access cannot access the memory". The properties
John's the psychological condition Hesitant, then it is... Our goal is to protect people's privacy. We believe our work has some... Lisa to give their memories as evidence, and if the user was guilty, the... interpretation is likely not going to be perfect. Its intelligence may also overcome the user's current state of... solution does not guarantee hacking attempts will not happen, which can also break users' privacy. Context interpretation is likely not going to be perfect. Its intelligence may also overcome the user's current state of mind. One delicate example would be if the user was in trial for a certain crime. If the user was requested to give their memories as evidence, and if the user was guilty, the system could sense the user is in trouble.
However, we believe justice is a greater good, and the system should not block the memories. This example illustrates how sensitive this topic is, and how open it is for discussion, for we have not come to a full conclusion on what the best solution regarding privacy is.

MyMemory may have more possible contextual elements. We opted for three (the person that is requesting, how the owner is feeling and where the memory is located), but certainly there is room for much more. Variables like "is the requester present in the memory?" or "action pattern in memory" do impact on whether the memory should be shared.

We expect a system that uses our ontology to have artificial intelligence capabilities. Speech and video recognition could be extremely helpful to identify who is requesting the memory or how the user reacts to the request. Also, future work may regard how to store the information the system collects about the user’s privacy wishes and feelings. Furthermore, it is also possible to explore the relationships among the different types of memories depicted in the External Digital Memory Ontology. For example, an important discussion would be about Collective Memory. Since one video contains an event with many participants, who is the owner (even if captured by only one individual)?

We could also extend the investigation to reflect on potential forms of abuse and discrimination that may stem from the use surveillance systems, e.g. the use of body-worn cameras by police. Different solutions are needed to maintain privacy in a world so public, in which people constantly share their memories and want to see other people’s memories. We have presented a way to incorporate privacy protection into Social Networks, but it can be used by any system that manages digital memories. We believe our solution is a start to many other features regarding privacy, but still leaves room for further investigation.

REFERENCES


