POSTER

Understanding Usage Control Requirements in Pervasive Memory Augmentation Systems

Agon Bexheti
Università della Svizzera Italiana (USI)
Via Giuseppe Buffi 13
6900 Lugano, Switzerland
agon.bexheti@usi.ch

Marc Langheinrich
Università della Svizzera Italiana (USI)
Via Giuseppe Buffi 13
6900 Lugano, Switzerland
marc.langheinrich@usi.ch

MUM '15 November 30 - December 02, 2015, Linz, Austria

ACM ISBN 978-1-4503-3605-5/15/11.
DOI: http://dx.doi.org/10.1145/2836041.2841216

Abstract

Mobile and wearable devices allow people to capture different aspects of their life experiences (e.g. family holidays, work meetings, running activities, etc.) in the form of photos, videos, physiological data, etc. An interesting avenue to explore is the usage of such captured experiences to support and augment human memory. Experiences of different events can be used to generate retrieval memory cues in order to trigger recall of those recorded events. In addition, captured experiences can be shared with other (co-located) people of the same event. The focus of this work is on understanding the privacy challenges with regard to using and sharing captured experiences for memory augmentation purposes. With the ultimate goal of an usage control model for the protection of personal memory cues, here we provide insights on: how sharing captured experiences is different from sharing experiences in social media networks, and what are some challenges in designing an usage control model for memory cues.

CCS Concepts

•**Social and professional topics** → **Privacy policies;**
•**Security and privacy** → *Privacy protections;*

Author Keywords

Life-logging; Memory augmentation; Episodic memory; Sharing; Privacy; Usage Control

Background

Human memory is inherently fallible and people have been using different kinds of techniques to better remember past events, e.g. logging their daily activities in diaries or creating photo-albums of important events. Such stored data - referred to as memory cue - serves as a trigger or a stimulus for the human brain to retrieve an instance of a past event. Results from psychology research show that memory cues can be used to reinforce and attenuate human *episodic memory* [10, 2]. *Episodic memory* is the collection of past events or experiences that occurred at a particular time and place and that can be expressed. In contrast, *prospective memory* refers to the ability of remembering to remember or remembering to perform a planned action. For example, a single photo can help one to remember the first bike ride, a flashcard can prompt one the name of a recently met person or an audio song can make one recall a day from high-school, etc.

An emerging space in this context is the potential of technology to support and strengthen human cognition with an emphasis on memory. Vannevar Bush in his 1945 essay "As we may think" [3] introduced the concept of a personal information system - the Memex which stores books, pictures, audio recordings, etc. - to complement the human memory. Bush's prophetic idea is raised now in the era of recent advances in technology which overly influence the way we try to capture, process, store and review our memories. Advanced mobile and wearable gadgets coupled with nearly unlimited storage space allow for quasi continuous recording of our experiences, and data mining techniques can be employed to extract meaningful memory cues. Personal displays - smartwatches, smartphones or laptops - and ambient screens provide many different ways to visualize and review captured memory cues (see Fig 1). The integration of such technology aspects opens up the opportunities for *pervasive memory augmentation systems*, which can be used in many different situations such as supporting people with failing memories, influencing behavior change or helping with better remembering previous meetings.

At the outset it seems that the only requirement for a memory augmentation system in terms of security and privacy issues is to employ an access control mechanism in order to prevent unauthorized access to captured experiences and memory cues generated from those experiences. The requirements for protecting memory cues increase significantly when considering *collaborative memory cues* - sharing memory cues with other (co-located) people. With the ultimate goal of an usage control model - a solution that goes beyond simply granting access permissions and provides ways to control the usage of memory cues - and a policy language for protecting memory cues, in this short paper we provide insights on:

- how sharing captured experiences and memory cues is different from sharing in social media (e.g. a single photo or a text document), and
- what are some challenges and requirements for the design of an usage control model for sharing memory cues.

Before describing any privacy control requirements it might be in order to first describe a scenario to illustrate the memory augmentation process and to get some understanding regarding the architecture of such a system.

Scenario

Team Alpha have their quarterly meeting and discuss future steps of their project. They decide to use the built-in recording system of the meeting room and capture their group discussions. Before starting the meeting, all participants provide their consent related to meeting capture.

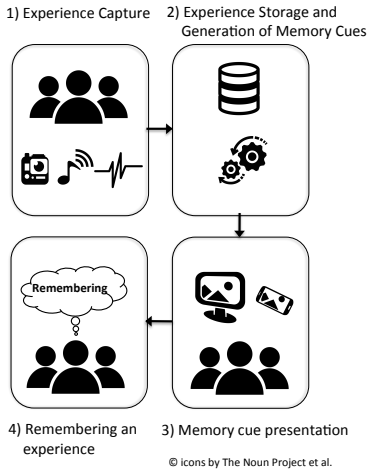

Figure 1: Memory augmentation process

The room is equipped with fixed video recording cameras that provide perspectives from different angles, microphones for enhanced audio recording and a dedicated camera for capturing white board content. In addition to the room's infrastructure, two out of four participants have small wearable cameras clipped on their shirts - which capture first-person images every 30 seconds. Captured data is automatically uploaded to the *MemoryVault* - a warehouse for storing captured experiences - and then processed in order to generate meaningful memory cues that reflect the meeting - for instance, images showing white board content, a list of topics extracted from the audio recordings, front face image of another person captured from one-to-one discussions, etc. Depending on their preferences, in the upcoming days participants will automatically and unobtrusively receive the memory cues of the meeting on their smartphones or their office mounted ambient displays. After reviewing the memory cues for some time, participants will vividly remember their last meeting.

Sharing memory cues vs. sharing social media

As number of users in social network sites (SNSs) has grown, so has increased the willingness of users to share information in SNSs. It is not unusual for people to share their life experiences and SNSs are places where people do this everyday. Privacy issues related to sharing are well studied with the most dominant strands in this context being privacy issues of location sharing [9], and privacy issues with regard to sharing audio visual information [1, 6]. Since this area is established and well studied, one can naturally ask why do we need something special for sharing captured experiences in the context of memory augmentation?
We have identified six key differences between sharing experiences/memory cues on SNSs versus sharing them in memory augmentation systems:

1. Sharing in SNSs is usually encouraged by the desire to communicate with other people and grow social relationships [11], while there is an utilitarian (give and take) incentive to share one's own experiences for memory augmentation purposes, e.g. combining experiences captured from several participants during a meeting can generate better memory cues to better remember the meeting.
2. Usually people share in SNSs data related to single events - e.g. pictures of visiting a new place or some occasional location updates. In contrast to this, memory augmentation applications may involve sharing of continuous experiences (life-logs) of longer events or even multiple events, e.g sharing data captured for supporting memories of half a day long meeting or experiences captured during one's full day at work.
3. A common practice is that users manually share data in SNSs despite that some services can be configured to automatically share data on behalf of the user (e.g. data from run trackers). In most of the cases,

the envisioned memory augmentation systems will automatically share experience traces when possible.
4. Captured experiences for memory augmentation can contain more personal and highly sensitive information than experiences usually shared in SNSs - e.g. in the meeting capture scenario, during a break period a user may issue a payment transaction and credit-card numbers can be captured by the room's built-in camera or the user's wearable camera. Sharing memory cues requires higher privacy considerations compared to sharing experiences in social media [5, 8].
5. Another issue that automatically follows up when sharing contents from one's personal MemoryVault is how to filter sensitive and private data. Imagine that in the meeting capture scenario, one has to browse three hours of video data from each fixed camera, thousands of pictures from a chest mounted camera, plenty of audio snippets to select what data can be safely shared with other people.
6. Since a personal MemoryVault contains continuous data streams from different sources - e.g. video from fixed cameras, audio recordings, pictures from wearable cameras, white board content from a meeting, etc - users themselves struggle to fully make sense of that data. In this case the sharer is not aware on how others can understand and interpret shared experience traces.

Usage control requirements

In order to protect memory cues from unauthorized access we need some sort of access control mechanism. Traditional access control solutions do not provide any mechanism to control data once access is granted [4]. The new family of access control - named as *usage control* - provide ability to monitor data usage and continuously evaluate access permissions [7].

We believe that usage control approaches are a viable approach for protecting personal memory cues and for securely sharing one's own memory cues. With the meeting capture scenario in mind - which shows the main characteristics of a memory augmentation system - we identify a set of common requirements to design an usage control model:

1. Users should be able to protect their personal MemoryVaults from unauthorized access in order to avoid some leakage of personal and (highly)sensitive information.
2. The data owner should have the possibility to conditionally share recorded personal experiences. Conditions can be thought as a pre-sharing agreement on some obligations regarding the usage of shared data - e.g. shared data can be used only once and must be deleted after a week or shared experience traces can be used as provided and cannot be further processed in order to generate better memory cues.
3. Ability for the experience sharer to revoke access in case of data misuse.
4. For experiences that have group ownership - e.g. data captured in the meeting scenario - the system should resolve conflicts when multiple users provide data access and usage policies. For instance, in the meeting capture scenario involving four people, two members are against the idea of sharing captured discussions with other people of the department that didn't attend the meeting.
5. Users should have some level of access to their own experiences captured from devices outside of their control.
6. The set of memory cues related to some event to be reviewed will have an impact on how that event will be remembered. It is essential that the system has some reliance mechanism to provide the provenance of

the memory cues, especially when memory cues are shared from other people or captured from devices outside of the user's control.

We see this non-comprehensive set of requirements as a starting point in our work in the area of usage control models for building secure and trusted memory augmentation systems.

Acknowledgments

The authors acknowledge the financial support of the Future and Emerging Technologies (FET) programme within the 7th Framework Programme for Research of the European Commission, under FET Grant Number: 612933 (RECALL).

References

1. Shane Ahern, Dean Eckles, Nathaniel S. Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed?: Privacy Patterns and Considerations in Online and Mobile Photo Sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM, 357–366.
2. Michael C. Anderson, Robert A. Bjork, and Elizabeth L. Bjork. 1994. Remembering can cause forgetting: Retrieval dynamics in long-term memory. *Journal of Experimental Psychology: Learning, Memory, and Cognition* 20, 5 (1994), 1063–1087.
3. Vannevar Bush. 1967. As we may think. *The growth of knowledge: readings on organization and retrieval of information* (1967), 23–35.
4. Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati. 2003. Access Control: Principles and Solutions. *Softw. Pract. Exper.* 33, 5 (April 2003), 397–421.
5. Daniel A. Epstein, James Fogarty, and Sean A. Munson. 2014. Failures in Sharing Personal Data on Social Networking Sites. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 695–698.
6. Patricia G. Lange. 2007. Publicly Private and Privately Public: Social Networking on YouTube. *Journal of Computer-Mediated Communication* 13, 1 (Oct. 2007), 361–380.
7. Jaehong Park and Ravi Sandhu. 2002. Towards Usage Control Models: Beyond Traditional Access Control. In *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies (SACMAT '02)*. ACM, New York, NY, USA, 57–64.
8. Reza Rawassizadeh and A Min Tjoa. 2010. Securing Shareable Life-logs. IEEE, 1105–1110.
9. Janice Y. Tsai, Patrick Kelley, Paul Drielsma, Lorrie Faith Cranor, Jason Hong, and Norman Sadeh. 2009. Who's Viewed You?: The Impact of Feedback in a Mobile Location-sharing Application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 2003–2012.
10. Endel Tulving. 1985. Elements of Episodic Memory. (1985).
11. Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman. 2011. Are You Close with Me? Are You Nearby?: Investigating Social Groups, Closeness, and Willingness to Share. In *Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp '11)*. ACM, New York, NY, USA, 197–206.