Submitted version of Davies, N., Friday, A., Clinch, S., Sas, C., Langheinrich, M., Ward, G., Schmidt, A., 2015. Security and Privacy Implications of Pervasive Memory Augmentation. IEEE Pervasive Computing 13, Jan-Mar 2015. Special Issue on Pervasive Security and Privacy.

Security and Privacy Implications of Pervasive Memory Augmentation

Nigel Davies[1], Adrian Friday[1], Sarah Clinch[1],
Corina Sas[1], Marc Langheinrich[2], Geoff Ward[3], Albrecht Schmidt[4]
[1]Lancaster University, [2]University of Lugano, [3]University of Essex, [4]University of Stuttgart

ABSTRACT

Pervasive computing is beginning to offer the potential to re-think and re-define how technology can support human memory augmentation. For example, the emergence of widespread pervasive sensing, personal recording technologies and systems for quantified self are creating an environment in which it is possible to capture fine-grained traces of many aspects of human activity. Contemporary psychology theories suggest that these traces can then be used to manipulate our ability to recall, i.e. to both re-enforce *and attenuate* human memories. In this paper we consider the privacy and security implications of using pervasive computing to augment human memory. We describe a number of scenarios, outline the key architectural building blocks and identify entirely new types of security and privacy threats – namely those related to data security (experience provenance), data management (establishing new paradigms for digital memory ownership), data integrity (memory attenuation and recall induced forgetting), and bystander privacy. Together these threats present compelling research challenges for the pervasive computing research community.

1. INTRODUCTION

Technology has always had a direct impact on how and what humans remember. This impact is both inevitable and fundamental – technology radically changes the nature and scale of the cues that we can preserve outside our own memory in order to trigger recall. Such change is not new – we have seen the transition from story-telling to written books, from paintings to photographs to digital images and from individual diaries to collective social networks. However, in recent years three separate strands of technology have developed to the extent that collectively they open up entirely new ways of augmenting human memory:

1. near-continuous collection of memory cues has become possible through the use of technologies such as Microsoft's SenseCam [9], social networks and interaction logs.

2. advances in data storage and processing now enables widespread mining of stored cues for proactive presentation, both in terms of cues collected by an individual and in terms of complex networks of related cues contributed by others.

3. the presence of ubiquitous displays (both in the environment and via personal devices such as Google Glass™) provides many new opportunities for displaying memory cues to trigger recall.

The result is that it is now feasible to use pervasive sensing to capture a very large amount of data on an individual's experiences, i.e. their memories, and then to use pervasive display technologies to trigger recall of these memories. Contemporary psychology theories suggest that these traces can then be used to both re-enforce and attenuate human memories [1]. This opens up the possibility of a very wide range of new applications for memory augmentation devices but it also raises new privacy and security concerns. Traditional research in this area has principally been concerned with privacy concerns for either third-parties captured in video footage or individuals wishing to anonymise their location traces. In this paper we discuss a range of new security and privacy threats that target manipulation of an individual's memories. Our contributions are threefold:

1. We highlight pervasive memory augmentation as an important area of future work for the community and provide a series of compelling application examples.

2. We describe the core architectural building blocks of a future pervasive memory augmentation ecosystem.

3. Based on our architecture we identify a number of privacy and security threats that provide research challenges for the community. These threats span a range of areas including data security (experience provenance), data management (establishing new paradigms for digital memory ownership), data integrity (memory attenuation and recall induced forgetting), and bystander privacy.

Note that we do not claim to have solutions to the challenges that we highlight – the field of memory augmentation is still sufficiently new that we believe there is significant value in laying out the potential problem space upon which others can build. Indeed, we hope that this article provides a starting point for significant community research activity in the area of security and privacy protection for pervasive memory systems.

2. FUTURE MEMORY AUGMENTATION SYSTEMS IN USE

We envisage an environment in which augmented memory systems make everyday use of peripheral, ambient multi-media content – delivered via large wall-mounted displays, smartphone wallpapers, or wearable in-eye projectors – to intelligently integrate, display, and enable the review of life-relevant personal data. Future memory augmentation systems will integrate information actively entered by the user (e.g., calendar entries, photos) with additional relevant data collected automatically through a multitude of capture technologies, in accordance with the user's privacy preferences. Through the ambient review of their activities over a range of timescales users will be able to actively manage their memories: they will be able to enhance the later accessibility of needed information, whilst attenuating the recall of unwanted information. Therefore, such systems not only bring together advances in capture systems and display technologies to provide cues and hints that prompt humans to remember, but also provide tools that allows users to more actively manage the accessibility of their memories in the future. Pervasive memory augmentation systems have the potential to revolutionise the way we use memory in a wide range of application domains.

2.1 Behaviour Change

Effecting behaviour change is an important objective in many important areas such as health (e.g., lifestyle changes such as increasing exercise or stopping smoking) and sustainable transport (e.g., encouraging people to make more environmentally-friendly transport choices). Unfortunately, despite good intentions, many people experience difficulty in implementing planned behaviour: for example, it is well known that many people are reluctant to make a trip to the gym despite paying large gym membership fees. Psychological theory stresses that intentional behaviours are more likely to be implemented when individuals are reminded of their own attitude towards such behaviours (e.g., the positive gains that will result), and the attitudes of significant others to the behaviour (what loved ones, family, friends, peers, and society in general think of the behaviour and its outcomes). In addition, realistic scheduling is important: planned behaviour is more likely to be performed if it is timetabled with the transition from immediately preceding activities in mind. Finally, behaviour is more likely if it is perceived to be more achievable and more enjoyable. Pervasive memory augmentation can help with the realistic scheduling and reminding of the planned activities, and can remind people at the point at which decision making is necessary (e.g., at the planned time to visit the gym) of the positive benefits from the behaviour, the previous good experience of the behaviour and the progress that is being made.

2.2 Learning

Pervasive memory augmentation technologies can also be used as part of a learning environment. In particular, through the use of ambient displays it is possible to cue recall, and hence reinforce learning of a wide range of skills. For example, the acquisition of a new language could be supported by providing appropriate cues to facilitate recall of vocabulary. Similarly, a class teacher could be encouraged to remember the names of their pupils, an expatriate could better remember local customs to ease office integration, and a study-abroad student could learn culturally-significant facts as they explore a new city.

2.3 Supporting Failing Memories

Research has shown that as we age, our ability to perform uncued recall is particularly vulnerable to age-related decline. Pervasive memory augmentation technologies could be used to help remedy this memory loss by providing older users with time-relevant and context-appropriate cues. In this way, older individuals could enjoy greater self-confidence and greater independence by being reminded of moment-by-moment situated details of where they were, what they were intending to do, and how they could get home. They may also enjoy better relationships if they could be reminded of the autobiographical details of their loved ones (such as the names and ages of their loved ones' children), or if they could review and then be reminded of the details of a recent conversation or event (e.g., a recent day out or family gathering).

2.4 Selective Recall

Through appropriate selection of memory cues that are presented to the user, pervasive memory augmentation can be used to facilitate selective recall. According to the psychological theory of retrieval-induced forgetting, the act of reviewing memories not only enhances the probability of spontaneously retrieving these reviewed memories in the future, but it can also attenuate the spontaneous retrieval of related but unreviewed memories. The study of retrieval-induced forgetting has largely been confined to the laboratory using lists of cat-

egorised words. It is of both pure and applied interest (e.g., the desired attenuation of unwanted, outdated, or traumatic memories; and the undesired attenuation of wanted but unreviewed memories) to see if this phenomenon can be observed when reviewing a subset of "real world" memories, and if so, we will be able to measure the extent to which unreviewed memories could be attenuated through selective reviewing.

2.5 Advertising

While many of the application domains for pervasive memory augmentation technologies are for the public good, the same technologies can also be employed in more commercial contexts such as the provision of new forms of advertising in which users have memories triggered explicitly to drive purchasing decisions. For example, when passing a shop selling luggage a cue could be presented that causes a passer-by to remember a specific experience from their past in which their own luggage didn't work satisfactorily. This may then cause the user to enter the shop and purchase some new luggage.

2.6 Social Acceptance

These scenarios illustrate the potential power of pervasive memory augmentation. While a number of news have reported social backlash from bystanders impacted by others' use of image-based lifelogging devices such as Google Glass™, two observations indicate that this may not be the restrictive factor that it first appears.

Firstly, although useful, mobile cameras are by no means an essential data source for triggering recall – location information is readily tracked by mobile devices and has been shown to improve memory reconstruction [7], other mobile sensors and non-image based lifelogging devices (e.g., step counters and heart rate loggers) can provide a wealth of relevant information, and mining existing 'fixed' data sources such as email, social networking, and calendar providers can also provide a rich description of our activities. While these can certainly be just as privacy invasive as video recordings, they don't trigger social backlash in the same way as image-based lifelogging devices can.

Secondly, we note that there are cultural differences in technology acceptance, and that social preferences often change over (fairly short) periods of time. For example, while in some countries capture of one's personal image is deemed an unacceptable invasion of privacy, in countries such as the UK the population has accepted that the security benefits of allowing personal images to be captured (i.e. as in CCTV) outweigh concerns regarding privacy. Equally, early adopters of smartphones encountered similar negativity to that currently targeted at some lifeloggers, as the use of smartphone cameras in public drew concern. However, such devices are now commonplace. Further examples can be drawn from the range of potentially privacy-invasive applications such as activity monitors (e.g., Fitbit), location-based services, and social networking applications that by now have been widely adopted. Note that the actual *reasons* for the gradual acceptance of these intrusive technologies may hardly be desirable (e.g., discounting privacy implications in favor of short-term rewards, or a certain feeling of helplessness given the ubiquity of today's privacy invasions). Obviously, pervasive memory augmentation devices should be designed with proper privacy safeguards in mind (see section 4).

Our long-term vision is of a privacy-friendly technology eco-system that uses a range of sensors and data inputs to support augmentation of human memory in application domains such as those described above and that could have a transformational impact on the lives of citizens by improving the acquisition of new knowledge, the retention of existing knowledge, and the loss of unwanted knowledge.

3. ARCHITECTURES FOR MEMORY AUGMENTATION

Early experiments into memory augmentation focused on architectures and systems in which experience data was gathered by devices worn or carried by a user (Figure 1). This data could then be locally stored or uploaded to cloud-based servers. Different user interface concepts were explored that allowed users to inspect the data, typically as part of a specific review activity. There are numerous examples of such systems ranging form those designed to support short term memory (e.g., Heyes et al. [6]) to those that attempted to create complete life logs (e.g. Gemmell et al. [4]). Many of the early systems looked at feasibility and focused on recording images, audio, and activities. Recently, quantified self technologies such as the FitBit (www.fitbit.com) have become commercially available that allow users to track a range of their activities.

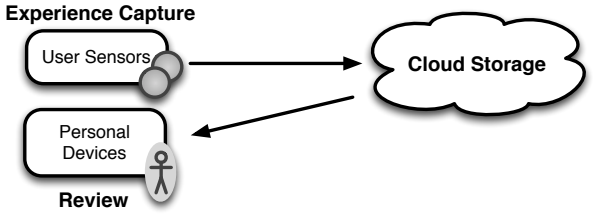

Figure 1: Early Pervasive Memory Architectures

However, this type of architectural approach has a number of shortcomings. Firstly, it relies on data captured exclusively by a specific user. This seriously reduces the number of data streams available and the

quality of these data streams. Consider, for example, attempting to capture a user's experience of a meeting. Using a microphone on a mobile device in the user's pocket is likely to offer significantly poorer results than using a high-quality audio conferencing microphone built into the meeting room. This problem extends to a wide range of contextual and environmental data and is particularly acute when considering interaction with cloud services in which the obvious source of the experience data is the service itself rather than an approximation of the interaction captured by the user.

Indeed, when designing capture systems there are several parameters that are important and that need to be considered. For humans the visual and auditory channels are dominant and recording these has been the focus in many projects. In the case of visual capture the visual field of view and the position of the camera is important (e.g. glasses with a similar view as the human view versus a device worn around the neck with a lower perspective and a wide angle lens). Of course visual capture could also be more powerful than human vision, e.g. using cameras pointing in multiple directions, with higher temporal and special resolution than the eye, or even recoding wavelengths the human eye cannot see.

Capturing meta information, and most importantly time and location, adds significant value to the data, as it allows selective access to specific experiences captured. Examples of sensors that are useful include location sensing, sensors that provide information about the physical environment, but also sensors that provide information about the users physiological state (e.g. excitement or attention). For captured visual information it may be of great value to know where the user was looking and hence eye-gaze information is helpful as meta-information.

Problems also arise when one considers data presentation using current architectural approaches. Very few users are able to take the time to review the memories that are captured during the day – witness the problems most users have these days managing a relatively small number of digital photographs. It is unlikely that a pervasive memory augmentation system that relies on users explicitly reviewing memories will deliver significant value.

Instead, we believe that future systems will rely on the ability to appropriate screen real-estate from the large number of displays that the user already looks at as part of their daily activities. Examples of displays that are likely to be appropriated include public signage, personal ambient displays such as photo frames and advertising display space embedded into applications such as Google Mail and search results. Access to recorded experiences may take a number of forms including: (1) using the material for specific but selective queries where the information is helpful, (2) reviewing a summary of the information recorded that is significantly compressed, and (3) having the information that is recorded presented in the periphery of the user to stimulate specific recall.

Based on consideration of both capture and presenting issues it is our hypothesis that future pervasive memory augmentation systems will form complex ecosystems of experience capture, storage and presentation devices rather than the user-centric approaches currently employed. In Figure 2 we show the key building blocks for future memory augmentation systems.

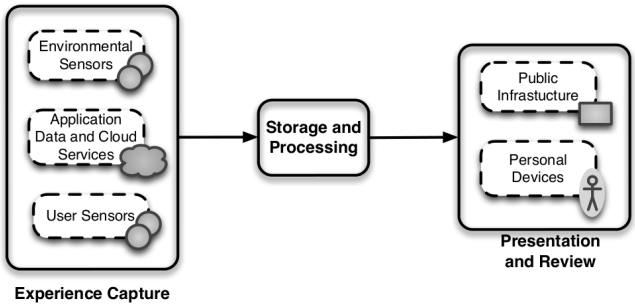

Figure 2: Pervasive Memory Architecture

4. SECURITY AND PRIVACY THREATS

Given the applications and architectures described above it is possible to envisage a series of areas of potential security and privacy threats.

4.1 Experience Provenance

Traditional experience capture systems typically use a device attached to the user such as a Sensecam or a health monitor. This device is assumed to be trusted and the data it produces is considered to accurately describe (within the constraints of the technology) the experience of the wearer. As discussed in section 2, we envisage a world in which many of the data streams that constitute an individual's memories are sourced from devices not worn by the user, and indeed, are outside the user's control.

This reliance on external data sources represents an obvious point of attack against pervasive memory augmentation systems. For example, if I am using a microphone in a meeting room to capture audio associated with a meeting how do I know (without carrying out a manual review) that the audio captured is indeed an accurate reflection of what occurred in the meeting? This problem obviously extends beyond audio to cover any of the wide range of experience capturing sensors on which future pervasive memory augmentation systems are likely to rely. It is worth stressing at this point we are not concerned with how to protect experience data once it has been captured – we believe there is a sig-

nificant potential for attack even before the data has been passed though and marked as being relevant to a specific user.

The specific challenge therefore is *how do users ensure the provenance of the data they store as memories?* This problem is related to that of securely associating with devices in the infrastructure which has been explored in a number of ubiquitous computing systems (e.g. in "The Resurrecting Duckling protocol" [10] that addressed the issue of secure transient association between devices). However, in the majority of these systems the user was connecting to a component in the infrastructure in order to affect an observable change (such as displaying an image on a projector or controlling the temperature in an office). In memory augmentation systems the challenge is that the user may only review the captured experience long after the event and at a point at which it is essentially impossible to detect that the original data stream was defective.

Overall we believe that it will be necessary to develop architectural solutions that are able to provide end-to-end guarantees for users of the provenance of data they are using as part of their digital memories. Such solutions may need to be developed specifically for memory augmentation but it may also be possible to repurpose solutions that are emerging in the Internet of Things domain to cover provenance of sensor data.

4.2 Memory Protection

Once experience data has been successfully captured and its provenance assured then this data will need to be securely stored. At some level this represents a traditional data security challenge. However, the focus on experience data that constitutes an individual's memories raises a number of unique challenges. Firstly, the data store itself is likely to highly distributed and be accessed by a wide range of third-parties, authenticated in some way by the user. For example, numerous data feeds will need the ability to upload data without going via any user applications. Moreover, applications designed to support recall may require access to this data and this complex network of data producers and consumers will require relatively sophisticated access control mechanisms married with very simple user interfaces.

The challenges of designing an appropriate access control mechanisms and associated interface increase significantly when sharing memories is considered. For example, in a meeting involving three people who owns the memory of the event ? Is it necessary for each of the people to keep their own copy of the memory and then manage there own access controls or is it possible for a single copy to be maintained with appropriate shared ownership ? As the various participants chose to delete their copies of the memory what happens when the last interested party deletes the memory ?

Indeed, the issue of protected memories is closely related to the issue of basic data management. It is almost certainly the case that we do not wish to remember everything – research has shown that forgetting is crucial to our ability to recover from emotional events and that as the number of digital assets in our lives increases so we are developing new rituals for forgetting.

Perhaps the ultimate test of access control occurs when we die. What should happen to our digital memories when we die? The topic of managing digital assets after death is starting to attract significant research attention. Many research disciplines are exploring the role of digital content (typically social media) in the grieving process [3] while the study of existing legal practices is highlighting challenges associated with managing digital asset ownership after death [2]. Existing research has predominantly focussed on social media such as email and social networking content, but as pervasive memory systems develop it seems obvious that we will wish to have a way to express our wishes regarding our digital memories after death. For example, we may wish to:

- make our memories available to our children so they can benefit from our experiences
- have our memories die with us so that we can control how people remember us
- donate our memories to science or history

Of course in practice the most likely scenario is that we wish to employ some combination of all of the above – some of our memories will be intensely private and we will wish those to die with us, while many memories we would be happy to contribute to society (perhaps after a time-period that ensures all those individuals captured or implicated have passed away) offering the possibility of transferring the way we capture and study history.

Recent experiences with a variety of digital assets has shown that inheritance, ownership and control issues pose significant challenge, particularly with regard to the range of stakeholders involved [2]. With respect to memory, we anticipate that the issues of managing and protecting our memories will be further complicated – a key research challenge therefore is to develop mechanisms to enforce the wide variety of policies desired by individuals to exercise control over access to their memories. This research challenge incorporates technical aspects – how should such systems be engineered – together with the need to address social and legal concerns.

In developing solutions to these challenges researchers will need to be mindful of the need to reassure potential users that their memories will be protected not just for the short-term but for many years. This implies a level

of forward planning that may be incompatible with the short-term focus of many new technology companies. As a result solutions may involve both a technology component and some form of certification or independent standards process that is able to provide users with the required confidence.

4.3 Memory Manipulation

One of the most exciting developments in the area of pervasive memory augmentation is the fact that contemporary psychology theories suggest that cued recall can be used to both re-enforce *and attenuate* human memories. In practice this means that is a system is able to cue a subset of your memories relating to an event then it is believed that there will be a corresponding decrease in your ability to recall other memories of the event. If these theories prove valid then the security implications this gives rise to are potentially immense. For example, imagine a pervasive memory augmentation system that is comprised and allows attackers to select which of your memories to cue and, by extension, which to try and attenuate. Advertises and brand management companies could pursue campaigns to make users forget bad customer experiences and "only remember the good times". Corrupt states could endeavour to influence entire populations while industrial espionage companies could attempt to alter the memory of top executives involved in complex negotiations.

Of course attempting to influence people through cuing memories has always been a part of advertising and brand management. The important new threat that pervasive memory augmentation gives rise to is that the cues and memories no longer need to be generic (e.g. pictures of Christmas trees to encourage recall of past family holidays) but can be specific to each individual (a picture of a specific moment last Christmas, recalled at the expense of memories of other Christmas moments), thus leading to much more effective forms of memory manipulation.

The key challenge we see with respect to memory manipulation is *how can a user tell if their memories are being manipulated ?* In other words, how can they tell if the memories being cued are part of the normal daily operation of the system versus being part of a concerted attack on their memories. To address this we suspect that it will be necessary for solutions to enable users to instantiate real-time monitoring of the cues that are delivered to them to look for unusual patterns of activity that might suggest they are under attack. In essence such real-time monitoring would be akin to a virus checker for a regular PC – a virus checker for our human memories – constantly monitoring activity to identify suspicious patterns.

4.4 Privacy of Bystanders

The widespread use of personal capture technology would also significantly impact the privacy of bystanders. While sensing strictly personal attributes such as one's location or vital signs is unproblematic, sensing and capturing people in one's vicinity, as well as their actions, will most likely run into social, in some cases even legal issues.

In many jurisdictions, personal data collections are exempt from data protection legislation. For example, running WiFi or Bluetooth scanners on one's own smartphone will most likely be perfectly legal in most countries. However, already a single photograph – while certainly legal for personal use[1] – can easily create significant social friction in certain circumstances. Wearers of Google's augmented reality glasses often come under social scrutiny, and a few cafes and restaurants have already started banning the use of Glass on their premises. The challenge is *how to protect bystanders while allowing substantial data collection for human memory augmentation.*

Even more problematic is the hidden recording of audio – in many countries an actual felony. The idea of having a personal system recording one's spoken conversation would require significant legal change – unlikely, if not even undesirable. One approach would be to focus on technologies that do not actually record anything but instead work like simple detectors – similar to recent Android smartphones that are able to detect a spoken activation command to wake up. To harness such an approach to aid personal recall, such audio detectors would need to be programmable, in order to support a wider range of individual words or phrases, and once detected keeping track of their frequency only, or maybe simply noting the time and place of detection. While certainly not yet with legal precedence, such "audio detectors" might be perfectly legal, given that they do not allow one to attribute any detected word to a particular speaker.

Similar technology might need to be developed for video recording devices, so that instead of high-fidelity video capture, only certain abstract elements of a scene get recorded – similar to the ability of motion capture devices such as the Kinect to create recordings of abstract stick-figures. While such approaches help with legal issues, they might still fall short of increasing social acceptance. At the outset, the use of such "vicinity sensing" technology might be limited to those situations in which photography is already much more accepted, e.g., during sports (e.g., running, skiing, hiking), in one's car (car-cam), work meetings (with employer permission), in participating museums, or around tourism hot-spots.

[1]Legal exceptions of course exist, e.g., around governmental sites or, in some countries, involving members of the police.

Solutions in this space are likely to combine elements of new technologies for creating abstract recordings with a robust way of announcing recording practices and policies to users (e.g. through the use of privacy beacons [8]).

5. LOOKING FORWARD

Pervasive memory augmentation systems are likely to become a reality in the next decade. The basic technologies for mobile and infrastructure-based experience capture and for near-ubiquitous display of memories are already commonplace. What is missing is an understanding of how to connect these components together via an appropriate memory store to deliver value such as the applications described in Section 2. However, this is clearly a solvable problem and we expect systems to emerge that provide increasingly comprehensive memory capture and recall.

While the benefits of pervasive memory augmentation are significant, in this paper we have attempted to highlight the challenges that such systems give rise to, particularly in the area of security and privacy. Of course, with respect to security and privacy, pervasive memory augmentation systems give provide new opportunities as well as threats. For example, if pervasive memory augmentation systems become established, then the underlying capture systems could also be used to provide additional data for context-aware authentication systems (e.g. Hayashi et al.'s CASA [5]). In such cases the threats identified in this paper have still greater significance as corruption of the memory traces could impact security more broadly.

Overall, memory and knowledge on a societal level is of great importance. Over the last $4,000$ years our way of recording information has evolved from stone carvings through printing to multimedia documents. However, despite our increasing ability to produce and store information, our society still follows the approach of selective capture and storage. Once memory augmentation systems become a mainstream technology we may see a radical transition from selective preservation of knowledge to preserving everything and only selectively removing parts we find inappropriate.

We hope that this article can serve as a starting point for significant community research activity, in order to make progress towards an overall goal of creating safe and effective pervasive memory augmentation systems.

6. ACKNOWLEDGEMENTS

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).

7. REFERENCES

[1] Anderson, M. C., Bjork, R. A., and Bjork, E. L. Remembering can cause forgetting: Retrieval dynamics in long-term memory. *Journal of Experimental Psychology: Learning, Memory, & Cognition 20* (1994), 1063–1087.

[2] Edwards, L., and Harbinja, E. 'what happens to my facebook profile when i die?' : Legal issues around transmission of digital assets on death. In *Digital legacy and interaction*, C. Maciel and V. Carvalho Pereira, Eds., Human-Computer Interaction Series. Springer, 2013, pp. 115–144.

[3] Ellis Gray, S., and Coulton, P. Living with the dead: Emergent post-mortem digital curation and creation practices. In *Digital legacy and interaction*, C. Maciel and V. Carvalho Pereira, Eds., Human-Computer Interaction Series. Springer, 2013, pp. 31–47.

[4] Gemmell, J., Bell, G., and Lueder, R. Mylifebits: A personal database for everything. *Commun. ACM 49*, 1 (Jan. 2006), 88–95.

[5] Hayashi, E., Das, S., Amini, S., Hong, J., and Oakley, I. Casa: context-aware scalable authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (2013), ACM, p. 3.

[6] Hayes, G. R., Patel, S. N., Truong, K. N., Iachello, G., Kientz, J. A., Farmer, R., and Abowd, G. D. The personal audio loop: Designing a ubiquitous audio-based memory aid. In *Proceedings of Mobile Human-Computer Interaction* (2004), vol. 3160 of *MobileHCI 2004*, Springer Berlin Heidelberg, pp. 168–179.

[7] Kalnikaite, V., Sellen, A., Whittaker, S., and Kirk, D. Now let me see where i was: Understanding how lifelogs mediate memory. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2010), CHI '10, ACM, pp. 2045–2054.

[8] Langheinrich, M. Privacy in ubiquitous computing. In *Ubiquitous Computing*, J. Krumm, Ed. CRC Press, 2009, p. 95–160.

[9] Sellen, A. J., Fogg, A., Aitken, M., Hodges, S., Rother, C., and Wood, K. Do life-logging technologies support memory for the past?: An experimental study using sensecam. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2007), CHI '07, ACM, pp. 81–90.

[10] Stajano, F., and Anderson, R. The resurrecting duckling: security issues for ubiquitous computing. *Computer 35*, 4 (Apr 2002), 22–26.