*Digital Enlightenment Yearbook 2013*
*M. Hildebrandt et al. (Eds.)*
*IOS Press, 2013*

*doi:10.3233/978-1-61499-295-0-59*



# Not So Liminal Now: The Importance of Designing Privacy Features Across a Spectrum of Use

Lizzie COLES-KEMP [1] and Joseph REDDINGTON
*Royal Holloway University of London, Egham*

**Abstract.** There are many communities of ubiquitous computing users that are on the periphery of society, and these liminal users are often left to negotiate their relationship with technology without the help and support provided to more mainstream users. One such community is formed around users of Augmentative Alternative Communication (AAC) technology. Changes in the commercial landscape have brought within reach dramatic improvements in AAC and made them more accessible and supportive to their user community. These improvements, though overwhelmingly positive, amplify a family of personal data management problems that are similar to those experienced by more typical ubiquitous computing users. This paper argues that information manaagement practices deployed by the AAC user community are ones that mainstream society may benefit from using. Accordingly, this paper explores a number of personal data management problems that arise during AAC use and considers how AAC users have developed work arounds and information management practices to protect their personal information. Whilst this paper is focused on AAC technology, the responses could be generalised for a broader spectrum of society.

**Keywords.** AAC, information management practices, personal data, ubiquitous computing



## 1. Introduction

As we look back on the late 20th Century, immersive and ubiquitous computing that increasingly touches every aspect of our lives might possibly be regarded as one of the most notable aspects of this period. Technological innovations have combined into socio-technical methods of engagement and delivery such as smarter cities, "digital by default" service delivery and consumerisation of information technology, and these new digital capabilities affect the lives of many. These themes are often shaped by service delivery paradigm shifts and are fuelled by economic drivers such as consumer choice, just-in-time delivery, personalisation, cost-effectiveness, and latterly government programmes of "austerity measures". Increasingly, the citizen is not only a consumer of data but also a producer of data and much of that data is personal and related to individuals. The value of this data is dynamic and individual and requires an increasingly sophisticated range of tools to manage it.

[1] Corresponding Author: lizzie.coles-kemp@rhul.ac.uk.

It is sometimes argued that technology design is a process that helps society develop its use of technology. Indeed, it is often argued that envisioning and re-envisioning the human relationship with technology is an important aspect of the design process [1]. Sometimes envisioning takes place through the creation of new technologies and sometimes envisioning happens more in narrative form where technologies are developed from those narratives. The cultural roots of technology narratives have been the study of some research [2–4]. These narratives are useful not so much for any predictive quality [2], but for what they tell us about anxieties related to contemporary technology use.

When new technologies emerge they can, in some sense, be viewed as a blending of science fact and fiction [5] and users are often required to adapt their lives to include these new technologies. This is particularly true of ubiquitous computing technologies where users can be observed shaping the technology around their lives and shaping their lives around the technology. The complex interactions between individual, society, technology, and institutions are apparent in the case of ubiquitous computing, and in the way that humans and technologies are enmeshed through ubiquitous computing results in many forms of security and privacy issues. Similar to the way in which narratives in the arts point to trajectories of technology use, a number of reports have been produced that describe potential trajectories of ubiquitous computing and internet technology use and the potential for security and privacy risks inherent in the immersion of these technologies. Two such examples are reports from ENISA [6] and SWAMI [7] that envisage scenarios where the user is dependent, socially and professionally, on ubiquitous, internet-enabled computing and where the user routinely faces the need to exchange privacy for service delivery. The narratives point to concerns about the loss of user control over their personal data, the lack of awareness of the impacts of digital practices on others, and obfuscation of the true proposition being presented by service providers when exchanging user data for services.

### *1.1. The Liminal Vanguard*

Notably, in the narratives about complex social technology use, whether from the arts or reports from research groups such as ENISA, the user is typically characterised as both the consumer and producer of data, much of it personal. These narratives paint a picture of a society where smarter cities, "digital by default" services, and the consumerisation of technology are all facets of everyday life. The narratives in the ENISA and SWAMI reports illustrate how the perceived value of personal data is shaped by the context and the feelings and responses that the data evokes. The reports also show that, to describe the potential risks that may emerge, the categories of information risk need to be extended to include risks to identity, risks to personal reputation, and risks to psychological well-being. The ENISA report also makes recommendations as to how to mitigate the risks. The risk management recommendations are made on the assumptions that end-users have the cognitive ability to: make informed choices about the value of their personal data; decide on information disclosure; and use devices unassisted and independently. Crucially, they are also predicated on the notion that end-users can choose not to use the technology. However, what options for personal data management do users have if they do not possess these capabilities?

A technically-mediated world is already the reality for many groups of ubiquitous computing users and not all of these groups are independent users capable of unassisted

**Figure 1.** An AAC user with device.

use. This paper examines one such group: users who rely on technology to communicate with the world around them. Electronic Augmentative and Alternative Communication (AAC) systems enable individuals with severe speech impairment to verbally communicate their needs. In many cases these devices are life changing. A user's device is designed to give greater independence and improved opportunities of social integration. AAC devices enable users to construct utterances, many of which describe themselves or aspects of their lives, including their interactions with others and, as such, can be considered 'personal data'. AAC devices can be used in all areas of the user's life and are always-on devices that frequently require assisted, rather than independent, use. It is important to note that this is not an homogeneous user group: a wide range of different needs benefit from AAC use and the wider user community represents users with all levels of cognitive and physical ability. For these groups of users, responses to personal data management problems that are predicated on informed choice, independent use, and the right to opt-out will not be effective or useful and, as a community of users, they have needed to develop other ways of responding to these problems.

This paper explores how AAC users develop their information management and technology practices to overcome difficulties with personal data management, and explores what mainstream society might learn from their endeavours. It is structured as follows: Section 2 gives an overview of AAC, including the technical landscape, the nature of the community, the implicit privacy concerns, and a brief survey of related work. Section 3 goes into some detail on the nature of the challenges faced by both mainstream and AAC communities and illustrates how AAC users might be considered in some senses to be the 'liminal vanguard' of mainstream society's movement to ubiquitous computing. Section 4 gives three examples of information management practices performed by AAC users and evaluates how these might be developed into design and practice principles for mainstream technology use. Section 5 gives conclusions, an agenda for future research, and our acknowledgements.

## 2. Cyborg People. Here! Now!

Augmentative Alternative Communication (AAC) systems (Fig. 1) are used to supplement or replace communication for individuals with severe speech impairments. Often

electronic, such systems are frequently the only means that an individual has to be able to communicate needs (both immediate: "I would like a drink", and long term: "I would like to start divorce proceedings"), or interact with society. Modern internet-enabled AAC devices are designed in such a way that AAC users assume the dual role of producers and consumers of personal information. Moreover, this is not a small user community: the Domesday Dataset [8] records over 8,000 purchases of speech aids by the NHS between 2007 and 2012 and estimates the overall spend during this time on speech aids as around fourteen million pounds. However, other than extremely non-standard cases such as Stephen Hawking, this is a hidden community of ubiquitous technology users and one that is rarely, if ever, considered when reflecting on the use of ubiquitous computing in contemporary society.

AAC devices may excel at needs-based communication (e.g. "*I am hungry*", "*I'm cold*", "*get the phone*") but they are limited for real conversation [9]. Typical AAC devices tend towards a hierarchical structure of pages, each of which typically focuses on a context (e.g. shopping) or a category (e.g. clothes, sports), rather than observations or recent personal stories [10]. Work by [11] reports that spontaneous conversation with typical devices is slow and difficult (new utterances are typically constructed at a rate of between 8 and 10 words per minute, slightly more if, for example, word prediction is used). Using pre-programmed phrases (which give a much higher number of words per minute) can reduce the ability for self-expression [12], which limits the range of exposable personal data. In general, new utterances must be prepared in advance either by the user or a carer, which requires a significant overhead in terms of time and effort. It is this implementation of functionality designed to speed up utterance production that restricts the production of personal data rather than the underlying technology.

So, in the current generation of AAC devices, the implications for both personal data generation and its use are relatively small because the linguistic capabilities are small. Even so, a range of authors [12,13] have acknowledged theoretical issues such as: anonymity; personalisation of services; identity management; autonomy; and the changing of relationship boundaries through mediation. With enhancements brought about through the use of internet-enabled services such as geo-location, more refined and more accurate logging of both speech creation and movement, and the ability to integrate the AAC device into a range of internet-enabled external services ranging from internet banking to on-line gaming, these personal data management challenges gradually cease to be theoretical. Moreover, recent work by [14–16], and [17] makes explicit use of personal data (about both the user and other parties) to improve the functionality of AAC devices, this results in a very direct, although not necessarily explicit, trading of personal data for personal capabilities. Such work puts previous abstract models of user-privacy into sharp relief and exposes deep tensions between the aim of user empowerment (which these developments are aimed to promote) and the protection of AAC users from threats to their privacy and safety.

### *2.1. Rapidly Evolving Community*

The tension between user empowerment and user protection becomes even more evident when the trajectory of the development of this type of ubiquitous device is examined. The more sophisticated the use of the AAC device becomes, the more able an AAC user is to produce personal information and make it available to those with whom they want

to converse. At the same time, the more access an AAC user has to personal information related to other people, the more effective their conversations can become. The range of ways in which personal data is harnessed in the AAC sector is increasing dramatically. Apple's iPad has caused a huge investment in AAC software for tablet technology. Multiple third party applications (e.g. proloque2go,[2] JabTalk,[3] and Talkadroid[4]) already exist that allow this new range of tablets to function as AAC devices. Information from the (AAC) Domesday Dataset [8] shows widespread adoption of tablet technology with implicit, and typically mandatory, usage of cloud storage [18]. The overall effect of the tablet entry into the marketplace is that hardware devices are becoming more standardised in terms of size, shape, capabilities, and design, while at the same time the software that runs on such devices is exploding in terms of variety and capability, particularly in terms of the ways that personal data can be exchanged for enhanced and more efficient functionality. The lowering of the barrier of entry to AAC technology foreshadows the "panoply of different privacy problems" that privacy theorist [19] envisaged when contemplating worlds that are mediated through technology in an increasingly complex manner. For this community of ubiquitous computing users, the privacy problems include: establishing privacy for the AAC user that is separate from their carers; the communication of privacy options to non-literate users; the balance between the logging of user activity to promote more rapid or richer speech and user activity logging to protect the user; and the ability of the AAC user to communicate and experiment with the identity that they project. AAC devices are designed to increase social interaction in all settings and therefore the devices, and their supporting approaches, must be able to respond to all settings, as is the case with ubiquitous technology. Also, AAC users themselves develop their uses and desires for communication [12] as their identity evolves and their relationship with their AAC device changes. Therefore, any approach to personal data management has to be highly context sensitive and capable of responding to changing requirements.

As the capability for interaction increases, both in terms of the user's capabilities and the functionality of the AAC software, the potential for increased personal data also increases. This has been somewhat exacerbated by a new generation of devices that are capable of using tablet hardware to geo-locate and mine social media to increase language support. The variety of personal information stored on AAC devices includes not only information about the data subjects themselves but also carers and other members of a support structure: for example, devices that log utterances made by a literate user implicitly record the whereabouts of staff members, the exact times of conversations and the subjects they discuss. Similarly, utterances that have been generated from input by teachers, care staff and parents can again potentially contain information about other individuals, as well as increase the range of information about device users themselves. There are also more mainstream issues: internet access as a medium brings a range of issues for personal data use in terms of the methods used to broadcast and replay utterances and it greatly increases the possibilities for data input (potentially including information about third parties) into the utterances. The general browsing facility of internet access increases the ability of users to communicate with the wider world, carrying with it a set of personal data management and privacy issues, much of which is the subject

[2]http://www.proloquo2go.com, retrieved May 2013.
[3]http://www.jabstone.com/, retrieved May 2013.
[4]http://www.epidream.com/, retrieved May 2013.

of ongoing research [20–22] that is focused on personal data management within mainstream society. Interestingly, such research does not consider the existing practices of ubiquitous technology user communities for whom the standard and existing information management practices are not effective or workable. As has already been identified, the constraints under which personal information management practices and technologies have to operate are considerable and are constraints that apply to a spectrum of ubiquitous technology users, not just those dependent on AAC technology. One could then argue that this is not so much a specialised use-case but an extreme use-case that has something to offer wider parts of society.

### *2.2. Related Work in AAC Literature*

Although ethical issues in the context of complex disabilities are well studied, there is little direct research into privacy and personal data management issues in AAC, much of the work is in small accompanying sections to other research contributions and focuses directly on personal data dissemination. For example, [23] notes that externally displayed lexicons (such as a communications board) violate some aspects of privacy and proposes finding ways to ensure that vocabulary can be delivered discreetly without affecting access. Additionally, there is some meta-work that looks at the ethics of research into AAC rather than AAC itself: [24] notes that the data collected by AAC devices makes identification of the individual trivial, especially when considering the relatively small pool of users, a theme that is also examined in work by [25] on logging output of AAC devices.

Privacy has also been raised explicitly in the AAC community by researchers considering design frameworks for next generation devices, e.g. [12] and [13].

Work on the future of AAC and internet connectivity (in particular key features highlighted in [13]) have great bearing on personal data management, although privacy and personal data management are not directly discussed. [13] discuss simplified usability, including 'embeddedness' functionality: making AAC devices unobtrusive in their environment. When simplifying usability, there is a tension between requiring user intervention and decision making automation. For example, where should consent mechanisms related to personal information disclosure be placed in such devices? Should such mechanisms be usable by carers as well as AAC users and, if so, how is informed consent ensured?



## 3. The Design Challenge

The ENISA report perhaps most clearly highlights and exemplifies the best practice advice that is typically given to users and providers of ubiquitous technology. The content of the ENISA report focuses on life-logging applications and was created by a number of specialists with an outstanding track record in personal data management research and practitioner support. The report is a well researched collection of use-cases for typical, mainstream immersive ubiquitous computing use and the life-logging scenario means that it is particularly relevant to use it as a comparator with AAC-use scenarios. The ENISA report highlights that three groups of stakeholders have a responsibility for responding to personal information management risks in internet-mediated communications: the individual, the service provider, and the state. These three groups of stake-

holders are equally relevant for AAC-use scenarios [26]. However, in the AAC context, the user community represents a significant challenge to designing personal information management functionality as part of internet services: as already outlined in this paper – much of best practice guidelines does not take into account the constraints that face parts of the AAC community and therefore the focus becomes designing technology and practices for the user rather than to the guidelines.

The ENISA report points out that users must take advantage of and use privacy protection and security functionality and this is a common thrust of best practice advice when it comes to managing personal information. In terms of the individual, the best practice advice is based on the premise that individuals must be better informed and by being better informed the user has control of their own data. However, the recommendations do not refer to the non-user roles. The non-user is the 'significant other' in the AAC usage story. It is a regular theme in Human Computer Interaction literature that the non-user plays an important role in technology use [27] although they may never become users of that technology [28]. In AAC, the significant non-user is an important role and one that is often adopted by members of the carer team, including family, but also potentially by teachers, healthcare professionals and friends. In many cases an AAC user's interaction with the world around them is mediated through not only the AAC device but also through a carer or other non-user. This poses a design challenge because delegation rights need to be developed and made accessible to both the AAC user and carer, and at the same time, an empowered user should be able to control access to their personal data – including the ability to forget and hide utterances. In addition, the role of the non-user extends the boundaries of the AAC system to include the social protocols that are used to manage and engage with the device.

The recommendations from the ENISA report also characterise the most significant challenges to an individual's take-up of best practice as: being poorly informed; protection technologies being too inaccessible; and a lack of empowerment to take control. In the case of AAC users, these problems exist but so do the problems related to the ability to: forget utterances that are regretted, hide utterances from significant non-users and control the identity projected of themselves and others. These forms of personal data management pose a design challenge for AAC technology designers because the needs and rights of the AAC user have to be balanced with the duty of care towards the AAC user which carers feel that they have placed on them.

The report recommends that the service provider designs life-logging services with accessible, privacy-friendly default configurations and settings. The report also recomends that the service provider performs impact assessments and assesses the personal information management risks. Finally, there is a recommendation that the service provider is transparent about access to data and with whom it is shared. Service providers are also called upon to make individuals aware of and control the privacy risks associated with use of life-logging services. From a technological perspective, use of encryption and stronger authentication is advocated. The service provider is also encouraged to use multiple data stores and control access to those data stores. All of these requirements pose design challenges for AAC technology designers who often have little control over these issues, either because of the platforms upon which the AAC software is designed or because of inherent problems with the architecture of bespoke AAC devices. There is also a question of education; AAC designers are not security specialists and have typically not had security engineering training.

The state, on the other hand, is encouraged to try and create a regulatory environment that provides incentives for privacy-aware or privacy-friendly devices and services while supporting competition through promotion of interoperability and interconnection between devices and services, as well as providers. The report also encourages the state to conduct impact assessments on service designs and to make the citizen aware of both the benefits and risks of using the life-logging services; more importantly, they should also aim to educate the individuals of the risks and ways to protect themselves (e.g. the inclusion of privacy training in computer science education). At a federal level, states are encouraged to harmonise laws and regulations across states. Regulators in general are encouraged to create strong incentives for companies to include user interface "nudges" towards safer behaviour by customers, as well as to consider privacy requirements in early stages of product development. It is important to reflect on the fact that whilst the AAC user community may be a hidden one, it nevertheless is part of society and resides under the same overall regulatory and legal framework as the rest of society.

Whilst the best practice messages of the ENISA community are relevant, the AAC scenarios foreground constraints to the implementation of best practice that affect not only the AAC community that other user communities dependent on assisted use, affected by literacy issues and isolated from mainstream society.

In response to these constraints, the AAC community also demonstrates information practices developed to overcome these constraints and put in place privacy controls. The next section outlines these information practices and considers their usefulness for other parts of society.

## 4. You Are what You Disclose: Management of Everyday Tensions in Personal Data Management

Many everyday tensions faced by AAC users have parallels in the themes and scenarios that are projected in the ENISA and SWAMI reports. In particular, the life-logging context described in the ENISA report presents many of the trade-offs that AAC users and their assistors must negotiate. This section examines three such tensions in personal data management problems, they are constructed with input from legal experts, speech and language therapists, youth work practitioners, and disability officers, as well as from observations of non-literate AAC users. These examples focus on non-literate use of AAC, a user context for which traditional privacy and security technologies are not a realistic solution and techniques to stimulate informed consent are also not usable. The responses describe forms of information practices that can be seen as a type of security and privacy in the wild. Security and practices in the wild have been observed in typical user communities [29–31] but not previously in disabled communities.

It is important to recognise, when considering the following examples, that the AAC community is very wide and all combinations of different levels of cognitive, social, and physical capability are represented. To categorise and map the solution space is far beyond the scope of this work. Instead we choose several recurring solutions that have particular resonance with issues faced by mainstream users. As with all information practices, these examples are of innovative solutions found by a number of individual users, rather than responses from the AAC community as a whole.

### 4.1. Example 1 – Communicating who You Are

Manufacturers of AAC devices take pains to provide devices with carefully designed sets of pages that they believe are most useful for the communication needs of the general user (users can build their own from scratch, but typically they simply edit an existing framework to better suit their needs).

One of the communication needs recognised by manufacturers and Speech and Language Therapists alike is that a user will want to talk about themselves, and many page sets include a templated page to do just that. Examples of phrases on an 'about me' page might include such fill-in-the-blank sentences as "My name is X", "I am X years old", "I have X brothers and Y sisters" and also includes space for other personal information, for example "I really like Disney films". A major part of preparing a device for a new user is the completion of such 'about me' pages.

This 'about me' page replicates, almost exactly, the 'about me' pages that users of social media have on services like Facebook and LinkedIn: showing what a user likes, which social groups they belong to, and other aspects of what they want to project about themselves.

For some, literate, AAC users this 'about me' set of utterances effectively represents their 'cocktail party' level of conversation, allowing participation in a social ritual that potentially may have no other goals than the social interaction itself. However, for others, such a system can quickly become out of date in terms of their preferences (for example, "My boyfriend's name is Jeff").

Whereas a mainstream user of social media, or a literate AAC user, can periodically, and silently alter their interests or other aspects of their social identity, non-literate AAC users lack this luxury because almost all changes to the device require a high level of engagement with care staff, as the user must explain to the care staff some fairly high-level concepts about change and make very explicit their desire to change what biographical data is communicated about them. The carer, of course, has the ability to interpret and adjust what is communicated. When this page represents more than just interaction, it illustrates the limitations of control a non-literate user can have over the functionality to express identity.

An observed work-around adopted by some AAC users in response to this limitation amounts to a wholesale rejection of the concept of digital presentation and the 'about me' because its functionality is not fit for the desired purpose. Instead, the core language in the rest of the voice is used to express likes, dislikes, passions, and dreams, which makes for a more fluid identity constructed of feelings and emotions rather then descriptions and attributes. The expression of identity is performed through the expressivity of the language rather than the biographical details that are projected and offers non-literate AAC users greater control over the identity that is projected of them.

The development of a more expressive language that projects identity is perhaps also of value to mainstream users of social network technology and life-logging applications. From the personal page, to Myspace, to Facebook and LinkedIn, to Twitter – there has been increasingly less space devoted to static display of the user-as-snapshot – and greater expression about what the user has been doing recently. Personal information practices that encourage greater expressivity of identity are a further means of users retaining control over the identity that is projected about them. Rather than solely focusing on internet safety, education that encourages users to explore their on-line expressivity may also help users to set and control boundaries.

### 4.2. Example 2 – The Ability to Hide Utterances

The limitations of the static identity discussed above represent a specific case of a more general problem – the ability to hide or remove utterances. If a user has had the personal phrase "Becky is definitely going to win this year's X-factor" or even "My girlfriend Susan loves me very much" permanently added to their device, the non-literate AAC user may not wish to draw attention to it by asking it to be removed if they change their mind or want to deny it, instead choosing just to ignore the existence of the phrase.

We can draw parallels between the list of all utterances programmed into an AAC user's device and the list of all comments and statements by a user on social media. Again, typical users have the luxury of being able to periodically 'curate' their social media stream, removing unwise commentary, deleting things that do not meet the standards of sober reflection, and to potentially reclaim their identity by, for example, removing all photos of them with an ex-boyfriend or girlfriend. Such an action is, by nature, a very private one, and again a non-literate AAC user cannot take such a set of actions without drawing direct attention to it (this is also a reflection of the complex and very real factor that so much effort has been directed into putting *more* capability into an AAC device, that any effort to reduce the expressivity of the device is not in line with the design ethos). Consequently, typically the response from the AAC user community is one of community values and principles rather than personal information management practice or technology redesign.

In general, the wider AAC community holds with the principle that an AAC user does not have to hold a view or want to say a thing simply because they have the option to; in the same way that debaters can argue in favour of a contrary postion to the one they hold. It is understood by the community that the statement may have been entered by carers, perhaps long gone, or be part of a joke or a page set and therefore not necessarily attributable to the AAC user.[5] Therefore, the overriding principle that the AAC community abides by is that AAC users are not solely accountable for the content on their devices, and utterances are confirmed and contextualised by communication partners.

We can draw a parallel here with some social network strategies seen amongst today's social-media users – the cultural tropes of 'vaguebooking', 'schoolboying' and being 'hacked' all, perhaps not intentionally, but certainly effectively, give users a degree of deniability for their own posts [32] and acceptance by the community that content is not necessarily attributable to the social-media user. However, wider society has a significant way to go before it accepts that the content of a ubiquitous device and the content of social and life-logging applications in some contexts is not necessarily controllable by the user, and that additional corroboration needs to be sought to assess the provenance of published content. In addition to internet safety education and training, the development of programmes to promote better understanding of the limitations of the nature of internet publishing and the control of ubiquitous devices may encourage a reflection on societal values in this area.

### 4.3. Example 3 – The Ability to Forget

Unlike Section 4.2, which focused on utterances explicitly programmed into a device, this section focuses on the records of phrases spoken, both individual utterances and com-

[5]The issues around post-literate users are yet more complex and will be explored in future work.

**Dad Cat**
Would you like to tell your Dad about a cat Dave?
*giggles and nods head*
**Dad Cat**
What is it that you'd like to tell your Dad about the cat?
**Dad Cat Car**
Oh – you think we should send Dad to get a cat?
*nods, grins*

**Figure 2.** Example script between an AAC user and their care staff. Utterances in device history (bold), motions by user (italic), and speech by communication partner.

binations, and focuses on the challenge of forgetting what has been previously published. It would be natural to assume that conversations had with AAC users become part of a corpus of information: unlike spoken conversation, AAC devices create embodiments of conversations that can be permanently stored or logged. Then conversations become data that largely focuses on living individuals, either the users themselves or their family and friends. The permanent nature of these embodiments means that the users can potentially lose the right to forget their utterances, delete their utterances and configure the ways in which their identity is projected. Indeed, issues of personal data for post-literate AAC users include such cases as users wanting to ensure that statements they have given to doctors, police, and loved ones are unrecoverable.

The ability for AAC devices to have direct "forget" functionality is difficult for AAC devices because they are memory devices and, therefore, utterances are stored for the lifetime of the device (and in some cases the devices themselves function as an external memory storage location for the user). AAC devices are designed this way because of the dependency that a user has on the technology and the severe impact that losing their 'voice' can have. However, the way in which AAC conversations work actually reduces and potentially removes the problem of forgetting.

In practice, conversations with non-literate AAC users are not subject to anything like the problems of, say, emails or blogging. This is partly because AAC devices do not yet routinely record conversations (logging for research purposes is discussed in [25]) but, even for the ones that do, the nature of the conversations had with non-literate AAC users is such that the information recorded is of little use without the recollections of either the user or the communication partner. Figures 2 and 3 illustrate the level to which, for some AAC users, the communitation partner, location, and the user's physical movements give semantics to the utterances. This is therefore a form of mixed media or mixed mode conversation and, combined with the logging mode options outlined below, provides a natural means of degrading the ability to remember a conversation.

We consider two ways of logging AAC conversations. Firstly at the phrase level, keeping track of the phrases used in the last hour, day, or seven days: this is often a useful feature for the user as it helps users repeat recent comments, or carefully constructed phrases (for example, one might want to say "We were late because of heavy snow at Junction 14" quite regularly on the evening that one was late, but not necessarily have it on the device for posterity). Secondly, recording can be done at the level of individual button presses, which is a feature intended to be used by carers and Speech and Language Therapists to see how much use is being made of various aspects of the device (this is an 'opt in' feature often included in Dynavox brand devices). Interestingly, these log-

**Dad Cat**
Would you like to tell your Dad about a cat Dave?
*laughs and shakes head*
**Dad Cat**
Is it something that's happened before?
**Dad Cat Car**
Oh – you want to us to tell the present 3rd party about the time that Dad took the cat in the car?
*laughs*

**Figure 3.** Another example script between an AAC user and their care staff. Utterances in device history (bold), motions by user (italic), and speech by communication partner.

ging modes, particularly when used together, replicate the gentle degradation of human memory in a much more accurate way than typical electronic systems.

If, for example, a digital camera's memory degraded in a similar way to human memory, then the oldest images would gradually lose their resolution and detail as new images were added to their memory; eventually the older images would merge together and then disappear entirely. In the case of AAC devices we see that much of the information degrades in a similarly gradual way. When AAC phrases are first constructed, we can recall both their structure and the fact that they were created in the last hour. After the hour we know only that they were created in the last day, and shortly the last week.[6] Following the end of the week (devices with this capacity often allow users to specify the amount of time before phrases are removed) the information may exist only as recorded in the count of button presses on the device, and as time passes and more and other events are recorded as part of the button press count, the information gracefully degrades. In this way, some features of AAC design present an elegant case study of an electronic device whose memory gradually degrades, not by intentional design, but as an emergent property of the interface.

This combination of technology design and personal information practice is perhaps something that should be considered for the design of ubiquitous technology and social and life-logging applications for the wider community. As an approach it offers a range of possibilities and enhances the user's control over the ability to remember and to forget and is perhaps more natural and sympathetic to the particular technology and service use.



## 5. Conclusions

Advances in natural language generation and speech processing techniques, combined with changes in the commercial landscape, have brought within reach dramatic improvements in the design of AAC devices. These improvements, though overwhelmingly positive, amplify a family of personal data use problems. This work has argued that the challenges faced by AAC users in managing their personal information can be generalised for other communities affected by low digital literacy, low literacy levels, and cognitive challenges. Accordingly, this paper explored personal data management problems

[6]For space reasons we gloss over a certain amount of technical detail of timestamps, but this is programatically solvable.

and considers some of the work arounds that AAC users have developed to protect their personal information.

These everyday work arounds from AAC users point to a different cultural reality and therefore a different design fiction, one that security and privacy technology design tends to ignore. A combination of personal information management practices, cultural principles and values, and technology design offer alternatives and work arounds to the difficult problems of personal data management, content attribution and the ability to forget and remember content. Perhaps, in the early part of the 21st Century, mainstream society could take the lead from this liminal vanguard of ubiquitous computing users and adopt and extend some of their techniques for everyday technology use.

## Acknowledgments

The authors must thank the tireless effect of many inviduals who made contributions to this work, in particular Kate Williams, Liz Panton, Sarah Moffat, Claude Heath, Stephen Bieniek and many others.



## References

[1] L. Bannon, "Reimagining hci: Toward a more human-centered perspective," *Interactions*, vol. 18, no. 4, pp. 50–57, 2011.

[2] P. Dourish and G. Bell, "'Resistance is futile': Reading science fiction alongside ubiquitous computing," *Personal and Ubiquitous Computing*, 2008.

[3] G. Bell and P. Dourish, "Yesterday's tomorrows: Notes on ubiquitous computing's dominant vision," *Personal and Ubiquitous Computing*, vol. 11, no. 2, pp. 133–143, 2007.

[4] J. Tanenbaum, K. Tanenbaum, and R. Wakkary, "Steampunk as design fiction," in *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems*, pp. 1583–1592, ACM, 2012.

[5] J. Bleecker, "Design fiction: A short essay on design, science, fact and fiction," *Near Future Laboratory*, vol. 29, 2009.

[6] I. Askoxylakis, I. Brown, P. Dickman, M. Friedewald, K. Irion, E. Kosta, M. Langheinrich, P. McCarthy, D. Osimo, S. Papiotis, *et al.*, "To log or not to log? – Risks and benefits of emerging life-logging applications," 2011.

[7] P. Alahuhta, P. De Hert, S. Delaitre, M. Friedewald, S. Gutwirth, R. Lindner, I. Maghiros, A. Moscibroda, Y. Punie, W. Schreurs, *et al.*, "Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities," *SWAMI Deliverable D*, vol. 2, 2005.

[8] J. Reddington, "The domesday dataset: Linked open data in disability studies," *Journal of Intellectual Disabilities*, 2013.

[9] G. Soto, E. Hartmann, and D. Wilkins., "Exploring the elements of narrative that emerge in the interactions between an 8-year-old child who uses an AAC device and her teacher," *Augmentative and Alternative Communication*, vol. 22, no. 4, pp. 231–241, 2006.

[10] D. Beukelman and P. Mirenda, *Augmentative and alternative communication: Supporting children and adults with complex communication needs*, 3rd ed. Paul H. Brookes, Baltimore, MD, 2005.

[11] D. J. Higginbotham, H. Shane, S. Russell, and K. Caves, "Access to AAC: Present, past, and future," *Augmentative and Alternative Communication*, vol. 23, no. 3, pp. 243–257, 2007.

[12] T. Rackensperger, C. Krezman, D. Mcnaughton, M. Williams, and K. D'Silva, "'When I first got it, I wanted to throw it off a cliff': The challenges and benefits of learning AAC technologies as described by adults who use AAC," *Augmentative and Alternative Communication*, vol. 21, no. 3, pp. 165–186, 2005.

[13] F. DeRuyter, D. McNaughton, K. Caves, D. Bryen, and M. Williams, "Enhancing AAC connections with the world," *Augmentative and Alternative Communication*, vol. 23, no. 3, pp. 258–270, 2007.

[14] R. Patel and R. Radhakrishnan, "Enhancing Access to Situational Vocabulary by Leveraging Geographic Context," *Assistive Technology Outcomes and Benefits*, p. 99, 2007.
[15] R. Black, J. Reddington, E. Reiter, N. Tintarev, and A. Waller, "Using NLG and sensors to support personal narrative for children with complex communication needs," in *Proceedings of the NAACL HLT 2010 Workshop on Speech and Language Processing for Assistive Technologies*, (Los Angeles, California), pp. 1–9, Association for Computational Linguistics, June 2010.
[16] E. Reiter, R. Turner, N. Alm, R. Black, M. Dempster, and A. Waller, "Using NLG to help language-impaired users tell stories and participate in social dialogues," in *European Workshop on Natural Language Generation (ENLG-09)*, 2009.
[17] J. Reddington and N. Tintarev, "Automatically generating stories from sensor data," in *Proceedings of the 15th International Conference on Intelligent User Interfaces*, pp. 407–410, ACM, 2011.
[18] L. Coles-Kemp, J. Reddington, and P. Williams, "Looking at clouds from both sides: The advantages and disadvantages of placing personal narratives in the cloud," *Information Security Technical Report*, 2011.
[19] D. Solove, *Understanding Privacy*. Harvard University Press, 2008.
[20] E. Kani-Zabihi and L. Coles-Kemp, "Service Users' Requirements for Tools to Support Effective Online Privacy and Consent Practices," in *Procedings of the 15th Conference on Secure IT Systems, Nordic 2010*, 2010.
[21] P. Kumaraguru and L. Cranor, "Privacy indexes: A survey of westins studies," *Institute for Software Research International*, 2005.
[22] S. Spiekermann and L. Cranor, "Engineering privacy," *Software Engineering, IEEE Transactions on*, vol. 35, no. 1, pp. 67–82, 2009.
[23] M. Smith, "The dual challenges of aided communication and adolescence," *Augmentative and Alternative Communication*, vol. 21, no. 1, pp. 67–79, 2005.
[24] L. Pennington, J. Marshall, and J. Goldbart, "Describing participants in AAC research and their communicative environments: Guidelines for research and practice," *Disability & Rehabilitation*, vol. 29, no. 7, pp. 521–535, 2007.
[25] G. Lesher, G. Rinkus, B. Moulton, and D. Higginbotham, "Logging and analysis of augmentative communication," in *Proceedings of the RESNA Annual Conference*, Citeseer, 2000.
[26] J. Reddington and L. Coles-Kemp, "Trap hunting: Finding personal data management issues in next generation aac devices," *Proceedings of the Second Workshop on Speech and Language Processing for Assistive Technologies*, pp. 32–42, 2011.
[27] C. Satchell and P. Dourish, "Beyond the user: Use and non-use in hci," in *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7*, pp. 9–16, ACM, 2009.
[28] J. Redström, "Towards user design? On the shift from object to user as the subject of design," *Design Studies*, vol. 27, no. 2, pp. 123–139, 2006.
[29] P. Dourish, R. E. Grinter, J. D. De La Flor, and M. Joseph, "Security in the wild: User strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.
[30] L. Palen and P. Dourish, "Unpacking privacy for a networked world," in *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, pp. 129–136, ACM, 2003.
[31] J. Lingel, A. Trammell, J. Sanchez, and M. Naaman, "Practices of information and secrecy in a punk rock subculture," in *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, pp. 157–166, ACM, 2012.
[32] A. Lenhart, M. Madden, M. Duggan, and A. Smith, *Teens, Social Media, and Privacy*. Pew/Internet, 2007.
[33] M. Kamp, P. Slotty, S. Sarikaya-Seiwert, H. Steiger, and D. Hanggi, "Traumatic brain injuries in illustrated literature: Experience from a series of over 700 head injuries in the asterix comic books," *Acta Neurochirurgica*, pp. 1–5.
[34] P. Golle, F. McSherry, and I. Mironov, "Data collection with self-enforcing privacy," *ACM Transactions on Information and System Security (TISSEC)*, vol. 12, no. 2, pp. 1–24, 2008.
[35] J. Cornwell, I. Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor, J. Hong, *et al.*, "User-controllable security and privacy for pervasive computing," in *Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on*, pp. 14–19, IEEE, 2007.

[36] C. Karat, C. Brodie, and J. Karat, "Usable privacy and security for personal information management," *Communications of the ACM*, vol. 49, no. 1, pp. 56–57, 2006.
[37] C. Bonnici and L. Coles-Kemp, "Principled Electronic Consent Management: A Preliminary Research Framework," in *2010 International Conference on Emerging Security Technologies*, pp. 119–123, IEEE, 2010.
[38] L. Coles-Kemp and E. Kani-Zabihi, "On-line privacy and consent: A dialogue, not a monologue," in *Proceedings of the 2010 Workshop on New Security Paradigms*, pp. 95–106, ACM, 2010.
[39] S. Balandin, N. Berg, and A. Waller, "Assessing the loneliness of older people with cerebral palsy," *Disability & Rehabilitation*, vol. 28, no. 8, pp. 469–479, 2006.
[40] J. Todman, N. Alm, J. Higginbotham, and P. File, "Whole utterance approaches in AAC," *Augmentative and Alternative Communication*, vol. 24, no. 3, pp. 235–254, 2008.
[41] S. Reilly, J. Douglas, and J. Oates, *Evidence-based practice in speech pathology*. Whurr, London, 2004.
[42] L. Wittgenstein, *Philosophical investigations*. (Trans. GEM Anscombe). Basil Blackwell, 1956.