Looking at Clouds from Both Sides: the advantages and disadvantages of placing personal narratives in the Cloud

Lizzie Coles-Kemp, Joseph Reddington and Patricia A.H. Williams

Abstract

This article explores the nature of cloud computing in the context of processing sensitive personal data as part of a personal narrative. In so doing, it identifies general security concerns about cloud computing and presents examples of cloud technologies used to process such data. The use of personal narratives in electronic patient records and in voice output communication aids is compared and contrasted and the implications of the advent of cloud computing for these two scenarios is considered.

© 2011 Published by Elsevier Ltd.

Keywords: Cloud, Healthcare, Disability, AAC, VOCA

1. Introduction

This article explores the advantages and disadvantages of using cloud computing in the context of processing sensitive personal data as a personal narrative. It focuses on two personal narrative examples and identifies tensions that subjects face with the adoption of cloud computing as a platform.

Information security architectures typically presume the ability to erect perimeters, both physical and logical, around areas of trust and control. An institution can control the flow of their information by controlling when and how information crosses boundaries. In the cloud environment parts of the perimeter move to the cloud and institutions must trust the cloud provider for perimeter control maintenance. In this sense, cloud computing follows on in the tradition of de-perimeterisation problems [1].

The main draws of cloud computing include, its configurability, availability and ease of support. Draft-NIST-SP800-146 defines cloud computing as: “a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” [2], and this definition is echoed in other cloud literature [3, 4]. Draft-NIST-SP800-146 also defines five essential characteristics: on-demand self-service; broad network access; resource pooling; rapid elasticity, and measured service. These characteristics are appealing for the provision of services to mass markets that require an element of self-service administration by the service user, by service providers who require high service availability at low cost, or who have a desire to outsource platform support. Health care, social care and education are all institutions for whom these characteristics are very appealing.

This article considers the domains of electronic patient records in healthcare and of vocabulary, utterance and log storage for Voice Output Communication Aids (VOCA). Electronic patient record (EPR) keeping enables healthcare professionals to store and process medical records digitally. With the advent of EPR, there is the ability to “push the boundaries” of healthcare [5] and to use the record to document the health of the patient in any number of contexts.
Moreover, the record can be shared with different health and care institutions for purposes such as data-mining and to extend the cycle of care given to a patient. EPR information comprises personal narratives about the health of an individual, and thus about the individual themselves.

At the more direct end of the digital personal narrative spectrum, VOCA devices enable individuals with little or no speech to verbally communicate their needs, often using Text-to-Speech technology. Such devices are designed to give communication impaired people greater independence and improved opportunities of social integration. The devices enable users to construct and store utterances, many of which describe themselves or aspects of their lives, including their actions with others and can thus be considered ‘personal data’. Personal data is defined in the Data Protection Act 1998 as data that relates to an identifiable living individual [6] VOCA devices can store personal narratives covering any aspect of a device user’s life in the same way that medical records contain an effective narrative of personal data whose value depends on the particular state of the individual.

To protect personal narratives, it is vital to comply with regulation, make access permissions configurable by both institutions and individuals and give individuals the capability to delete data. In the EPR scenario, data protection requirements are understood and institutional compliance apparatus is in place. In the VOCA device environment, data protection requirements are less well understood [7]. Access control at the institutional and personal level is extremely complex in both scenarios and will be explored further in this article.

For both EPR and VOCA technology, cloud technology is emerging as the default platform, almost by stealth. In this article EPR and VOCA service providers using cloud technology are termed “service user”, the users of their services are termed “end-users” and the cloud providers are termed “cloud infrastructure providers”. Classically, four deployment models are presented [2]: private; community; public; and hybrid clouds. The differences between these deployment models are significant in security terms because of the differing levels of control offered to institutions using cloud infrastructure and to those using the services provided by those institutions. The level of control possessed by both an end-user and service user of cloud computing depends on the model of deployment and therefore some models require a greater dependence on the cloud provider for security of data than others. Typical approaches to cloud security produce one-size-fits-all governance and technology security architectures; however, the level of control offered to an end-user of cloud computing depends on the physical location of the cloud and the service provider and the service user’s technical ability to configure protective boundaries around the cloud resources.

These dependencies have the potential to pose problems in the EPR and VOCA technology scenarios. In particular, the one-size-fits-all approach is potentially problematic for applications that contain a blend of personal data and sensitive personal data, particularly in applications where the value of the personal data is fluid. The conditions under which this type of data can be processed are context dependent and there are scenarios in which the physical location of the cloud platform and the access rights to the data pose issues at different times. This level of necessary protection is variable and can be traded for accessibility depending on the context at that moment in time. For example, EPR contain a blend of personal data, much of which resides in the narrative contained in the medical record which documents the patient’s views about their health. As an example, the need to access a patient’s description of their symptoms can vary over time. If a patient’s conditions worsen, the need to access these details can increase and the significance of these details can increase. In addition, the need to share these details with other healthcare service providers can also increase. These types of changes are today controlled using informed consent. However, in the EPR and VOCA scenarios where end-users have various levels of cognition, literacy and digital literacy, technology design is key to delivering informed consent.

2. Cloud computing in the context of EPR

The benefits associated with on-demand service provision make cloud computing an attractive alternative to traditional IT service delivery for the healthcare environment. Industries such as healthcare, where computing is a support service and not a core business function, often use external outsourcing for technical support. The benefits of digitizing a person’s health records for cloud storage are the reduction in administrative complexity and the increased mobility of access. From a patient perspective the flexibility and consistency of access to their medical history (within the limitations of what is uploaded) provides an incentive to have greater input, autonomy and management of their health status. However, the complexity of EPR systems and the security needed for the data they contain makes using a cloud computing solution problematic and problems are compounded by the unstructured and dynamic nature of the personal narratives that EPR records can contain.
Cloud computing enables greater flexibility in EPR access, enables end-users to have access to their records on demand, enables end-users to be active managers of their own health record and extends the use of EPR into other aspects of healthcare:

- Microsoft HealthVault, which was launched in 2007 is designed as a direct-to-consumer system which facilitates self-service by the end-user. Thus, end-users can create a record of their health data, manage who has access to it, and import data from monitoring medical devices. It also links to other applications to promote ease of uploading information such as prescriptions from pharmacy providers, and integrated health promotion tools [8]. This conceptualisation of a health record extends the boundaries of the use of health records in the way that Layzell et al [5] discussed. The nature of the cloud computing platform facilitates the sharing of EPR data across services and between service providers but also increases the number of stakeholders and systems sharing that data.

- Cloud subscription services, such as Dells MSite, Flexiant's Extility and GE Healthcare's Centricity provide specific healthcare information system platforms using private clouds and a full range of technical services including disaster recovery. These types of services provide both electronic healthcare record solutions and practice management applications [9]. This also gives healthcare providers opportunities for mobile clinical computer applications that might otherwise not be possible with current internal infrastructure. Inherently, the private cloud should offer increased (or at least more traceable) information security and privacy leading to more transparent compliance. Major cloud providers are investing heavily in the infrastructure to support cloud services as well as structure to support the use of these services to attract healthcare providers [10]. This flexibility enables EPR systems on demand and increases the range of applications that can read/write to an EPR. It also de-perimeterises EPR systems by enabling the potential for greater and diversified EPR access.

Early adopter case studies, such as Miami Jewish Health System [10], indicate that the business drivers and increased operational efficiency together with improved patient care have given rise to the implementation of cloud solutions. Efficiency savings are a powerful driver for introducing cloud computing into the delivery of EPR. Simplifying information technology delivery and reducing costs are persuasive arguments for using these services. We note that whilst healthcare delivery is about patient care, there is a huge administrative element to any healthcare organisation and the use of cloud services for both data storage and software deployment can be beneficial as for any large commercial organisation.

Empowering end-users to have active control of their patient record and give the end-user easy access to their patient record, promotes the concept of a more patient-centric healthcare system. The UKs National Health Service E-Health Cloud project, piloted at Londons Chelsea and Westminster Hospital in 2011, moved its patient records to a centralised database in the cloud. The move was claimed to show an emphasis on providing a better communication channel between the patients, consultant and GP [11].

There is a privacy and security trade-off for EPR systems. Whilst these benefits may bring patient empowerment on the one hand, it also potentially reduces a patient’s control over the flow of their health data. As the examples above show, EPR systems delivered using cloud technologies, increase availability and configurability of patient records. However, deploying a security model to control access is complex because much of an EPR is unstructured and comes in the form of narrative where the healthcare professional records the patient’s views during consultation. This narrative can have varying levels of sensitivity and varying levels of relevance for different healthcare teams. The value of this narrative is also intrinsically linked to the care that a patient needs at any moment in time. Communicating these fluid and dynamic security requirements to a third party provider is difficult. Typically, security requirements are communicated in a one-time fashion using a service contract, rather than communicating variations to requirements as the context dictates. In the case of EPR, an alternative means needs to be found.

From the security perspective, healthcare information gathered in the cloud is an attractive target for malfeasance. Unfortunately, getting accurate data on any security breach is difficult particularly in countries where there is no requirement for breach reporting. However, what data is available shows that (in the US) hacking is responsible for only 6% of health data breach, whilst some 60% is due to physical theft and loss [12]. The cloud is then no less safe, and perhaps safer currently than other local solutions. However, in the cloud scenario, there are complications in questions of standardisation, ownership, legal compliance and the longevity of data. These points are expanded below.
2.1. The implications of cloud computing for healthcare

Providing on-demand services, increasing end-user control over their records and extending the use of EPR into other aspects of patient care raises a number of challenges for the healthcare sector. A major concern with cloud computing is the unknown nature of the details of the security provision and perceived service user and end-user’s lack of control over the placement, processing and security of information. In opting for a cloud service delivery model, fundamental security issues associated with externalising data management become apparent; for example, relinquishing control when integrating internal and external services. This is in addition to major issues in adopting models of cloud services, which include: lack of security standards; questions of ensuring confidentiality and integrity of data stored in the cloud; and ensuring regulatory compliance is met. These issues are expanded on below:

2.1.1. Trust, standardisation and ownership

An issue in the use of cloud based health databases is convincing health practitioners to use them. This is based on the premise that a reliable and useful patient record will only be created if support and information is uploaded by the healthcare provider. Most healthcare providers will not give out test results and other aspects of medical records and without healthcare providers using the system, no useful record system can be created [13].

The biggest challenges are the lack of consistent and interoperable security and data access infrastructure and agreed recording methodology (‘coding’ in healthcare terms) that is required in health records. It is this lack of standardisation and the inevitable use of personal narratives, that is the basis for the difficulty in sharing electronic health records for all local and national systems. This data becomes virtually unusable for monitoring and maintaining the quality of personal health care. Whilst the use of cloud services for an individual may appear desirable, its use in ongoing healthcare is limited if it cannot be guaranteed that all significant episodes of a patient’s health care are catered for. At a fundamental level, the consistency of coding of critical data elements such as medications, allergies and problems will limit the records usefulness for clinical practitioners.

In addition, and no less significantly, the ownership of data is becoming more complex in regards to control and responsibility. In any healthcare system currently, the patient does not own the data that is recorded about them and used to provide their care. The healthcare provider is the owner or the custodian of that data. They therefore have control of that information when it is in situ. In the cloud the service provider actually retains the control over access. The question is then, particularly if the service is at no cost and no agreement has been entered into, is the cloud service provider the custodian of that data? In general the person or organisation who created the record owns it [14], which clearly becomes complex when a patient adds to their record but with information created from another source, such as test results or a summary from a primary care practitioner or hospital discharge summary. This is further complicated by the nature of the record. From a patient’s perspective, they are communicating with their health practitioner and their expectation is that this narrative is looked after by their practitioner. Explaining the complexity of EPR ownership potentially changes the trust relationship between the patient and the practitioner.

2.1.2. Access, privacy, legislation and hacking

The nature of the information held in healthcare and the privacy issues that drive much of the discussion on sharing patient data, are also overarching concerns foregrounded in the cloud context. It is this multi-faceted vulnerability of data and services utilising the cloud that is most difficult for end-users to comprehend. Further, in publicly available databases (and advertiser controlled) there is also the issue of linking to other sites and services the company owns. Whilst linking may appear a good use of information, it also means that added security must be taken to ensure that cross service security incidents do not compromise the health records one.

Another major issue for any cloud solution is the need for laws governing the protection of the information. Unlike specific location based authority, and organisations such as hospitals, where legal protection mechanisms are in place, cloud solutions pose more difficult jurisdictional questions [13]. Consumers need to be clear what authority and legal framework their data is encompassed by; significantly, the US, Europe and Australia all have significantly different legislation around the protection and access to medical information. Similarly, another area of concern not fully addressed and linked to regulatory compliance, is that of cross border information flows and compliance to local and originating privacy laws. There will be obligations based on patient consent and confidentiality agreements between the patient and healthcare provider that must be ensured as consistent with the cloud infrastructure provider. This is an issue and discussion that will need to occur before widespread adoption of cloud services will be seen [10]. Data
at rest (where it is stored) is a key issue since data that resides on a storage device in a country, comes under the laws of that country.

Educating and communicating with patients about the nature of privacy issues and communicating the changes to access is not trivial and communication mechanisms need to take varying levels of literacy and cognition into account.

2.1.3. Longevity, stability of providers and quality of service

Longevity of data stored in the cloud and the longevity of cloud solutions are open issues. In a particular recent case, Microsoft agreed to transfer those records that were formally stored on Google Health to HealthVault, when the former closed. This raises difficult questions not only about ownership but also how long those records are to be in existence. In addition, in the US at least, reticence to use a public system by consumers is due to a lack of confidence that the data will not be put to some other use by health insurance companies and others who may be given access [15]. Another concern is the on-going availability of services when required and the dependency on the Internet connectivity are rightly causes for concern.

3. Cloud in the Context of Voice Output Communication Aids

There is a parallel between the issues of ownership, access, standardisation and longevity identified for EPR systems and those found in the context of Voice Output Communication Aids (VOCA) used by individuals with limited speech to formulate and output utterances. As in the case of EPR, much of the data that a VOCA device stores and processes is in the form of a personal narrative. The VOCA manufacturing industry is currently undergoing major changes (we discuss further in Section 3.1). Previously, relatively few manufacturers dominated the field with systems that, while serviceable and robust, are also expensive [16] and firmly rooted in early 1990’s philosophy of design. A situation existed that innovation mainly focused on the inputs and output to any given system rather than the system as a whole. As a result, the security features of the VOCA platform is not consistent and does not address the full range of security issues [7].

To understand the implications of cloud technologies on the VOCA market, the data control implications of future technologies need to be identified and understood. The potential for innovation is well-supported by recent research trends: work by [17], [18], and [19] makes explicit use of personal data (about the end-user and other parties) to improve the use of VOCA devices. Such research moves toward VOCA devices that automatically generate text from, e.g., GPS sensor data or internet sources (such as talking about the weather or recent trips) that can be coupled or merged with input from other sources, increasing the ability of users to develop additional novel utterances. Depending on context, the use of these utterances may be controlled under data protection legislation in institutions such as school and work or in social settings, such as the home, their use may be influenced more by social norms.

From a security perspective, it is important to model VOCA devices as location independent where the personal narratives held on the VOCA device can be of interest to family, education, health and social care institutions as well as the individual. An example of a VOCA device is illustrated below; it should also be understood that VOCA device users may use their devices in any aspect of their lives. As a result, the device can hold banking information, health information, tax and personal administration information as well as social and needs-based communication. This information will be stored in forms of personal narrative and not in an ordered, segregated filing system. The wide range of data and information is due to the fact that devices are ubiquitous and used in the home, out shopping, when travelling, or when taking part in a youth group - in essence these devices are the user’s ‘voice’ and can be used anywhere. Thus utterances can include all manner of comments and diary events: including family events, mood changes at home, what the user ate for tea and what they watched on television. Perhaps the best analogy for this type of device is a speaking diary that contains mainly free text, analogous to the aspect of EPR which can be regarded as a type of health diary.

3.1. The Implications of Cloud Computing in the Context of Voice Output Communication Aids

In a similar way to the provision of EPR systems moving to cloud platforms because of changes in the industry delivering the services, similar shifts are also changing the nature of VOCA devices. The introduction of cloud into the Augmentative and Alternative Communication (AAC) arena is happening by virtue of the change to the VOCA manufacturing industry. In 2010 Apple released the iPad, followed by the iPad 2 in early 2011. From an engineering
perspective the iPad only suffers in comparison to existing devices in terms of ruggedness; however, at potentially one fifth the price\(^1\), it is comparatively replaceable. From a software perspective the iPad gives many ‘cottage industry’ developers for AAC a low cost way to enter the VOCA market. Such developers already include Alexicom, TapToTalk, Prologue2go, and MyVoice. Such developers are well placed to take advantage of the platform’s underlying hardware. MyVoice provides location-based vocabulary choosing using the platform’s GPS, whereas Alexicom, TapToTalk, and Prologue2go use cloud based storage to sync between devices. Lastly almost all applications integrate flawlessly with Internet searching, emailing and SMS use.

Given the comparatively massive market capitalisation of Apple, this challenges the position of traditional VOCA manufacturers. In fact, Apple represents simply the tip of a tablet iceberg - companies such as Samsung, HP, and (via the Android operating system, and the purchase of Motorola) Google \([20]\) have invested heavily in tablet technology, and it is likely that one or more manufacturers will move to develop a ‘ruggedised’ tablet device for either military or medical use. Such a tablet, particularly if it made use of the android operating system, which has its own large group of dedicated developers, would open a ‘second front’ from the point of view of the existing manufacturers. There is a potential future landscape dominated by many small software developers on a range of platforms. The use of cloud technologies is implicit in this development because the platforms on which these applications are built, are steeped in cloud technology. Such technologies could potentially arrive very quickly. There are, of course, casualties. The earliest known electronic AAC device was the Patient Operated Selector Mechanism, created by Reg Maling in 1960 \([21]\), Maling went on to found Possum, an assistive technology company, which last month announced it was withdrawing from the AAC market, in part due to the competition from iPad and android devices \([22]\).

The full implications of this market shift for security and privacy are unknown but AAC is a market that already lacks a consistent information protection and control architecture \([7]\) and it is a market in which there has been relatively little discussion of the implications of technology development for the rights and capabilities of the AAC technology users. Ownership of the data on the VOCA device is a complex issue but the complexity is somewhat different to the ownership problem in EPR. In the case of VOCA devices, there are intellectual property rights issues and complications related to the cognitive ability of some of the VOCA device users \([7]\). This has the potential consequence of VOCA users losing control of their data. This potential problem is compounded by the move to the complex cloud environment: a move happening by default rather than by design. In the cloud scenario, the data is stored in the cloud and the ownership of that data is dependent on the agreement in place. There are also issues related to longevity of data, transfer of data and access to data that parallel the problems described for EPR. Given that the AAC market is dominated by small software developers and by users with individual and, from a security technology perspective \([7]\), non-standard security and privacy needs, many of the standard responses for cloud security \([1]\) can not be deployed and therefore need to be designed into the technology itself. For example, many VOCA device users can not simply opt out of using cloud technology as it is becoming the de-facto platform for an essential service but thought could be given to options for storing certain types of narrative locally. Also VOCA device users can have forms of cognitive impairment so the interpretation of options for security and for understanding the terms of the consent can require additional support. Encryption also is problematic, given the potential for the need for multi-agency and intra-institutional access.

\(^1\)Based on a £3000 per VOCA device estimate from \([16]\)
3.2. Examples of access control and data ownership issues in an AAC context

Figure 2 shows information flows in a non-cloud environment. We note the information flows are varied and take place in device to device, human to device, and VOCA-mediated human to human flows. For example, this information flow diagram can be considered in the context of the “How was School Today...?” (HWST) project [18, 19], which generates stories for students with complex communication needs at a special needs school by electronically tracking student interactions. In this figure, it can be seen that there are many possible input and output streams for the VOCA devices. It is also important to appreciate that VOCA device users often do not use their devices unsupported and that family and social care “scaffolding” is unlikely to diminish. Therefore the stakeholder picture is complicated: there are the device users themselves, the non-device users in a scenario that may be featured in the personal narrative, the institutions who support the device users and the service and technology providers. The cloud introduces an additional set of technology providers and potentially increases access by other service providers.

In this scenario, potential utterances built in school include:

- details about events in the classroom, including events in which involve third parties,
- information about personal routines such as visits to the lavatory, the user’s eating choices and medication record
- impressions of AAC-user mood both by staff working with the individual and the AAC-user themselves
- levels and types of contributions in the classroom

Due to the digital nature of VOCA utterances, personal data output by a device is regulated by data protection legislation when being processed in the context of institutions such as schools, health, or social service. Young adult AAC-users with sufficient cognitive abilities are the data controllers under data protection legislation. “Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.” [6] However, as speech, language and communication disabilities are regularly a pan-disability, the AAC-user may also be cognitively impaired and a parent or guardian, would in that case, be regarded as the data controller. In the cloud scenario, the cloud infrastructure provider might become a data processor. "Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller” [6]
When thinking about the types of data flow controls that can be developed for a VOCA device it is important to understand that AAC users will typically have considerable intervention from education and health support workers. Unlike spoken forms of conversations in other care situations, AAC utterances have a digital embodiment which makes them similar to EPR narratives. Whilst many institutional issues are related to personal data use, importantly, AAC users are likely to use devices for personal data disclosure outside of the institutional context as part of family and social life. In this instance processing is controlled by social norms and practices that could be considered a social contract.

When cloud computing is introduced into the school scenario, such as HWST project, the potential opens up for the personal narratives to be distributed across a number of physical and geographical locations and for access to be available to the third parties supporting the VOCA platform. In the cloud computing scenario a VOCA device user’s ‘voice’ can be stored in the cloud. For the device user this brings a more guaranteed availability, which is extremely valuable for those users dependent on the device for communication. For the AAC manufacturer the cloud reduces infrastructure costs and enables an outsourcing of the maintenance of the service. However, the introduction of the cloud further complicates an already complex stakeholder picture.

In the HWST context, cloud computing results in data about a child’s movements and interactions being stored by a third party (the cloud infrastructure provider). In order to reduce chances of unauthorised or unexpected data access, the data could be encrypted between the device and the cloud and when the data is at rest in the cloud. However, this data might need to be shared between multiple institutions at various points in the AAC user’s life and the key management complications in terms of resource and technical capability could make plain text preferable for cloud service users and their institutional customers.

Defining the security requirements to be placed in the service agreement between the cloud infrastructure provider and the AAC service provider and then ultimately the end-user is difficult and provision would need to be made for potential requirement change. This is because the value of data varies depending on what is entered into the personal narrative and the current circumstances of the VOCA user. VOCA devices, as a simple example, can be used to store bank details, pin numbers and so on. Another, more complex scenario, is that a VOCA device user stores an utterance about an event that happened, which at the time, had little value but as circumstances change the content of the utterance becomes more sensitive and the implications of unexpected disclosure, greater. In these scenarios, VOCA device users may want to opt out of cloud storage for that part of their narrative.

4. In conclusion: Moving personal narratives into the cloud

In this section we consider the implications for personal narratives, both in medical records and in VOCA devices, when moving their processing to the cloud. In the case of EPR, the cloud is already in operation. In the case of VOCA devices, the personal narratives have the potential to move to the cloud by virtue of the platforms they reside on. In the case of EPR, systems are often designed with the cloud in mind. The general challenges, common to both EPR and VOCA, for moving personal narratives into the cloud are:

- Variable nature of the sensitivity of the narrative
- The need for multi-party access to the narrative by different health, social care and educational institutions
- The variable and often low technical ability of the service user
- The question of ownership complicated still further
- The terms of the longevity of the data
- The lack of security design in the client device

When considering the security problems of the cloud [1] responses include:

- the use of encryption for data at rest and in transit,
- the deployment of additional perimeter controls by the cloud service user,
the use of informed consent and the ability to opt-out by the individual.

In the case of the personal narratives that we are considering, these security responses are all problematic. The use of encryption is fraught because of the number of institutions potentially requiring access. These institutions potentially have different encryption standards and different key management capabilities. In addition, in the case of VOCA devices, the devices are supported by family and social care members who often do not have a high level of digital literacy. In addition, the need for access by the individual and by the institutions change depending on the scenario. In the case of EPR, access to medical information depends on the condition of the patient and a parallel can be drawn in the VOCA device environment. To always permit access by the institutions can remove privacy rights from the individual, equally there are times in the care of the individual when access could be required. Hence, “break the glass” policies need to be considered where access policy overrides can be implemented. This is already considered in EPR design but the lack of a standardised security platform for VOCA devices means that this, today, could not be implemented. The deployment of perimeter controls requires technical capabilities by both the individual and the institutions. To a lesser extent this is challenging for EPR systems, although it is a much greater issue for AAC platforms.

It is in many contexts expected that the implications of cloud computing will be understood by the terms of the service agreement and the legal apparatus of informed consent. However, in the case of both EPR and VOCA devices, the design of informed consent needs to consider different levels of cognition and literacy. A total opt-out in the case of personal narratives is not an option for users. However, technology design should consider opt-out for certain aspects of the narrative.

In conclusion, cloud computing, whilst not necessarily making personal narratives of the type discussed more insecure, does foreground and accentuate a number of security and privacy issues, the solutions to which are not readily available and will require, in many instances, technology redesign.

References

URL http://www.aclweb.org/anthology/W10-1301


URL http://www.bbc.co.uk/news/business-14530543

URL http://informahealthcare.com/doi/abs/10.1080/07434619412331276740

