End User Effects of Centralized Data Control

Peter Imrie and Peter Bednar

Abstract Within distributed technologies there is a need to manage and control the data stored on devices for it to be useful. This control can include limiting what data is stored on the device, applying software updates from different sources and even accessing the private data that is stored on the device. Different approaches have been taken to manage the content on distributed technologies and some of these methods have the potential to negatively impact their usefulness to the end user. In this paper we look at approaches for managing data within the contexts of either the end user or a centralized server and their effects on the usefulness of the support to the end user. Following this we discuss advantages and disadvantages and give examples of technologies that utilize different methods of data control and discuss our conclusions within the context of end user support.

Keywords Data control · Data management · Access control · Categories of support

1 Introduction

Recently the US Navy has announced [1] their new approach to distributing eReader technology to the staff on their vessels. Due to the nature of the environment in which the device is used, there is a desire to manage the connectivity and data stored on the device to ensure it is secure [2]. Although this approach was found to be secure for use within the US Navy the implementation can potentially

P. Imrie (✉)
University of Portsmouth, Portsmouth, UK
e-mail: pch.imrie@gmail.com

P. Bednar
School of Computing, University of Portsmouth, Portsmouth, UK
e-mail: peter.bednar@port.ac.uk

P. Bednar
Department of Informatics, Lund University, Lund, Sweden

T. Torre et al. (eds.), *Empowering Organizations*, Lecture Notes in Information Systems and Organisation 11, DOI 10.1007/978-3-319-23784-8_17

limit the usefulness of the device for the user. Within this scenario the usefulness of the technology to the end user is affected by the very same limitations designed to improve the devices usability [3]. This scenario also demonstrates the need for our on-going exploration of the different approaches to data control and the effects of each from the perspective of the end user.

In this paper we begin with drawing upon the different categories of support that have been previously described [4]. The categories of support can be used to help us to relate the relationships between categories of who controls the data used by the end user with categories of who has access to this data. By discussing the relevant categories (and their relationships) we create a basis for categorising the different methods of content control within the context of who benefits from the control of the data (and potentially in what way). Following this we will discuss a number of strategies for data control as identified by their interactions with a centralized system (not controlled by end-user). These strategies categorise the technologies approach to controlling data. Once we have an understanding of the categories of support and the strategies for data control we analyse key advantages and disadvantages of each strategy/approach to data control and how it affects the end user (from the end user point of view). This is supported with examples of identified type of support. The findings of this exploration are concluded with a brief description of key advantages and disadvantages of each approach including their potential impacts on the end user.

2 Background

Recent events have drawn highlighted issues with the security and control of personal and public data [5–7]. Many users are now paying attention to who has access to their data when using a service or mobile technology. As advances in connectivity are promoting a more centralized approach to data management with 'cloud' technologies and distributed services it is becoming more important to be aware of the advantages and disadvantages of this approach. With the continual development of Internet of Things (or indeed internet of everything) these and similar data control issues are becoming more and more relevant to address and explore from many stakeholder perspectives.

When discussing these advantages and disadvantages it is important to take into account multiple stakeholder views of each point (including the "end-user" or "client" etc.). Usually, disadvantages for one stakeholder would not (purposefully) be implemented unless they were advantageous for another. This means that something (e.g. feature) may be seen by a manufacturer as an enhancement of usability (for the end user). The same feature can be perceived by the end user as negatively impacting the usefulness of "their" device. Within this context the distinction between usability and usefulness is defined by the stakeholder that perceives an advantage of a device "in the context of their own actual use in their own real life situations". If a device is more usable then it may have more possible functionality or potential usefulness, but the usefulness is not guaranteed. A device is more useful if the end user sees these possible functions as an effective solution [3].

2.1 Categories of Control

The controller of the data can be categorized drawing upon the previously developed categories of support as part of a model of infrastructure [4]. The categories described within this infrastructure help to identify key differences between what may on the surface appear to be similar approaches to providing support to the end user while handling data in different ways. The specific categories we will be focusing on are the user controlled services and the information service provider categories as seen within Fig. 1.

2.1.1 Information Service Provider

The information service provider category of support utilizes centralized data control to provide services for the end user. The information service provider has

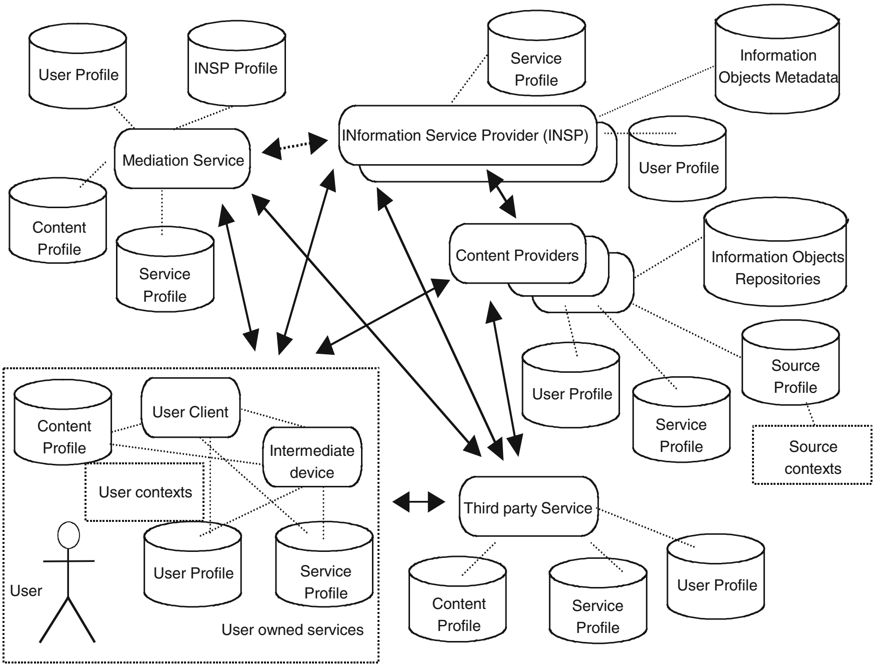

Fig. 1 Categories of support [4]

control over how to respond to an end users request for support. This can potentially allow for prioritizing certain responses that would benefit the information service provider. The information service provider also has access to all data created from the request by the end user and can potentially use this to build on its own service providing capabilities.

2.1.2 User Owned Services

The user owned services category of support uses locally controlled data to keep the control within the context of the user. This includes technologies that remain entirely disconnected with localized data and under the control of the end user e.g. localized chatbots [8], as well as systems that utilize online services on behalf of the end user e.g. virtual personal assistants [9]. A key aspect of this category is the control of the data used to support the end user remains in their control locally.

2.2 Methods of Control

There are a number of different approaches to maintaining access to or control over the data used by the end user. This can include access rights to the data as technologies such as mobile applications require the user to accept the developer's access requirements before it is usable [10]. Data control can be categorised by the method in which the device interacts with a centralized network to provide a service. With the methods of data control on a device categorised we can visualise the differences between similar technologies that differ with who controls the data.

2.2.1 Disconnected Technologies

One approach to data control through managing connections is to create a totally disconnected technology. These technologies have no ability to connect to an outside network and in some instances will have no ability to connect to any other devices at all. For the end user this means that no centralized server will be able to access this data and is most notable on technologies that can use personal data or create data based upon interactions with the end user. The contrast to this is seen in technologies that cannot be managed by the end user despite their disconnected nature. This allows for the creator of the technology to ensure that only the data they intend to use on the device can be operated allowing them to control the device without the need to directly connect to it.

2.2.2 Centralized Technologies

Another example of data control through connectivity management is the approach of making a technology only functional when it is connected to a centralized server. This can be for a number of beneficial reasons, such as distributed processing and using the connection to connect to other users and services, but can also be imposed to ensure that a device can only be used when the (local device specific) data is accessible by the centralized server.

2.2.3 Technologies with Intermittent Connection

It is possible for technologies to have the ability to utilize connections to enhance their functionality but still be able to function (potentially with limited functionality) offline. In these instances the characteristics of usage of the connection can be used to identify who is in control of the data available on the device. For example, end user supporting technologies may have the ability to access the internet and carry out functions on behalf of the end user, but still be capable of providing support to the user when disconnected. In contrast to this a device that is controlled by a centralized server may use connections to update itself and apply changes to the data on the device at the request of the centralized server. It may also have any or all functionality disabled when disconnected.

2.3 *Methods of Control Within the Context of Categories of Support*

Within the context of the categories of support that we have discussed, we can identify different approaches to data control and categorise them according to which stakeholder has control of the content. This categorization helps to visualise the boundaries between technologies that are supporting different stakeholders but take a similar approach to controlling the devices data. Table 1 shows a table of examples of different methods of control within each category.

Table 1 Methods of control within categories of support

Controller of content	Example of disconnected data control	Example of partially connected data control	Example of fully connected data control
Information service provider	United States Navy's NeRDs	Games consoles, on-board computers in cars	Apple's Siri, possibly Microsoft's Cortana
End user	Localised chatbots	Virtual personal assistants	Remote access media servers

This table uses examples of end super supporting systems to illustrate the differences between each method of data control in relation to the controller of the content. With the different methods of data control show in this table we can examine each approach in detail. Although the categories can seem (superficially) similar between each category of support, the controller of the content can affect the advantages and disadvantages of this type of support for the end user.

Technologies that take the disconnected approach to controlling data tend to be more oriented towards providing privacy and security at the expense of access to a larger selection of services and functionality that would potentially come from allowing an connection to some form of centralized server. Devices that utilize intermittent connectivity have a tendency to focus on being more useful to the end user regardless of who is controlling the technologies content. The device remains usable even in an disconnected environment but has the ability to benefit from services provided by a centralized server. This does however open the device up to the security risks that come connecting to external sources. Devices that require a connection to function have a more strict approach to data control in the sense that they require a primary stakeholder to have access to the device to function. This does allow for tight control over who access and manages data on the device but can even go as far as reducing a devices usability to ensure that data is not being altered in the absence of the controller of the data.

3 Centralized Data Control

Within this section we will discuss how centralized organisations exhibit control over data. This control can be to update and manage software to provide support for the end user by maintaining the distributed technology from a centralized source. In contrast to this, data can be controlled by recording or managing an end users data on a system. This can be to ensure the data on the device is what the centralized organization intended or as a way of gathering data from an end user.

3.1 Control via Required Connection

There are examples of technologies that require a connection to a centralized system despite the fact that a large number of the functions present of the software are capable of working offline with the data stored locally on the device. In some instances this is down to specific attributes of the functionality either requiring an internet connection or even having shared processing.

One example of this can be found in Apples Siri. Siri requires an internet connection to allow the software to pass data to the Apple cloud for all of its functionality [11]. This includes accessing contacts and applications stored locally on the phone. It has been claimed that this mandatory connectivity is due to Apple recording interactions between the end user and Siri [12]. A mandatory connection to the Apple servers has advantages however. Siri can categorise its user with similar users in an attempt to provide a more personalised solution than a generic response to service requests. This can include refining search responses to attempt to provide more useful outputs for the user [13]. With modern advances in mobile connectivity the issue of being disconnected is becoming less significant. The concern with a mandatory connection for this software comes in the form of the privacy of the data. Even with access to an internet connection, users may wish to opt out of transmitting information over the internet and still wish to access the functionality provided by Siri. Microsoft's Cortana could potentially fit into this category as well but the current functionality of the device is unclear [14]. The program itself does have similarities to Apple's Siri and marks Microsoft's take on the same type of supporting technology. Microsoft may potentially use this opportunity to create a competitor to Siri that is still useable by the user when offline.

3.2 Control via Intermittent Connection

Another approach used by some distributed technologies is to utilise connections to manage the device by applying updates to the device from a centralized server. Updates of this type do not require permanent connections, meaning that the systems functionality is retained when it is disconnected. This method of connection allows software to be modified without requiring a new instance of the technology to be created and distributed.

One example of this approach to data control can be found within games consoles. Games consoles are perfectly capable of functioning offline and the end user to play games as they wish but have the capability to connect to a centralized server to play games online. This same connection can be used to update the software on the console, allowing the centralized server to ensure that they still have influence of the consoles themselves. These updates do allow for updates such as improved security but could potentially require people that play games online to allow the centralized server to have access to data stored on the device [15]. This is achieved by including a mandatory update to the consoles software that is required to allow it to play games online but also effects the terms and conditions of which the company has access to the end users data [16]. The end user is left with the choice of adhering to these new terms or losing the online functionality of the console [17]. With recent pushes into the realms of streaming and using consoles for other online activities a lack of connection can be a significant loss of functionality and impact the usefulness of the device.

A second example of this approach to data control is the use of managing on-board systems on cars. As technology is becoming more and more present in our day to day lives, the use of on-board computer system in a car is becoming more important. These on-board computer systems can be updated by the manufacturer to add new functioning or enhancing systems already present [18]. This is currently achieved by either a distributed USB stick [19] or a trip to the cars dealership. While this can provide an advantage to the end user in the form of enhances usefulness and functionality in the on-board computer systems, it does raise some significant security concerns. If a manufacturer can effect a cars on-board computer systems via software on a USB key they it is only a matter of time before malicious hackers can also effect this software. Depending on what systems are linked to the on-board computer systems, this could potentially be a life-threatening risk [20]. Alongside this there is ‘considerable interest’ in the auto industry developing remote updates for cars [21]. The manufacturers are hesitant to take this method of applying updates to cars after researchers were able to remotely take control of a car and force the breaks on [22].

3.3 Control Through Limiting Access to a Device

One method of controlling the data on a technology is to remove any way for the end user to effect what is stored on the device. This ensures that the system will be used as the creator intended and removes any concern of more data being added to the device or the device being used in different ways. This does however also remove the ability for the end user to personalise the device, meaning that there are imposed limitations on how useful the device will be to the end user.

An example of this can be found in the United States Navy. The US Navy has recently adopted a device named ‘NeRD’ (Navy eReader Device) to provide its staff access to eBooks in an environment that requires strict control over any data emissions [23]. The devices will be loaded with 300 books ranging from classics to best sellers, and at launch 5 devices will be distributed to each US Submarine. The intention is to function as a replacement for personal mobile devices such as tablets and phones as the crew are unable to use them on-board vessels due to security concerns about the possibility that their data emissions could be tracked. It is also apparent that there is very little space on-board vessels, leaving little room for any entertainment. It has been said that because of this what few books are available are shared amongst the crew until they fall apart [1]. A need for innovation was identified and a solution was created in the form of the NeRDs. While this does give the crew access to the digital media the Navy has prepared, it raises some questions about the effectiveness of this solution.

The device has all of its ports, network access and removable media connections disabled. This means that once the device has been loaded with its books, no more can be added or removed. Even when the device is in a safe environment or with physical access to a secure system the device cannot have its stored books changed. This raises concerns about how future proof this solution is in regards to the changing trends of eBooks. How useful would a library with a total of 300 books be, when all of which are selected by others? The security concerns for this technology are legitimate but the precautions may be overbearing with their restrictions to the point of hindering the usefulness of such a device. It could be argued that the device would be just as secure aboard a vessel even if it had the ability to physically connect to secured navy systems in dockyards, allowing for the device to be managed between deployments. The 300 books that are present on the device are from a library of 108,000 books that the US Navy has digital access to [24]. By removing the devices ability to ever be able to connect to this digital library a huge amount of already available digital media will be unable to be deployed for the crews access on-board vessels.

4 Local Data Control

Within this section we will discuss local data control, where the content is under direct control of the end user. This can be due to a system remaining disconnected while an end user can still manipulate the data stored on the device. This can also be achieved by the system connecting to other sources on behalf of the end user, instead of on behalf of the external source. This allows the technology to utilize these outside sources without changing the focus of support away from the end user.

4.1 Disconnected Data

In some instances an end user has control over their data because the device functions completely disconnected from any centralized server. Users can freely manage and manipulate data on such a device locally and are at no risk of this data being micromanaged by a central source. This allows for the end user to develop a secure private data set on the device to provide a more personalised end user supporting service. An example of a device that provides disconnected data management is the chat bot Kari [8]. As we have previously investigated, Kari can be used well beyond its original intended purpose with the utilization of the data and metadata it creates. Due to the amount of control the end user has over this program it can be manipulated and trained to be a powerful end user supporting tool purely because there are no restrictions to the end users control over its data [22].

4.2 Utilization of Connectivity

Another example of end user data control can be seen in technologies that carry out actions on behalf of the end user. These technologies do have interactions with connected systems and even interactions with centralized servers but do so on the request of the end user, not at the request of the centralized server. This means that a system may be requested to retrieve information by searching online as an extension of the user. One example of this type of system is HAL [9]. HAL is a virtual personal assistant that attempts to use natural language capabilities to hold meaningful and valued discussions with its end user. It has the capability to build up metadata from the data it gathers from the end user to form a locally controlled data library. HAL also has the ability to utilize connections to the internet on behalf of the end user to carry out simple requests such as searching for information the user has requested. The results of which and the data created with the user through discussion are not available to the network it has connected to but is still utilized to support the end user.

4.3 Fully Connected End User Support

It is possible for a service to provide data control to the end user over a connection. This approach doesn't necessarily localise the data with the end user, but gives the end user the ability to manage the data remotely. These services provide support to the end user by distributed data from a remote source or allowing the user to manage the data at the remote source. An example of this can be seen with the PLEX media server [25]. PLEX allows the user to stream media to other devices such as a TV or a smart phone from a user controlled server. The user has direct control over all of the content of this server but requires a direct connection to be able to access the content. This approach allows the end user to access large amounts of media from devices with only a small data capacity and access to the network with the server. Users with this technology will be able to access their entire library of media from a TV with no data storage, but will lose all of its data if the connection is disrupted. A issue with this approach is the concern that the connections may not be fast enough to stream the media at will, resulting in the user waiting on buffering times.

5 Benefits and Limitations

Through discussions around examples of each method of data control within the context of centralized service providers it is possible to identify trends in the advantages and disadvantages of this approach when compared to end user supporting services. Each approach to data management by the centralized organization can negatively impact the usefulness of the device to the end user in some way. This is due to limitations placed on the device to prevent the user from managing the data on a technology without the connection (or lack of connection) that the manufacturer desires.

Examples of this can be seen with limitations such as the loss of functionality when not connected to a network or not updated via connecting to a centralized server. Alongside this disconnected devices can be seen to be restricted by losing their ability to form any connections at all. These limitations are in contrast to potential benefits for the end user when these approaches to content control are within the context of the end user. With disconnected devices, the user has the opportunity to control personal and private data with the intention of better serving the needs of the individual. With devices that can utilize connections the end user has the ability to draw upon content and services that would otherwise be too large to store on the device. This is done as an enhancement to already present functionality and serves to improve the usefulness of the device to the end user. User controlled servers allow devices with no content to utilize connections and become methods of accessing the users controlled media. It is these differences between devices that can lead to the centralized approach to data control being perceived as less useful to the end user. There are advantages for the end user in each centralise approach too, as most approaches are adopted for a purpose that holds some benefit for the end user.

Disconnected devices, even with total restrictions to connectivity and content personalisation, still allow for the end user to use these devices in environments where no other device would be allowed. This approach may be limiting but can allow a large number of users to benefit from technology where there may be no acceptable alternative. Devices that use internet connections for updates via connections to a centralized server may on occasion be limiting as it may require updates before use. This does however go hand in hand with the ability to adapt and potentially remain useful for longer than the expected original product life because of enhancements to the device that are applied remotely. Other devices that require a connection to function may lose all of their functionality when offline, but benefit from the wealth of content built up by the service provider. This could be anything from large volumes of media available for streaming to refined service providing based upon data gathered from actions of the servers entire user base. End users could potentially see benefits from centralized control approaches. However while many approaches can provide usability for the end user—they can also be viewed as directly detrimental to the usefulness of the devices. In effect it is quite possible that some restrictions and limitations purposefully implemented on a device (such as those for organisational security purposes) may result in such a lack of usefulness to completely defy the purpose for why the device was created in the first place.

6 Conclusions

Within the context of distributed technologies the control of the data stored on each device has direct impact on its usefulness to the end user. Devices that function in a completely disconnected environment are shielded from the effects of centralized data control but lose access to the services that come with it. While this does in some situations better fit the need of the end user it can also largely limit the usability of the device. The contrast to this is found in devices with a mandatory connection to a centralized service. This can provide a greater array of services but limits the user's ability to use the device. Although high levels of centralized control can negatively impact the usefulness of a device, there is also the prospect of a win-win situation for all of the stakeholders involved. Some methods of data control via intermittent connections have the potential to enhance the usefulness of a device by allowing information service providers to provide and support services without altering or effecting the end users ability to control and access data.

It has been the intention of this paper to categorise and compare the different approaches to controlling data on distributed devices and their effects on the usefulness to the end user. Each approach has its own advantages over the other approaches and each has its own situations to be used in. To best support the end user careful consideration over how data on a device will be utilized by both the end user and the service provider is required within the context of the technologies intended purpose. This will ensure that the end user has the appropriate amount of control of the data on the device to make it usable, while still receiving the services needed to make the device useful.

References

1. Bayluxe: NeRD. US Navy's own e-reader. http://beyluxe.com/articles/technology/nerd-us-navys-own-e-reader (2014). Accessed 07 July 2014
2. Enis, M.: U.S. Navy launches NeRD, a security enhanced e-reader. http://www.thedigitalshift.com/2014/06/ebooks/u-s-navy-launches-nerd-security-enhanced-e-reader/ (2014). Accessed 09 July 2014
3. Bednar, P., Katos, V.: MCIS2009: 4th Mediterranean conference on information systems. In: 4th Mediterranean Conference on Information Systems, pp. 900–912 (2009)
4. Bednar, P.M., Welch, C., Graziano, A.: Learning objects and their implications on learning: a case of developing the foundation for a new knowledge infrastructure. In: Harman, K., Koohang, A. (eds.) Chapter 6 in Learning Objects: Applications, Implications and Future Directions, pp. 157–185. Informing Science Press, New York (2007)
5. Orlowski, A.: 77 % of Google users don't know it records personal data. http://www.theregister.co.uk/2006/01/24/google_privacy_poll/ (2006). Accessed 08 July 2014
6. Channel 4: Thursday 16 January 2014 UK What GCHQ knows about us—a timeline of revelations. http://www.channel4.com/news/gchq-timeline-revelations-snowden-spying (2014). Accessed 08 July 2014
7. Greenwald, G.: NSA collecting phone records of millions of Verizon customers daily. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (2013). Accessed 05 July 2014
8. Lhandslide Studios: Advanced virtual girl with artificial intelligence. http://www.karigirl.com/ (2012). Accessed 02 July 2014
9. Zabaware Inc.: Ultra hal can hold conversations with you. http://www.zabaware.com/assistant/index.html (n.d). Accessed 09 July 2014
10. Tsavli, M., Efraimidis, P.S., Katos, V.: Reengineering the user: privacy concerns about personal data on smartphones. In: Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance, pp. 80–89 (2014)
11. Apple: Siri. Your wish is it's command. http://www.apple.com/uk/ios/siri/ (n.d). Accessed 15 April 2013

12. Ozer, N.: Note to self: siri not just working for me, working full-time for apple, too. https://www.aclunc.org/issues/technology/blog/note_to_self_siri_not_just_working_for_me,_working_full-time_for_apple,_too.shtml (2012). Accessed 22 April 2013
13. Apple: Siri FAQ. http://www.siriuserguide.com/siri-faq/ (2014). Accessed 05 July 2014
14. Microsoft Windows: The most personal smartphone assistant. http://www.windowsphone.com/en-us/features-8-1#Cortana (2014). Accessed 09 July 2014
15. Martin, M.: Xbox One won't play games on day one without mandatory update. http://www.gamesindustry.biz/articles/2013-11-08-xbox-one-wont-play-games-on-day-one-without-mandatory-update (2013). Accessed 05 July 2014
16. Makuch, E.: Microsoft changing Xbox live terms of use. http://www.gamespot.com/articles/microsoft-changing-xbox-live-terms-of-use/1100-6415826/ (2013). Accessed 05 July 2014
17. Klepek, P.: You must agree to all of Xbox live's new terms of service. http://www.giantbomb.com/articles/you-must-agree-to-all-of-xbox-lives-new-terms-of-s/1100-3846/ (2011). Accessed 07 July 2014
18. Zax, D.: A software update for your car? http://www.technologyreview.com/view/427153/a-software-update-for-your-car/ (2012). Accessed 09 July 2014
19. Ford: How to install Ford SYNC updates in your vehicle. http://support.ford.com/sync-technology/install-updates-sync (2014). Accessed 05 July 2014
20. Vincent, J.: http://www.independent.co.uk/life-style/gadgets-and-tech/researchers-hack-cars-to-remotely-control-steering-and-brakes-8733723.html (2013). Accessed 05 July 2014
21. Bullis, K.: Why your car won't get remote software updates anytime soon. http://www.technologyreview.com/news/524791/why-your-car-wont-get-remote-software-updates-anytime-soon/. Accessed 09 July 2014
22. Bednar, P., Imrie, P.: Virtual personal assistant. http://www.cersi.it/itais2013/ (2013). Accessed 11 July 2014
23. Griggs, B.: Meet the 'NeRD,' the Navy's new e-reader. http://edition.cnn.com/2014/05/08/tech/gaming-gadgets/navy-nerd-e-reader/ (2014). Accessed 05 July 2014
24. Baker, B.: US Navy develops world's worst e-reader. http://www.naval-technology.com/features/featureus-navy-develops-worlds-worst-e-reader-4265782/ (2014). Accessed 05 July 2014
25. Plex: What is Plex? https://support.plex.tv/hc/en-us/articles/200288286-What-is-Plex (2014). Accessed 09 July 2014