Di.me Userware Evaluation – Users in all life spheres

Richard Wacker, YellowMap AG – *richard.wacker@yellowmap.de*
Sophie Wrobel, CAS Software AG - *sophie.wrobel@cas.de*

Date: 10/12/2013

The di.me project aims to develop a new kind of social network with two central characteristics: (1) unlike conventional social networks, the **user maintains control over his personal data**, and (2) **support for trustful interaction** within the available functionality in order to reach a maximal user acceptance. The **di.me userware** was designed to achieve this, and is composed of two parts:

The **di.me personal server** acts, as its name suggests, as a user-controlled server. It offers secure and intelligent data management, and numerous data protection technologies such as automated privacy warnings. Further, it enables the integration of existing social networks, web services, and communities.

The **di.me client** is a single user-controlled access point to all of the **di.me server** functionality. Within the project, clients were developed for browser-based access as well as a mobile-optimized Android solution.

The **di.me userware** demonstrates that a broad scope of social networking functionality is technically feasible, while preserving user control over his personal data in social networking. As we show in this document, the **di.me userware** also meets user's expectations towards trustful design, support by intelligent advice, and multiple identities.

Motivation of the di.me project

An individual's personality is composed of multiple facets, each emphasizing different personal attributes and relationships. Depending on the context, some of them are shown and others are hidden; some are emphasized and others are intentionally understated. It is a fundamental human right for every individual to choose which personal attributes are visible to whom and in which context. This human right is the very basis of any data protection legislation – in Germany this basis is called the *"right to one's own picture"*. Keeping in mind that this picture varies depending on its context, it should be renamed as *"right to one's own pictures"* – the right of an individual to decide which personal characteristics is visible to whom. In the offline world, this can simply be achieved by one's appearance and behavior in different and separated life spheres like family, circle of friends, and business.

In our modern data-driven society, the formalization of personal attributes and relationships is on the rise. Such information could be used to digitally reflect the offline situation, which means supporting separated and unlinkable context sensitive identities. But as digitalized information is easily accessible, it is very likely to be misused to establish a complete profile of an individual, as described in Figure 1. In this latter case the result violates the "right to one's own pictures" as it allows an observer to generate a comprehensive profile of a targeted individual.

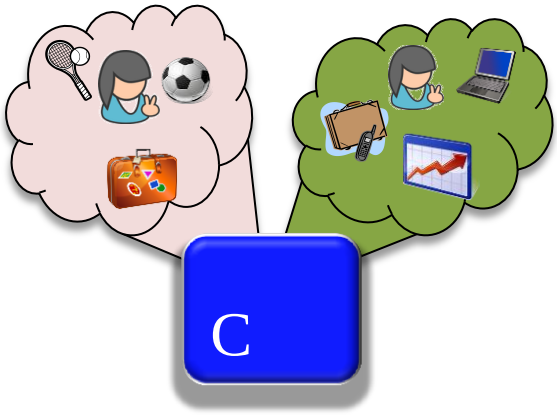

Figure 1 each user has multiple context-specific digital identities.

In online social networks (OSNs), the difference between mirroring our offline habits and establishing a surveillance platform is extremely critical. Participation in social networks is widely popular and encompasses all life spheres for a

modern individual. However, OSN providers typically forbid the use of pseudonyms – despite knowing that revealing a real name eases linking different facets to one whole picture, and thereby strongly compromises an individual's privacy (Facebook's practice of blocking user accounts, 2013).

Consider another characteristic that digitalized information aggravates: As the individual and the receiver of information often do not know each other, the latter's interpretation is completely out of the individual's control. As both are digitalized, the original and interpretation are hard to distinguish from a third party's perspective. The consequences can be dramatic: An individual's private affairs can affect his business affairs, and vice versa.

Ultimately, individuals are forced to avoid any behavior that could be misunderstood in any context from public, self-published information. Fundamental rights like freedom of speech or freedom of action are factually repealed. A promising approach to address this issue would be an OSN that explicitly supports multiple identities and monitors unlinkability. Even though European officials recommend separating personas in digital environments (Santucci, 2013) social network providers hesitate to respond to such appeals. The loss of privacy is instead justified by user friendliness and even security (Facebook Privacy Guidelines, 2013), but there are suspicions that the true reason lies in the respective platforms' financial interests, as OSNs are primarily financed by advertising revenues (Pettey, 2012).

di.me Userware vs. conventional OSNs

In conventional OSNs, privacy shortcomings result from a variety of reasons under which the centralised structure plays a major role. This not only offers an ideal attack point, but also establishes the provider as middleman in any transaction. Technically, the user has no private space in an OSN, as the provider controls all uploaded information and every inbound and outbound communication channel. A closer look at the underlying terms and conditions shows that the providers grant themselves extensive rights to use this personal information for their own purposes.[1] Additionally, OSN

[1] A prominent example is one of the latest changes to the terms of use in which Facebook added a clause to allow the use of profile photos for their advertising. See http://www.heise.de/newsticker/meldung/Sponsored-Stories-Facebook-aendert-Spielregeln-fuer-personenbezogene-Werbung-1946275.html

providers tend to enforce the use of one comprehensive personal profile. They only provide some rather simple self-configurable access restrictions. Sharing operations, which are extremely critical from a privacy perspective, are implemented in a very simple manner, but this is accompanied by a significant lack of transparency regarding potential consequences.[2] Last but not least, extensions such as external services are intensively advertised, but the inherent privacy risk is often only mentioned in a footnote, or hidden somewhere in the tenuous terms and conditions text.

The ***di.me userware*** was developed to address these issues by creating a technical platform that realizes user-controlled, decentralized social services. A demonstration prototype was implemented showing privacy support for typical social networking functionalities like file sharing or messaging for users in all life spheres. Referring to the presented argument of OSN providers regarding the need to reveal a true identity, ***di.me*** shall give an answer to the following question:

Is preservation of a users' control over his personal data, and intelligent support for trustful interaction a core value to the users in social networking?

Following from that central aim, the **di.me userware** has to meet two major user requirements:

1) It has to provide significantly more control and transparency to the user concerning his personal information.
2) It has to provide intelligent advice to strengthen his privacy awareness.

Therefore the di.me approach significantly differs from standard OSNs. In particular the ***di.me userware's*** privacy technologies are not just enhancements but an example of "privacy by design" (Ann Cavoukian, 2009).

---

[2] The implications of Facebook's intransparency became quite prominent in Germany when a 16 year old accidentally posted a public invitation to her birthday party on Facebook. Thousands of members followed. See http://www.sueddeutsche.de/panorama/facebook-party-in-hamburg-gaeste-elf-festnahmen-drei-anzeigen-1.1105389

The di.me Architecture

The central requirements of providing the user with more control over his data and offering intelligent advice are addressed by the **di.me userware's** architecture. The architecture of the ***di.me userware*** is depicted in Figure 1. It is comprised of three layers which communicate via defined interfaces.

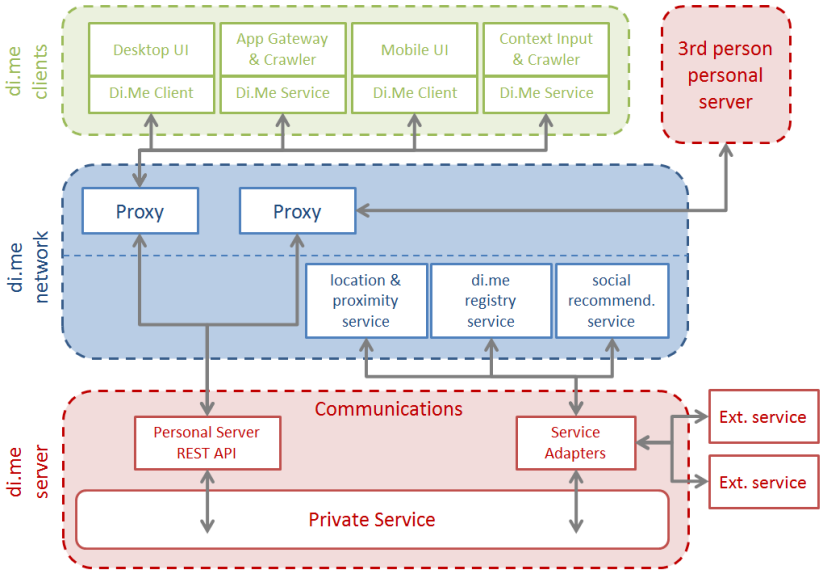

Figure 1 di.me userware architecture

The ***di.me clients*** layer which is highlighted in green consists of the two alternative user interfaces – ***di.me mobile*** app and the ***di.me desktop*** – and the associated crawler components. These crawler components collect context-specific data from the user's device and send it to the di.me server in order to enable context-specific functions such as situation recognition, neighborhood analysis and discovery of nearby points of interest (POIs). Both provide a single user-controlled point of access, illustrated in Figure 2. Generally the context-sensitivity is an opt-in feature that the user needs to explicitly activate.

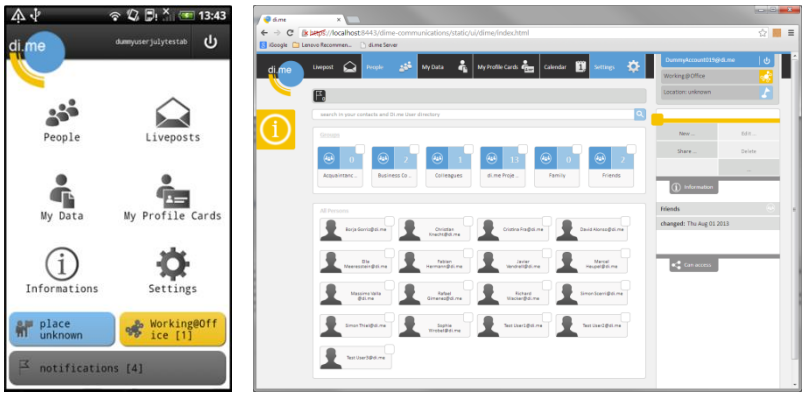

Figure 2 di.me Userware Clients: the mobile app (left) and the desktop (right)

The ***di.me mobile*** (left) is a native android application, while the ***di.me desktop*** (right) is a browser-based application. In order to support alternative mobile platforms, the ***di.me desktop*** is also usable on a mobile device, but due to access limitations regarding the device's sensors, some the crawler functions are restricted to ***di.me mobile***.

The medium layer (blue), called ***di.me network,*** provides secured communication between the client and the corresponding personal server. Additionally, it integrates necessary (di.me registry) and optional (location and proximity) platform services.

The most basic layer of the ***di.me userware*** is the ***di.me server*** layer. It implements all functionalities and also provides the technological basis for all privacy-enhancing technologies (PETs) like:

- A ***decentralized storage model***. External data storage and undesired data disclose is effectively avoided.
- A ***decentralized peer-to-peer communication*** without any potentially untrusted middleman.
- Explicit support for ***multiple personas*** which are, by default, not linked to each other.
- An ***ontology*** that models all related entities and their relationships as semantic basis for
    - advanced context aware features, and
    - an effective risk detection mechanism.

Di.me User experience

The following section provides a brief introduction to the ***di.me userware*** from a user's perspective. A central element is the single unified user interface to a personal data sphere, which is offered by two ***di.me clients***. Both clients are available in the form of a fully integrated prototype. They share many fundamental usage concepts, whereby the mobile app combines it with android-specific UI design patterns.

Multiple Profiles in di.me

Support for multiple identities is one central characteristic in the ***di.me userware***. This feature is implemented by the concept of different user-defined profile cards, which represent multiple identities in di.me. For each context in which ***di.me*** supports social media activities, the user can create a corresponding profile card that exactly covers a set of necessary attributes. Hence this concept strengthens two fundamental principles of data protection. First, it improves *data purpose binding* – attributes attached to a single profile card

which is used in a certain context are only visible in this context. Second, it strengthens the principle of *data economy* as the set is reduced to what is really needed in this context.[3] All other attributes remain invisible to the receiver. If profile cards are appropriately defined by the user (no unique information appears in different profiles), any of them appears as a unique individual in di.me. As a result, a ***di.me user*** may potentially have multiple entries in his contact list that factually refer one individual.

Manage Contacts in di.me

As in any other social network, the user has the ability to manage personal contacts. In di.me, the contact list is a list of di.me profiles from other users, which as stated above, is not necessarily the same as a list of users. To ease management, these contacts can be organized in self-defined contact groups like family, friends or company.

Contact entries originate from three sources: They can be added manually by searching the di.me user directory, they can be recommended by the contact and group recognition component, or they can be imported from a connected OSN-account. In the latter case, the system automatically adds the corresponding external source to the contact details.

In order to support privacy preserving mechanisms, each contact has a trust level assigned (high, medium, low). This setting is considered in any sharing operation. The default trust level, which applies to any newly added contact, is "low", which implements an analogy to an opt-in. By assigning a higher trust level, the user can opt-in to disable certain privacy warnings regarding that contact.

Share information in di.me

One main function supported by di.me is information sharing via either a livepost or a data element. The latter covers files of arbitrary kind which can be uploaded to the di.me server. To ease management and sharing of data elements, elements can be organized into data boxes. Hence a sharing operation can either apply to a single data element, a data box, or a livepost.

With respect to potential privacy risks, each data element and livepost has an assigned privacy level (high, medium, low). Newly added data elements always get the highest privacy level, which ensures that the maximum of protection applies to

[3] See Directive 46/95/EC Article 6, section c.

them by default. The standard sharing dialogue always requires, besides the addressees (contact or contact group) and the subject (document or data box), the user to specify a profile card. These combinations of subject, object and profile card are evaluated by the built-in warning mechanism. It detects the following three cases, which all represent risks to an individual's privacy:

1. *A document with a high privacy level is shared with a less trusted contact.* This could imply that sharing the specified document with one of the contacts was not intended, or that the trust level of him or the privacy level of one of the data elements was not appropriately set.
2. *The specified profile card was never revealed to one of the addressees.* This could either mean that the user specified the wrong profile, or that the contact concerned has multiple relationships to the user (for example private and business).
3. *The document was already shared with one of the addressees using another profile card.* This violates the rule of unlinkability because the receiver gets the same information from different senders and could infer that these senders are associated to the same individual.

In all three cases, the di.me system provides a privacy warning message that explains the issue and lists the offending contact(s) which triggered the warning. The user has the option to correct his choice or to ignore the message. Ignored warnings are used by di.me to derive additional knowledge: the first warning could also appear from inappropriate privacy or trust level settings. If such a warning is repetitively ignored regarding the same contact or document, the user receives a recommendation to correct the privacy or trust setting to a more appropriate value.

Extending di.me

Besides the base functionality described, the di.me system can further be extended by activating additional connectors and services. If a user for instance already is member of a conventional OSN like Facebook, Twitter, Google Plus and Linked In, he can use the corresponding connector and import external contacts. Additionally he can activate a variety of external services that provide advanced context aware features – namely the *location*, the *proximity*, and the *YellowMap Places Service*. *The location service* detects the users current location stores it to the di.me server and matches it to the places provided by the *YellowMap Places Service*. The *proximity service*

shares the current location with other registered di.me users and thereby enables advanced group and contact recognition. As a result, the user receives contact and group recommendations when registered users or a group of his existing contacts happen to be located at the same place over a certain time interval. The *YellowMap Places Service* additionally locates interesting locations near the user's current position, which can be rated by him or set as favourites.

Again, with respect to privacy, none of these services is active by default. Hence these privacy-relevant services, like all other functions in di.me, strictly require an opt-in. Additionally, the proximity service, which makes potentially intimate information available to other di.me users, has to be configured with a profile card. So, the user has the option of choosing a profile card without any identifying information and a pseudonym.

Automate your di.me

All advanced functions of di.me, as well as of the integrated trust engine, are based on a comprehensive ontology-framework that models all actions, assets and their relationships. Much of the systems behaviour is driven by rule-based reasoning on top of this semantic model. While most of these procedures run below the surface the automating feature of di.me enables the user to compose own rules to personalize and enhance his di.me server. Therefore an intuitive rule editor is provided.

This feature on the one hand allows extending the convenience in ***di.me userware*** but also bears privacy risks. To address this issue, the user must be able to understand the consequences of a rule. Providing him with the full expressiveness of the underlying logic could possibly overburden him. Hence, the editor is restricted to simple implication rules with conjunctions.

Feedback on di.me

From July until October 2013, the di.me prototypes were evaluated in a test trial conducted by the project consortium. In it, testers were invited to a prepared environment consisting of a number of preconfigured servers and a comprehensive set of information and test materials. After finishing the validation, test subjects were requested to fill out a questionnaire comprising of questions about the core privacy related features of the di.me userware. The underlying question to be answered was:

Do the basic concepts of di.me proof to address an important demand of users in online social networking?

Therefore, the validators had to ask two questions regarding any central feature. The first one referred to the general rating of the feature in question, and the second question asked directly whether the tester would be interested in such a feature as part of a product. In addition, testers could provide a free-text comment to each feature. The summarized result from about **130** responses was:

- **90 %** rated a ***decentralized social network*** positively and even **59 %** indicated that they would use it.
- **81 %** liked the idea of ***multiple digital identities***, **64 %** users indicated they would use it.
- **84 %** appreciated the idea of ***privacy recommendations***, **66 %** indicated that they would be interested in such a product.

In particular, the remarkably high values for the latter responses indicate that there is a market need for the shown functionalities, and not just curiosity. This also shows up in the text comments.

"The concept is very interesting."

Anonymous user feedback

"It is very convenient; most people would use at least personal and professional cards."

Anonymous user feedback

"If the additional effort is minimal, I could fancy using this program in daily life."

Anonymous user feedback

The generally positive feedback on ***di.me userware*** also reflected in general comments during the dissemination activities.

"Great initiative!! ... Looking forward to see what it'll become."

Charles Bonneau-Parquer (Belgium)

"Very promising. Follow it."

Carsten Rose (Germany)

"For me all this projects are interesting and it will be nice to see how it all plays out in the future?"

I. Miguel P. Tavares (Portugal)

Conclusion

In summary, the ***di.me userware*** shows significant market potential, as a large majority of testers indicated a strong interest in privacy-enhancing technologies. ***Di.me*** reinforces user's control in social networks which could be the keys to success in the next generation of social networks. In the di.me userware, these features are deeply integrated in system's design, which is a unique feature among all currently available OSNs on the market.

Nevertheless, as an OSN's success strongly depends on the network effect (Jackson, 2008), and ***di.me*** has yet to reach a critical mass (Westland, 2010) of users. Therefore, it first addresses users that completely, or at least partly, abstained from social networking due to privacy concerns. For them, ***di.me*** offers an extensible range of OSN functionality in a convenient manner, without forcing them to disclose personal information to a provider based overseas with nebulous intentions. Secondly, as ***di.me userware*** allows managing existing user information from other OSNs, the consumer's switching costs (Thomas A. Burnham, 2003) are outstandingly low. Thirdly, the ***di.me userware*** is much more cost efficient than any competitor. Due to its decentralized structure, the ***di.me client*** and ***di.me server*** can be run on a user's device. The only centralized structure needed is located on the ***di.me network*** layer which is highly scalable and resource efficient. Hence providing di.me to a large user community does not require a server farm whose costs have to be compensated by extensive advertising. Additionally, the reduction to a relatively small set of central has another desirable effect. As the provider of the network layer has much less insight than a typical OSN provider, the legal obligations to fulfil are also less complex. Last but not least, the di.me framework is offered

as an open-source platform solution licensed under the EUPL. It is supported by an open-source community operated by the involved research partners (see Acknowledgements) and openly usable for all parties interested in elaborating on the di.me concepts and creating privacy-preserving social media and social networking applications on top of it.

Benefits in Summary

In summary, the ***di.me framework*** provides magnificent benefits for OSN users in all life spheres and especially in direct comparison against conventional OSN platforms.

Support of personas: By supporting different and unlinkable profiles (personas) the ***di.me***-user can retain the separation of different life spheres.

Confidentiality: Due to the personal secure and decentralized storage model of ***di.me*** user data is effectively protected against intrusion.

Transparency and Control: In ***di.me*** the user itself determines, which data is shown to whom as any disclosure of data has to be explicitly triggered by him.

Awareness: The detection and warning mechanism boosts the awareness of the ***di.me***-user regarding actions that potentially compromise his privacy.

Context-aware features: The ***di.me***-system includes advanced context-aware features like the places service including community rating, proximity analysis and group and contact recognition.

Extendibility: ***Di.me's*** core application can easily be extended by additional services and service adapters providing the same level of security and privacy protection.

Legal Compliance: In contrast to conventional OSNs ***di.me's*** privacy preserving features are design immanent which is a central precondition to comply with the actual and future European data protection legislation (European Commission, 2012).

References

Ann Cavoukian, P. (2009, 08). *Privacy by Design - The 7 Foundational Principles.* Retrieved 09 20, 2013, from Privacy by Design: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Beier, G. e. (2006). Die Akzeptanz zukünftiger Ubiquitous Computing Anwendungen. *Mensch und Computer 2006: Mensch und Computer im Strukturwandel* , pp. 145-154.

Davis, F. D. (1989, 9). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* , pp. 319-340.

European Commission. (2012, 1 25). *Proposal for a European Data Protection Regulation.* Retrieved 9 20, 2013, from Official Website of the European Union: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Facebook Privacy Guidelines. (2013). *How we use the information we receive.* Retrieved 09 20, 2013, from www.facebook.com: https://www.facebook.com/about/privacy/your-info

Facebook's practice of blocking user accounts, OVG Az. 4 MB 10/13 and Az 4 MB 11/13 (Schleswig-Holstein Higher Administrative Court 02 14, 2013).

Jackson, M. O. (2008). *Social and Economic Networks.* Princeton, NJ, USA: Princeton University Press .

Pettey, v. d. (2012, 07 25). *Newsroom.* Retrieved 09 20, 2013, from Gartner: http://www.gartner.com/newsroom/id/2092217

Santucci, G. (2013, 09). *Privacy in the Digital Economy: Requiem or Renaissance?* Retrieved 09 20, 2013, from The Privacy Surgeon: http://www.privacysurgeon.org/blog/wp-content/uploads/2013/09/Privacy-in-the-Digital-Economy-final.pdf

Sproll, S. P. (2010, 10). From product concept to user experience: exploring UX potentials at early product stages. *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries (NordiCHI´10)* , pp. 473-482.

Thomas A. Burnham, J. K. (2003 , April). Consumer Switching Costs: A Typology, Antecedents, and Consequences. *Journal of the Academy of Marketing Science* , pp. 109-126.

Venkatesh, V. a. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* , pp. 425-478.

Westland, J. C. (2010). Critical mass and willingness to pay for social networks in: Electronic Commerce Research and Applications Vol 9. *Electronic Commerce Research and Applications, Volume 9, Issue 1* , pp. 6 - 19.

Acknowledgements

The following authors contributed to this report:

Richard Wacker, YellowMap AG – r*ichard.wacker@yellowmap.de*
Sophie Wrobel, CAS Software AG – *sophie.wrobel@cas.de*
David Alonso, AMETIC – *dalonso@ametic.es*
Fabian Hermann, Fraunhofer IAO – *fabian.hermann@iao.fraunhofer.de*

This project is a collaborative effort between

Fraunhofer IAO,
YellowMap AG,
University of Siegen,
CAS Software AG,
AMETIC,
Barcelona Digital Technology Centre,
National University of Ireland (Galway) and
Telecom Italia S.p.a.

It is funded under the E.U. 7th Framework Programme, Target Area Intelligent Information Management (ICT-2009.4.3), target d) "Personal Sphere".