1st International Workshop on Values in Design – Building Bridges between RE, HCI and Ethics

6th of September, 2011, Lisbon, Portugal

Christian Detweiler, Delft University of Technology, The Netherlands
Alina Pommeranz, Delft University of Technology, The Netherlands
Jeroen van den Hoven, Delft University of Technology, The Netherlands
Helen Nissenbaum, New York University, USA

Table of Contents

Preface

Designing for values has become increasingly important for technology development. In many technological systems (medical applications, social networks etc.) values (privacy, autonomy, trust etc.) play a role and are sometimes violated. In working with stakeholder requirements or user needs, various design methods in requirements engineering (RE) and human computer interaction (HCI), in specific user-centered (UCD), deal with “soft issues”, “social issues”, “people issues” or values. At the same time, applied ethics has begun to pay attention to design. We believe that many of the approaches could complement each other in useful ways. The aim of this workshop is to bring together people from different disciplines to share knowledge and insights about how to account for values in technology design, and to work towards integrating approaches, thereby putting value conscious design approaches (e.g. values-in-design or value sensitive design) to practice.

Nine submissions were selected for inclusion in the workshop. Topics included approaches to various aspects of design (Thew and Sutcliffe; Normark et al.; Sanches and Bylund), applications (Stark and Tierney; Caplan and Hockenberry; Koch et al.), reflection on existing technology (Dechesne et al., Bozdag and Timmermans), and enquiry into industrial practice (O'Kane et al.).

Christian Detweiler, Delft University of Technology, The Netherlands
Alina Pommeranz, Delft University of Technology, The Netherlands

September, 2011

Organization

Workshop Chairs

Christian Detweiler, Delft University of Technology, The Netherlands
Alina Pommeranz, Delft University of Technology, The Netherlands
Jeroen van den Hoven, Delft University of Technology, The Netherlands
Helen Nissenbaum, New York University, USA

Program Committee

Joost Broekens, Delft University of Technology, The Netherlands
Catholijn Jonker, Delft University of Technology, The Netherlands
David Keyson, Delft University of Technology, The Netherlands
Cees Midden, Eindhoven University of Technology, The Netherlands
Mark Neerincx, TNO, The Netherlands
Barbara Paech, Heidelberg University, Germany
Jens Riegelsberger, User Experience Design, Google, UK
Alistair Sutcliffe, University of Manchester, UK
Yao-Hua Tan, ICT, Delft University of Technology, The Netherlands
Michael Zimmer, University of Wisconsin-Milwaukee, USA

Keynote Talk:
Serving a Community of Homeless Young People through Value Sensitive Design

David G. Hendry

Value Sensitive Design Research Lab
The Information School
The University of Washington
Seattle, Washington, USA

Abstract. For the past four years, we have conducted an unfolding series of service, design, and research projects in a community of homeless young people. Working within the value sensitive design methodology, the overarching aim of this work is twofold: First, to understand how homeless youth adopt digital media and personal digital technologies and generally bring information systems in their lives; and second, to develop design knowledge for improving the welfare of homeless youth through information systems. Our design stance, while explicitly precautionary, is oriented towards intervening through policy, social organization, and information systems. In this talk I will introduce value sensitive design, the project, some key values and value tensions, the direct and indirect stakeholders, and some of the empirical methods that we have been using. I will conclude with some lessons learned and open questions for the application of value sensitive design in this community.

Invited talk: Designing for Trust

Andreas Woelk, Manager, User Experience Design, eBay Marketplaces

As Manager of User Experience and Content Strategy at eBay Inc., Andreas Woelk is leading an effort to create a design and communications framework that seeks to better understand and influence the perceptions of trust within a dynamic, global marketplace.

Since its formation, eBay has provided a platform built on trust that allows buyers and sellers to connect and conduct business on a global scale. In recent years, the company has strongly invested in actively shaping the experience between buyers and sellers and their overall relationship with eBay.

The key focus of this new framework is to put structure around these relationships in order to develop bilateral trust not only between buyers and sellers, but also between buyers and eBay as well as sellers and eBay. To achieve this goal, Mr. Woelk and his team conducted extensive global research, identifying the top priorities and nuances between these relationships and the opportunities to develop them further in unique ways.

The introduction of strategic programs such as purchase protection and seller certification as well as enhancements to the feedback system were important steps taken to support buyers in making informed purchase decisions based on trust in the marketplace. Further, to keep these critical relationships in balance, the team actively engaged the seller community to understand the overall impact to their perception of trust and to ensure that these buyer programs did not come at the expense of sellers' trust overall.

Mr. Woelk is excited to be part of this year's panel on "Values in Design - Building Bridges between RE, HCI & Ethics". He will be discussing the challenges and opportunities uncovered during this unique initiative as well as the innovative methodology that was employed throughout the process.

Values in the filter bubble Ethics of Personalization Algorithms in Cloud Computing

Engin Bozdag and Job Timmermans

Delft University of Technology
Faculty of Technology, Policy and Management
Section Philosophy
P.O. Box 5015, 2600 GA Delft, the Netherlands
{V.E.Bozdag, J.F.C.Timmermans} TUDelft.nl

Abstract. Cloud services such as Facebook and Google search started to use personalization algorithms in order to deal with growing amount of data online. This is often done in order to reduce the "information overload". User's interaction with the system is recorded in a single identity, and the information is personalized for the user using this identity. However, as we argue, such filters often ignore the context of information and they are never value neutral. These algorithms operate without the control and knowledge of the user, leading to a "filter bubble". In this paper, by building on existing philosophical work, we discuss three human values implicated in personalized filtering: autonomy, identity, and transparency.

Keywords: value sensitive design, personalization, filtering, computer ethics, cloud computing, software as a service

1 Introduction

Emerging web technologies such as Cloud Computing allow users to outsource their computing and storage needs to data centers managed by a third party [12]. This transforms the computing world rapidly towards developing software for millions to consume as a service, rather than to run on their individual computers [4]. One of the most important ethical implications of this technological development is the shift of control from users to software providers [18]. Not only do users lose control of their personal data, but computation as well. Cloud service providers can change features and the algorithms of an application "on-the-fly", without the control of the user.

Cloud services, such as Facebook and Google Search inherit these ethical problems and often deal with large amounts of user generated data. The availability of immense computing power and storage offered by the cloud leads to a fast increase in the generated and stored data.[1] The amount of data makes it very difficult for the user to select and process relevant information. In order to overcome this "information overload", cloud services started developing personalization algorithms.

[1] According to Cisco's latest research, in 2015, consumer generated data on the Internet will be 4 times more than what it is in 2010 [5].

Web personalization is the process of changing the content and structure of a web application to adapt it to the specific needs, goals, interests and preferences of each user [7]. By building a user model, the beliefs and knowledge that the system has about the user is captured [7]. This way the system can predict what will be relevant for the user, filtering out the irrelevant ones, increasing its personal relevance to an individual [2].

For instance, according to Pariser [14], Google uses various "signals" (previous search keywords, location, status updates of contacts in social networking sites, etc.) in order to customize search results per user. Facebook on the other hand checks a user's interactions with other users, and filters certain users' posts. This means user activities (click history) are translated into a single identity, and on the basis of this identity certain information is filtered out. Further, photos and videos receive a higher ranking than regular status posts. Facebook therefore determines the importance of the information on behalf of the user.

The problem with this sort of algorithmic filtering is that information is filtered before reaching the user, and this occurs silently. The criteria on which filtering occurs are unknown; the personalization algorithms are not transparent. The user's previous interaction with the system is the basis of future personalization. However, as we later will argue, we have different identities, depending on the context, which is ignored by the current personalization algorithms.

Personalized filtering is gaining importance and it is used by many cloud services. Considering the increase of popularity of cloud services, we can expect to see personalization more often in the future. This, therefore, requires a good analysis of the implicated values in the design of such algorithms.

In this paper we use Value Sensitive Design methodology [6] to identify the values and value assumptions implicated in personalization algorithms. In Section 2, we start a conceptual investigation by clarifying the (moral) value of information and the necessity of filtering in the information age. In Section 3, the concept of 'personalized filtering' is investigated by relating it to a theory of filtering. Next, in Section 4, building on existing philosophical work, we discuss three human values implicated in personalized filtering: autonomy, identity, and transparency. Finally, in Section 5, we conclude with a list of guidelines to consider when designing personalization algorithms.

2 Value of Information and the Need for Filtering

In his book *A Theory of Justice* [16], John Rawls introduces the concept 'primary goods': goods that are supposedly useful (or at least not harmful) to anyone, irrespective of their conception of the good. By applying Thomas Pogge's widely accepted interpretation and extension of the Rawlsian idea of justice [15], Van den Hoven and Rooksby [10] argue that information should be accepted as a primary good within Rawls's theory. Information online is vital for people to plan their lives rationally and to participate adequately in the common life of their societies [10].

Thus, having access to information affects the worth of liberty felt by an individual. We therefore argue that personalizing algorithms affect the moral value of information as they facilitate an individual's access to information. Contrary to earlier stages of the Internet-era, when the problem information access boiled down to having access to hardware, nowadays the problem of access to information concerns the ability of intentionally finding the right information, or unintentionally stumbling on upon relevant information. We rely more and more on technology to find relevant information. In the cloud, relevance is determined to a large extent by algorithms.

The lowering of cost of communication and production of informational goods enabled by the Internet, has led to an enormous increase in information available to the public both in quantity and diversity [1, 17]. The declining influence of traditional news media as filters to the flood of information that is unleashed every day, the threat of information overload arises. *'Having too much information with no real way of separating the wheat from the chaff'* is what Benkler [1] calls Babel objection: *'individuals must have access to some mechanism that sifts through the universe of information, knowledge, and cultural moves in order to whittle them down into manageable and usable scope.'*

The question then arises whether the service providers currently active on the Internet are able to fulfill the 'human need for filtration'. Although the fulfillment does not hinge on proprietary services alone as there are cooperative peer-production alternatives that operate as filters as well, the filtering market is dominated by commercial cloud services like Google and Facebook[2].

3 Filtering

In this section we first give a theory of filtering based on Goldman [8]. We later describe the characteristics of personalized filtering done by algorithms.

3.1 A theory of filtering

According to Goldman [8], filtering involves a designated channel of communication and a system of people with three kinds of roles (Figure 1): senders, receivers and the filterer (or gatekeeper), an individual or group with the power to select which of the proffered messages are sent via the designated channel. When a gatekeeper disallows a message, this is filtering. According to Goldman, not every form of filtering is censorship. Filtering occurs for instance in peer-review process in scientific journals where the reviewers are the gatekeepers, or in the system of trial procedure, where the judges are the gatekeepers. Certain filtering practices are commonly rationalized in terms of helping the relevant audience to determine the truth.

Goldman identifies 3 doxastic stages, processes that ultimately produce belief (See Figure 2). In order for people to believe truths and avoid believing falsehoods, some selections must be made at one or more stages. If filtering happens at the reporting stage, the gatekeeper filters some of the sources or certain types of information to be sent to the receiver. If filtering happens at the reception stage, all the information is sent to the receiver, and the receiver himself can choose which messages he wishes to receive, that is, read, and digest. The receiver does this by first

[2] In 2010 in the UK for instance, Google and Facebook dominate as gateways to the wider Internet [9].

selecting which channels to tune in to and then selecting which messages aired or displayed on those channels to 'consume' (read or listen to). Finally, in the acceptance stage, the receiver, having read a certain number of messages on a particular topic, must decide which of these messages to believe. According to Goldman, if the gatekeepers, for instance newspaper editors, are not competent enough, filtering done at the reporting level might not be reliable.

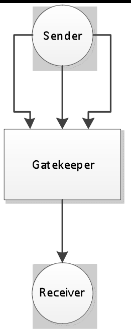


Figure 1. Roles of filtering

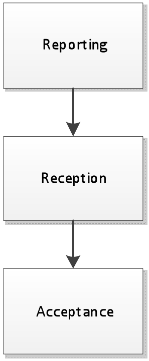


Figure 2. Doxastic stages

3.2 Personalized filtering

In Cloud Computing, algorithms practice the role of the gatekeeper, reducing the volume of information reaching their users (receivers) during the reporting stage (Figure 2). Depending on certain criteria, the information is personalized per individual user. Because of this, the information is filtered before reaching the user, and it occurs silently. If important and diverse information is already filtered out by the system, the user might come into a different belief. User also cannot customize the filtering. If he is aware of it, opting out is possible. However, as we have argued in Section 2, the filtering is needed; an option to turn it on or off is not enough.

Since the outcome of personalized algorithms depend on many factors (number of users who are using it, differences in languages, variability of the user input, etc.) the outcome and reliability of the algorithms are very difficult to predict, even for the engineers who developed them. According to Pariser [14], complex systems such as Google search engine have reached a level of complexity at which even their programmers cannot fully explain any given output.

4 Values in Personalized Filtering

In their article on the politics of search engines, Introna and Nissenbaum [11] claim that the design of search engines is 'not only a technical matter but also a political one.' (p.31) Building on the Rawlsian notion of information as a primary good, they argue that the design of technical mechanisms behind search engines should transcend commercial needs as dictated by the marketplace and involve political choices concerning social justice such as equality and inclusiveness. This boils down to design challenges such as the incorporation of 'human values', e.g. "relevancy", into the search algorithm. Introna and Nissenbaum thus argue that these algorithms must be considered as value-laden or non-neutral.

The main mechanism behind search engines is filtering; these systems filter at the "reporting" stage (Figure 2.) Personalization algorithms, just like search algorithms also contain embedded values. In this section we discuss three human values implicated in personalized filtering: autonomy, identity, and transparency[3].

4.1 Autonomy

In section 2 we discussed the Babel objection to stress the necessity of filtering. This objection, Benkler [1] argues, can only be answered when it is accepted that filtering is vital to an autonomous individual (p.174). The ability of filtering of informational goods thus is closely related to autonomy.

According to Brey [3], to be autonomous is to be a self-governing agent. Autonomy can thus be defined as *'self-governance, that is, the ability to construct one's own goals and values, and to have the freedom to make choices and plans and act in ways that are believed by one to help achieve these goals and promote these values.'* [3]. Autonomy is therefore essential for a life to be meaningful and fulfilling.

In order to be self-governing and make choices one needs to be properly informed. The unprecedented availability of information offered by the Internet can be regarded as an increase in the degree of autonomy of individuals. The quantity of information available makes filtering inevitable, however. The reliance of individuals on web services supporting their quest for relevant information, without providing insight on the filtering process, can decrease user autonomy.

Although it is impossible to sift through all sources of information ourselves, in order for us to employ our capacity for choice, it seems that we at least need to be able to assess and influence the mechanisms that are doing the filtering for us. The value of autonomy thus implies more influence and control of users over the filtering process in order to align it to their personal preferences. The promise held by the Internet of an increase in the degree of autonomy due to a wider availability of information can therefore only be fulfilled when there is proper filtering in place.

The filter bubble is a phenomenon that is closely related to what Sunstein have called "echo chambers" [17]. Sunstein worried that citizens would use technological tools to over-customize their information sources, leading to what he calls "echo chambers" or "information cocoons" [17]. However, there is a major difference; filter bubble occurs without the autonomy of the user.

It should further be noted that the value of autonomy is potentially in conflict with a defining feature of Cloud Computing: the shifting of control from users to third party service providers. Because of this control shift, the service providers can add features to the existing software, such as personalization, without notifying their users. Thus, while autonomy entails controlling the filtering service, the technological properties of the underlying architecture and software make it more difficult to realize this value.

4.2 Transparency

[3] Due to limited space and time available we focus on only three values. Further analysis is needed to identify other values and value assumptions, such as trust, anonymity, etc.

Transparency is closely related to autonomy. A user cannot assert control in an opaque system, since he will not be well informed how the system works. If the user has prior knowledge to the information requested when he uses the cloud service, he can assess the quality of the delivered information. However if the user does not know what he wants, then he cannot assess if he is receiving relevant information. For instance, a query for "Ajax", intending the mythological Greek hero, is returned by Google with a first page filled with results about Amsterdam's football team (which is also called Ajax), because I live in the Netherlands. Since I know which result is relevant to me, I can check other pages or revise my keyword to find the information I am looking for. However, if I am searching for "best digital camera", and Google assumes that the price is the most important criterion for me (because of my previous search keywords), then I will not be able to assess the quality of this information.

According to Introna and Nissenbaum [11], users have the right to demand full and truthful disclosure of the underlying rules or algorithms governing indexing, searching, and prioritizing, stated in a way that is meaningful to the majority of Web users. Even though this helps spammers, authors argue that this will lead to a clearer grasp of what is at stake in selecting among the various services. Pariser [14] argues that for the users to control the services they are using, users must know what information is used for personalization and how their data are used.

We are not so sure whether full disclosure of the underlying algorithm will lead to full transparency and better user experience. Not only because of possible misuses such as spam and conflicts with trade secrets, but it will be very difficult for an average user to comprehend the algorithm. Instead, the implications of such algorithms must be shown to the user. When a personalized filtering takes place, the user should be notified of this filtering activity and also on what basis the system is filtering. This way he will know that he might be missing some information..

4.3 Identity

In personalization, by tracking the online activity associated with the user a profile is created that represents traits of the user's identity. Personalized filtering is thus based on an interpretation of a user's identity. Identity refers to people's understanding of who they are over time, embracing both continuity and discontinuity [13]. To a certain extent there is also a discontinuity of identity when a person moves from one context to the other. In her account of privacy as contextual integrity, Nissenbaum [13] argues that the kind of privacy needed depends on the particular context personal information is flowing to. In each context individuals have different expectations of what kinds of information are appropriate and inappropriate and how that information should be distributed. When these information norms are violated, an individual's privacy is infringed. According to Nissenbaum, privacy thus involves a person's ability to control the flux of his/her personal data being distributed for each particular context.

The idea that a person has different expectations per context about what information she wants to share can be useful in explaining filtering needs. Just like sharing, as a person has expectations about what information she holds as appropriate or suiting to receive in a particular context. In a social context, such as being amongst friends, sustaining relationships might be more important than realizing professional ambitions (although these goals sometimes do coincide).

When contextual expectations are taken into account, autonomy is not just dependent on filtering as such, but more specifically on filtering according to particular contextual requirements. These requirements are related to traits of one's identity materialized in a profile used by algorithms to personalize filtering. Currently personalized filters used by most cloud services often do not take the context of a person into account. As a result all information is filtered to a generic identity or profile of the user. For instance, in Facebook, if I do not show interests in the pictures of a contact, the system will assume that I have no interest in this contact at all. However, I might be interested in his status updates about work related links.

The one-filter for all interactions principle can be omitted when discontinuity of identity in different contexts is taken into account. When different personalized filters can be deployed in different settings, conflicting context specific requirements are no longer in each other's way.

5 Conclusion and Recommendations

To recapitulate, building on the work of Van den Hoven [10], we showed that access to information should be viewed as a primary good in terms of Rawls theory of justice. Then we argued that due to enormous increase in information supply this good can only be obtained by individuals if they rely on filtering technology. Next, we showed by extrapolating on the work of Introna and Nissenbaum [11] on search engines that filtering is not a value neutral process. We then dicussed three values in design of personalization systems: autonomy, identity and transparency.

We argue that implicated values should be taken into account during the design of personalized algorithms. In order to do that, it would be useful to come up with a list of guidelines to consider when designing such algorithms. Accordingly, we have a tentative suggestion of what such a list could look like. This list is intended to be a first proposal, not as the final and only possible list.

Our analysis of the cloud services is based on personal interactions with these systems and the work of Pariser [14]. More empirical study is needed in order to understand full implications of these algorithms. Further, even if the service providers design personalization filters that respect the identified values, the user can still trap himself in his own "echo chamber"[17]. This brings the question whether information intermediaries such as Google and Facebook have a social responsibility to expose the user to public values, in order to increase diversity of information. This will allow the user to encounter information he did not know and that was not available through his friend network. However, questions such as which public values should be included remain open. More debate is needed to answer these questions.

Table 1. Guidelines for Designing Personalization Filter Algorithms
1. Make sure different identities are allowed per user, which might differ per context.
2. Design for autonomy, so that the user can customize the filter, and change the identity that is formed on basis of his previous interactions.
3. Design for transparency, so that the user is aware that a filter is taking place. The user must be able to see which criteria is used for filtering, and which identity the system has of the user.

Funding

This research is supported by the Netherlands Organization for Scientific Research (NWO) Mozaiek grant, file number 017.007.111

References

1. Benkler, Y. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom (Yale Press).
2. Blom, J. (2000). Personalization - A Taxonomy. CHI 2000. April (2000).
3. Brey, P. (2000). Disclosive computer ethics. SIGCAS Comput. Soc. 30, 4.
4. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems 25 (6) , 599–616
5. Cisco Systems (2011). Cisco Visual Networking Index: Forecast and Methodology, 2010–2015, whitepaper.
6. Friedman, B., Kahn, P. H., & Borning, A. (2006). Value Sensitive Design and Information Systems. Technology, 3(6), 1-27. ME Sharpe.
7. Garrigós, I,. Gomez, J., and Houben., G. (2010). Specification of personalization in web application design. Information and Software Technology, 991- 1010.
8. Goldman, A. (2008). The Social Epistemology of Blogging. Information Technology and Moral Philosophy. Cambridge University Press.
9. Hitwise (2010) Social networks now more popular than search engines in the UK. Available at http://www.hitwise.com/index.php/uk/press-centre/press-releases/2010/social-media-alert-june-2010/ (Accessed:27 July 2011)
10. Hoven, MJ van den & Rooksby, E (2008). Distributive justice and the value of information: a (broadly) Rawlsian approach. Information technology and moral philosophy (pp. 376-396). Cambridge, New York
11. Introna, L.D. and Nissenbaum, H. (2000). Shaping the Web: Why the Politics of Search Engines Matters. *The Information Society,* 16, 169-185
12. Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud Computing and Information Policy. Journal of Information Technology and Politics 5 (3).
13. Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review* Vol 79, No. 1, February 2004: 119-158
14. Pariser, E. (2011), The Filter Bubble: What the Internet Is Hiding from You. Penguin Group USA
15. Pogge, T. (1989). Realizing Rawls. Ithaca: Cornell University Press
16. Rawls, J., A Theory of Justice, Cambridge Mass., Belknap Press of Harvard University Press, 1971
17. Sunstein, C. (2007) Republic.com 2.0, Princeton University Press

18. Timmermans, J., Stahl, B.C., Ikonen V., and Bozdag, E. (2010). The Ethics of Cloud Computing:A Conceptual Review. Cloud Computing, HCI, & Design: Sustainability and Social Impacts, 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, USA.

Application Autopsy and Artifact-Altering Technologies

Robyn Caplan[1], Matthew Hockenberry[1]

[1] Department of Media, Culture, and Communication, New York University
239 Greene Street, 7th Floor New York, NY
{rdc310, hock}@nyu.edu

Abstract. Product Autopsies “dissect” material goods to understand what goes into them, where these components come from, and what that means for producers, consumers and owners. We extend this idea to digital “goods” — looking at the autopsies of web sites and web applications in order to better understand them. Every web application is the product of a careful process of construction. Libraries, platforms, links, and embeds are pulled together to construct a commodity with a seemingly concrete appearance. App Autopsies expose these connective threads in order to understand the implications for the site, and its visitors, across a variety of value dimensions.

Keywords: Internet ethics, open source, commons-based peer production, reflective design

1 Introduction

Product autopsies take apart a finished artifact to examine the parts constituting the whole. They take objects that have been packaged, boxed up, and commodified, and open them up to inspection and scrutiny. The dismantling of a product results in its contextualization and creates a design methodology that investigates the ramifications of design decisions. This "dissection" opens up the internal workings of products and technologies and, in doing so, asks designers to observe the effects of particular design decisions, their externalities, consequences, and future implications. They may notice that items which are presented as functional (screws or other fastenings) serve only an aesthetic role, while other components selected for particular technological capabilities have design consequences that shape the form and function of the object [1]. *App autopsies* extend this practice to digital artifacts, opening them up to understand the consequences and concerns of particular technological choices made in their construction.

Our work (http://appautopsy.com) implements this analysis with digital dissections inspired by those conducted on products (and bodies of all kinds). While the name implies the inspection of a dead object, the autopsy of the digital more precisely performs dissections on living artifacts; websites and other applications; artifacts which are in active use and are therefore still capable of being transformed. This reveals elements of digital design that cannot be directly seen, or are intentionally obscured, through the interface.

At the centre of this project is a belief in reflective design. Sengers et al. define this approach as one of "critical reflection." A process of "bringing unconscious aspects of experience to conscious awareness, thereby making them available for conscious choice" [2]. Without this critical reflection, they argue, individuals will embrace and maintain attitudes, practices, values and identities without a conscious acceptance or understanding. Our implementation of "The App Autopsy" was built to further the ends of this reflective practice. Through a visualisation of the constituent elements of digital applications, it supports a new awareness of the political and cultural choices being made as a result of the use of digital applications. It stands in opposition to an *instrumental theory of technology*, which would view digital applications as value "neutral," indifferent to the political and economic systems (such as socialism or capitalism) which exist in the modern world. Instead, the App Autopsy is used to bolster a *critical theory of technology*, as developed by Andrew Feenberg [3]. This theory resembles a *substantive theory* in rejecting the neutrality of technology, but, rather than place the moral emphasis on technological design, as substantive theory suggests, a critical theory would take a descriptive approach to the technology and determine where and how these technologies - or our relationship to these technologies - can be changed. The App Autopsy is therefore a tool which can be used to transform a critical theory of technology into *praxis*.

It is through this theory that one can begin to delineate a place for values alongside the other technical standards and functional goals of design. App autopsies aid in the descriptive theory of a technology, in an effort to promote critical reflection. To demonstrate the existence of values within technical systems and devices, there was a pragmatic and conscious attempt to integrate values into the design. The App Autopsy was built using the methodology, *Values at Play,* provided by Mary Flanagan and Helen Nissenbaum, in "Embodying Values in Technology: Theory and Practice," [4]. This methodology holds that to achieve a technical design which soundly incorporates values, designers must not only be competent with the technology and science, but they must also have a reflective understanding of relevant values and the way in which these values function in the lives of peoples affected by the technical systems in question. Values at Play postulates that conscientious designers must "juggle" the relevant dimensions of three interrelated modes of inquiry: the engagement of scientific and technical results, relevant philosophical reflections on values, and empirical investigations of values in relation to individuals and their societies.

2 The App Autopsy

The App Autopsy is a tool which can be used to critically reflect on any digital application. When entering the site, the user encounters a screen providing a url prompt. Entering a url into this text box results in an *autopsy* of a site, visualized as a three dimensional cube comprised of multiple layers. Each layer represents an application or technology that has been used in the construction of the site. The user can analyse these results by choosing from a list of values. The visualizations are then ordered by the coded value. For example, a user concerned about web standards would see those components which conform to WC3 standards in white, and those which do not conform, in magenta. In this way, the App Autopsy makes clear the values latent in the technological construction of the artifact.

Those applications normally hidden from view, become visible, allowing the user of our product to assess the state of the applications they use frequently. This inward look at digital applications is critical reflection, "bringing unconscious aspects of experience to conscious awareness," thereby making them available for conscious choice [5]. The App Autopsy is an attempt to draw attention to the blind spots. The site acts as a perceptual field, but one that is dependent upon the observer, and requires participatory design to expand the value categories used to classify various applications.

2.1 Technological Mode

The App Autopsy is structured to be extensible and generic. At a broad level, given a specific url, it extracts the markup rendered and processes it to discover specific technologies. It does this by operating a series rule files that describe regular expressions, heuristic rules, and other techniques for determining the existence of a particular technology. For example, it may determine that the jQuery javascript library exists based on the presence of a specific javascript include, the use of specific jQuery functions throughout other javascript files, or a reference from a mainstream content delivery network. As the rules process, it builds a key-value listing of the technologies and versions of those technologies that are revealed by the process. Once a key-value listing has been built, the system loops through sets of value files that map values to particular technologies. Value file contain additional meta information (citations, descriptions, etc.) as well as particular value-ranking pairs. Additional value ranking pairs can be constructed, but the core free and open value set demonstrates the mapping of values to particular technologies. In addition to the value rankings, notes and citations accompany the value mappings in order to allow users to evaluate them.

We agree with the suggestion that a design team should consider recent developments in their field of interest on design specifications that might help them in realizing values within the design process [6]. In the technical mode, a designer reflects upon existing technologies which might realize the technical standards and values the designer is attempting to leverage. The site was built by extending the opensource project WhatWeb, a system that parses web applications to examine individual technological components, and integrates services like geocoding and visualization [7]. In addition, we merged this information with a system of annotations that would serve to classify each application being parsed. These annotations classify an application based on the presence or absence of certain features. They are themselves extensible, developed in a similar manner to other open source collaborative projects following the format of citation, argument, and value assignment. This process began with values developed from the free and opensource software community, an exemplar value set that can be taken and extended [8].

Four programs were found which exemplified the functionality required by the App Autopsy: Builtwith, WhoApi, Quarkbase, and WhatWeb [9]. Each of these sites use algorithms designed to gain back-end information on a digital application through various data sources. Their purpose and often their analysis differs from that required by the App Autopsy, although they are certainly *app autopsies* of a sort. Builtwith, WhoApi and Quarkbase are programs intended for commercial purposes, and give their users information on the functionality of a site, and its popularity online. WhatWeb provides an opensource scaffolding that is directly extensible to us. We can not only integrate additional services with WhatWeb, we also modify the character of its output, producing a three-dimensional visualization in an architectural metaphor. Each layer signifies a technology that comprises the application located at the url queried. This analogy of a building highlights the aggregate nature of applications, which are composed of many elements built upon one another, and resting atop tangled networks constructed by users and designers. The code used to build an application serves as a blueprint for what they eventually become, each element regulating a range of possible behaviours and experiences online. The construction of a site and the use of one component over others is the realization of one value in the place of another.

2.2 Philosophical Mode

The philosophical mode implores designers to address questions about the origin and scope of values relevant to their technical creation. While this mode necessitates a discussion on the contentious debate of the origin of values, this will not be addressed in this work. This section will, however, outline those values which were instructive in the development of the App Autopsy.

The values of the site itself were informed by existing work done in the philosophy and history of technology, and in the field of human-computer interaction. Fundamentally, the site presupposes that technologies can have politics and are therefore not value neutral, expanding Langdon Winner to treat this idea as a *practice* of inspection [10]. Arguing that one must "pay attention to the characteristics of technical objects and the meaning of those characteristics," Winner has arguably set the stage for product autopsies. By studying the constituent elements of applications, it is possible to determine where meaning and values are produced in seemingly apolitical digital products. Winner also suggests that technological objects should not be removed from their context and should be examined in favour of explanations that seek to expose an "interplay of social forces." The applications studied using the App Autopsy cannot therefore be separated from communities which already adhere to a particular set of values.

Following from this idea, in performing autopsies using our site, users can parse applications according to an exemplar value set. We selected as an exemplar value set, those that are found in the free and opensource software community. In particular we draw these values from the Debian Constitution and Social Contract which emphasizes freedom, openness, and transparency [11]. Development of additional value sets can be accomplished by following traditional opensource development. While developers are not able to contribute directly to the value definitions and rankings in app autopsy as hosted, they are able to create their own forks. By observing these forks, we can pull additional value definitions (or possibly alternative rankings for existing values and technologies) and merge them into our value definition. These values are extensible. Users are able to develop annotations with different value categories and evaluations of particular technologies (the justness of a javascript library, for example).

This approach follows from a principle of technological change [12]. Technologies built using an open source framework introduce an expectation of participatory and incremental innovation and growth. Postman argues that one must acknowledge that technological change is ecological, not additive, and "therefore too important to be left entirely in the hands of Bill Gates." The participatory requirement of the App Autopsy is founded in this necessity for placing both these determinations of value, and the information informing these decisions, in the hands of the largest amount of individuals possible. This type of organization follows from Yochai Benkler's *commons-based peer production*; a model which describes the leveraging of large numbers of individuals who coordinate work on projects, often attempting to evade a hierarchical structural organization [13]. This socio-economic system of production, both Nissenbaum and Benkler argue, has emerged "in the digitally networked environment" and is facilitated by the material and technical infrastructure of the Internet [14]. In this system, no one owns a free software, project…[and there is] no formal manager who tells different people what they must do so that the project can succeed." While this type of system of production is available to all, it does, however, require a degree of computer and web literacy that is not attainable by every individual online. In terms of the App Autopsy, every individual can, in theory, reap the benefits of this system of production, but only those with even a basic knowledge of open-source software development will be able to contribute to the design of the tool.

Regardless of the level of technical skill of potential contributors and modifiers, the App Autopsy can be used by any individual to reveal the back-end of applications in a comprehensible format. This practice is intended to address another principle of technological change espoused by Postman:

> *"*[T]*echnology tends to become mythic; that is, perceived as part of the natural order of things, and therefore tends to control more of our lives than is good for us."*

Postman's continuation of Barthes' idea describes a process wherein objects become naturalized; technological creations, once developed and laboured over by human hands and minds, become accepted as fixed objects without histories or futures. The technology is then seen as beyond modification or control, and is transformed into a black box which hides the character of its internal workings, making it immune to inspection.

Digital applications have gained this mythic status for many users. A lack of literacy in code, or an understanding of the function of various web applications, can have consequences for individuals using these products. For instance, without this understanding individuals use applications that compromise their privacy, unknowingly releasing their data. While this practice is legal, digital applications go to great lengths to minimize the visibility of this practice. Without knowledge of these operations taking place, an individual can neither consent nor object to the practice. The App Autopsy reveals this practice under the assumption that if such operations are made visible, users will be aware their data is being monitored, stored, and even shared, online. The openness provided by the App Autopsy might have the unintended consequences of creating security vulnerabilities for certain websites and web applications, however, with an increased awareness of such vulnerabilities, developers have the opportunity to address the problem.

2.2.1 Value Nomenclature

The App Autopsy uses a classification system for digital applications that is influenced by the values the authors themselves hold. The system addresses the challenges for classification systems outlined by Geoffrey C. Bowker and Susan Leigh Star, in “Sorting Things Out: Classification and its Consequences” [15]. The classifications use a consistent citation structure, which uses similar language for each category to identify whether an application (through its operationalization or implementation) fulfills the requirements for inclusion or exclusion. The classification is done through an assessment of presence or absence of certain features that gave us the nomenclature positive, neutral and negative. This limited classification system was done to constrain any ambiguity; either the application has features indicative of a category inclusion, or they do not. They are visible in that the classification is available in the code, and open to inquiry should a user want to use the code to produce their own site with alternative classifications. Evidence must be provided, and the source used for the classification is available to view.

As an example, consider Opengraph, Facebook’s technology for manipulating and storing the social graph created by their social network. The rankings for Opengraph have been generated by surveying news stories and articles that highlight opinions about Opengraph with regard to our exemplar value set - we look for consensus among multiple sources when possible. For example, we rank it as non-private, it is widely reported to hoard invasive user metadata. We evaluate it as non-webstandard, developed and owned by a commercial entity, and leveraged for profit making. At the same time we rank it as transparent and accessible, because it is well documented, publicly presented, and presents useful capabilities and technology hooks for developers. Each of these rankings is accompanied by a link or a note justifying the process

The App Autopsy relies on information acquired through production. The common goal of the project, a record of present state and changes made to digital applications, benefits greatly from repeated inquiries into the changes made to web applications over time. As it stands, the only way to accomplish this would be through multiple instantiations of App Autopsy tools, which address different values drawn from different sets of value annotations.

2.3 Empirical Mode

Using the methodology provided by Flanagan, Howe and Nissenbaum, empirical investigations would be required to examine whether our attempt at embodying the values embodied in the App Autopsy has been successful. We did discover, however, that the site cannot parse for subdomain information. This will be addressed as we continue the investigation. Empirical investigations with users have not been fully developed. To test whether the site provided additional information not known to users before the use of the site, a survey administered both prior and post-use of the site could be helpful in determining whether the site was successful.

While the relevant interest groups have not yet been fully exhausted, we have identified several groups who have a vested interest in performing Application Autopsies. These are: governmental organizations assessing the conformance to web standards, programmers and web application designers, owners of web applications, and lastly, curious individuals online (ideally all individual impacted by web technology would share this interest). The first three categories have a direct participation in digital application design but their roles in this process are frequently quite different. The last category encompasses those affected by design and who influence a digital application through use. This category has been further stratified in terms of technological and non-technological individuals and is more inclusively considered.

3 Conclusion

The classification system is one way in which we can innovate in the future. Ideally individuals would be able to create their own systems of classification, and add information to the site without needing the technical skill necessary to fork and develop the value sets through a technological practice. This, however, would require servers that could provide a degree of data protection and privacy that would correspond with the values embedded in the goals of the site itself. Additionally, we hope to be able to store various changes in the design and development of web applications. This feature would be able to track changes made to the code of sites like Facebook, which would highlight the transformations in technology that would have repercussions for categories such as privacy and property. Ideally this would involve caching a site to provide a snapshot of a digital application during a specific period of their development. Lastly would be a modification of the site that would demonstrate any overlapping between the use of specific technologies, between sites. This would be in an effort to examine how different communities of sites (perhaps with their own social, commercial and political agendas) form around various technologies.

Product Autopsies are performed to introduce a critical theory of technology into practice. The App Autopsy acts as a tool to aid individuals in understanding more about the applications they are using online.. Since the artifact scrutinizes other digital applications, it became necessary throughout the design process to subject the App Autopsy to the same criticisms. Every design decision was evaluated to ensure that we did not violate one of the values that we used to classify other digital applications. While our values did become embodied within the site, we will remain open to scrutiny by those who hold different values from our own. This can be done through modifications of the code provided online.

The App Autopsy was developed in an effort to both integrate values in design and showcase the values embedded in other design systems. The site attempts to prevent the closing down of digital technologies, to demonstrate the flexible nature of digital design.

Acknowledgments. We would like to thank Helen Nissenbaum for her generous support and feedback on this work.

References

4. Bonanni, L., Parkes, A., and Ishii, H. Future Craft: How Digital Media is Transforming Product Design. In CHI '08 extended abstracts on Human factors in computing systems. (2008)
5. Sengers, P., Boehner, K., David, S. and Kaye, J. “Reflective Design.” Culturally Embedded Computing Group. Ithaca, NY: Cornell Information Science, 49-58. (2005)
6. Feenberg, A. *Transforming Technology: A Critical Theory Revisted*. New York, NY: Oxford University Press. (2002)
7. Flanagan, M., Howe, D., and Nissenbaum, H. "Embodying Values in Technology: Theory and Practice." Information Technology and Moral Philosophy. Eds. J. van den Hoven and J. Weckert. Cambridge: Cambridge University Press, 322-353.(2008)
8. [Sengers et. al.]
9. [Flanagan et. al]
10. WhatWeb, http://WhatWeb.com
11. Constitution for the Debian Project (v1.4), http://www.debian.org/devel/constitution; Debian Manifesto, http://www.debian.org/doc/manuals/project-history/ap-manifesto.en.html
12. BuiltWith, http://builtwith.com; WhoApi, http://whoapi.com; Quarkbase, http://quarkbase.com; WhatWeb, http:WhatWeb.com.
13. Winner, L. "Do Artifacts have Politics?" The Whale and the Reactor. Chicago: The University of Chicago Press, 19-39. (1986)
14. [The Debian Project]
15. Postman, N. "Five Things We Need to Know About Technological Change." Denver, CO (1998)
16. Y. Benkler and Nissenbaum, H. "Commons-Based Peer Production and Virtue." Journal of Practical Philosophy. 14(4), 394-419. (2006).
17. Geoffrey C. Bowker and Susan Leigh Star, in “Sorting Things Out: Classification and its Consequences,” (1999).
18. Friedman, B. & Nissenbaum, H. Bias in Computer Systems. ACM Transactions on Information Systems. 14(3), 330-347. (1996)

Requirements for Reconfigurable Technology: a challenge to Design for Values

F. Dechesne, M.J. van den Hoven, M.E. Warnier

Department of Technology, Policy and Management,
Delft University of Technology, The Netherlands
Jaffalaan 5, 26282 BX Delft
The Netherlands
Tel. +31-15-2785143
Fax. +31-15-2786439
F.Dechesne@tudelft.nl, M.J.vandenHoven@tudelft.nl,
M.E.Warnier@tudelft.nl

Abstract.

With the increasing use of information technology for different societal goals, the demand for flexible and multiple-functionality appliances has risen. Making technology reconfigurable could be a way of achieving this. This working paper is written against the background of a large scale research project developing reconfigurable sensors in order to achieve a continuous and affordable infrastructure for both safety and security (STARS). Our role in the project is to explore the ethical challenges reconfigurability raises for sociotechnical systems like sensor networks. We foresee that reconfigurable technology adds an extra challenge to the identification and specification of functional and non-functional requirements for the technology.

Keywords: reconfigurability, design for values, sensor networks

1 Introduction: the STARS project

This paper is written against the background of a large scale research project in The Netherlands called STARS: Sensor Technology Applied in Reconfigurable Systems. The STARS project is still in its initial phase, and involves both academic and private research partners. The project is motivated by the fact that our current society shows an increasing complexity and associated risks, under the influence of developments like globalization and the growing use and dependence on technology. In response to this, more technology is developed and deployed in order to manage both complexity and risks. Sensors (like, e.g., cameras or motion detectors) are viewed as important sources of information that can be used to protect our society against threats on the one hand, and to help resolve crisis situations on the other. Such sensors are connected in networks, allowing for gathering and analyzing the combined information, and making it accessible to human decision makers. Especially the application area of security has pushed the development of all kinds of sensor technology.

The goal of the STARS-project is the development of "*necessary knowledge and technology to be able to build reconfigurable sensors and sensor networks*" [14]. By making sensors reconfigurable, the project aims to deliver a continuous and affordable infrastructure for societal security, but it also anticipates possible use in other application areas. Reconfigurable parts of sensor networks that will be looked at are antennas, receivers, transmitters, on-chip and off-chip communication. As an example, one may want to be able to transform a sensor network installed in a harbor for security purposes, e.g. to prevent theft or sabotage, into an information system for rescue workers during a fire in the same harbor.

The security domain is characterized by the great diversity of threats and the absence of warning time. The creativity of the opponent ensures that the circumstances change continuously and unpredictably so. It is therefore essential to be able to anticipate and respond adequately to new situations. The societal problem is that it takes too long, and it is too expensive, to invest over and over again in new systems to be developed to protect against ever changing threats. Truly successful security technologies should therefore satisfy a number of characteristics: reliable and affordable, sustainable and effective, multi-domain and multi-service.

Reconfigurable sensors are developed to have these characteristics. They allow for flexible application, because the functionality enclosed in the system can be altered relatively simply and quickly. In the scenarios that are expected, reconfigurability is used to instantaneously optimize for foreseen situations and the corresponding tasks. In the new, unexpected scenarios, the reconfigurability is used to respond to circumstances that were unforeseeable at the time of the system development, by adapting the functionality of the system to the new situation.

With this as motivation, the feature of reconfigurability will be leading in the design and development of the architecture and technologies in the STARS-project. Although the first use cases primarily speak of the police, security- and information services fire brigade as intended users, it is expected that the technology, if successful, will cover a broader application area by a broader range of users. During the project, system concepts and application potential are to be defined and explored.

The reconfigurable sensor networks are developed to serve the societal goals of safety and security, but it is not just the technical features of the network that will determine the effect of the technology. The effect will be determined by the way in which the system with its features is embedded in social and societal structures: What data will be gathered and by whom? Who will handle the data? How will the data be used? Who determines the priority of functionalities, if the system is intended to serve different goals? The aspect of reconfigurability makes these questions even more complex, but also more pressing. The role of the authors of the current paper is to evaluate societal and moral implications of the technology that is developed within the STARS-project.

We illustrate these issues in the next section, where we describe a use case from the STARS project. As the project in itself is still in its initial phase, this paper presents an initial exploration of questions we think will be the relevant ones, rather than giving theories and answers. In the rest of the paper, we aim to show that reconfigurable technology adds an extra challenge to the identification and specification of functional and non-functional requirements for the technology. Already, the wide applicability of the technology in society (*logical malleability* in Jim Moor's terminology [8]) requires that societal and moral values are considered in the application phase, and ideally also already in the design phase. With the flexibility of reconfigurable technology, this requires new tools. A specification language that is both general and specific enough to cover all possible uses is needed.

2 Use Case: Sensor Usage in a Large Mainport

The intended application of the reconfigurable sensors and sensor networks is the safety and security domain. A use case for the sensor networks is for example the situation at a mainport: a large port area (for example, the port of Rotterdam or Shanghai). Radar systems are used in large ports to 'follow' the movement of ships. Ship sizes can also be determined by these systems. Such radar systems consist of a number of radar devices, which send their data to a central control center. Here the data is processed to provide a full overview of the whole area. Other sensor data, for example from camera surveillance systems (CCTV: *closed circuit television*) or motion detectors (around security gates) is also sent here, providing even more information in case of an incident.

Numerous issues around safety and security can arise in a port environment, including fire hazards, drug trafficking, terrorism, people trafficking or transport of hazardous chemicals. During an incident all sensor data can be combined to coordinate emergency services. Reconfigurable sensors can be very useful in such environments, since they can be used for different tasks as the need arises, whereas previously multiple sensor systems were required. Consider, for example, the case where a small plane crashes into the port area. The police might be worried that this is part of an organized terrorist attack, in which case (part of) the radar system can be reconfigured to look for other (low flying) planes. Information provided by the reconfigured radar system can be very useful in this case, but it also leads to a number of problems.

First of all, by reconfiguring the radar system, the 'normal' radar view of the ships in the harbor is compromised: the spatial resolution will go down, making it harder to distinguish different ship sizes. Part of the harbor may not be visible at all. This might be acceptable in a crisis situation, but it does lead to another issue: Who decides if the radar system may be reconfigured, and under which circumstances? Is the fire brigade in charge or the police? Or perhaps the port authorities or the government? Clear policies need to be defined for this, policies that can become more complex as the sensor systems' reconfigurable functionality increases. Although the aim is to be almost instantaneously reconfigurable, initial versions of the technology will be likely to need some processing time for each reconfiguration. This can be crucial in crisis situations: during reconfiguration sensors cannot be used, leaving the control center in essence blind to the current situation. This may be acceptable if reconfiguration time is in the range of fractions of seconds, but longer delays may compromise the functionality of the technology.

All these issues stem from the same core problem: reconfigurable systems have more functionality than normal systems, but they cannot use the added functionality concurrently. One can either search for ships or for low flying planes, not both (at the same time). If different functionalities support different values, who gets to decide which value should be given priority?

3 What is reconfigurable technology?

Before we head on to discuss ethical and societal issues that we expect to come up in the development of reconfigurable sensor technology, we briefly reflect on the notion of "reconfigurable technology". It turns out this notion requires a deeper analysis.

The computer (the 'universal machine') possibly seems the most obvious example of reconfigurable technology. In his seminal paper *"What is Computer Ethics?"* [8], James Moor refers to the *logical malleability* of computers as the essence of the revolutionary character of computer technology, from which the need for a separate attention for computer ethics follows:

> *"The essence of the Computer Revolution is found in the nature of a computer itself. What is revolutionary about computers is logical malleability. Computers are logically malleable in that they can be shaped and molded to do any activity that can be characterized in terms of inputs, outputs, and connecting logical operations.*
>
> *[…] This is all I need to support my argument for the practical importance of computer ethics. In brief, the argument is as follows: The revolutionary feature of computers is their logical malleability. Logical malleability assures the enormous application of computer technology. This will bring about the Computer Revolution. During the Computer Revolution many of our human activities and social institutions will be transformed. These transformations will leave us with policy and conceptual vacuums about how to use computer technology. Such policy and conceptual vacuums are the marks of basic problems within computer ethics. Therefore, computer ethics is a field of substantial practical importance."* [8]

Here the logical malleability of computers is taken as the central cause of several effects computers will have on society, and from these effects, the need for computer ethics follows. What we would like to explore, is what ethical issues follow from the aspect of reconfigurability in itself (hence, not from the effects) in reconfigurable technology. Does reconfigurable technology ask for different types of functional and non-functional requirements? Do we need to specify meta-requirements to capture requirements on the level of the reconfiguration process?

We think it is important to distinguish flexible functionality from flexible configuration: the relationship between them deserves some more detailed study (also beyond this paper).

Literally "*reconfiguration*" means: to modify the configuration, i.e. the arrangement of the parts (of a system). The use of computers has extended functionality of sensor systems already, for example the enhancement of CCTV systems with software that processes faces and compares these to a database with known subjects in order to identify them. In a sense this extension could be described as a reconfiguration of the CCTV system, since the original functionality of the system is altered for a specific purpose. But not every alteration or extension of *functionality* is necessarily a reconfiguration. In the case of adding computers for information processing in a sensor network, this is not just a rearrangement of existing parts of the system, but *adding* elements to the system. Furthermore, reconfigurability is not essential for a piece of technology to have multiple functionality: the same piece of technology may have very different functionalities depending on how and with which intention it is used. An example of this is a plane: usually a means of transportation, but can be used as a highly destructive explosive in the hand of terrorists without any adaptations to the configuration.

Returning to the concrete background of this paper: what kind of reconfigurability can we expect within the STARS-project? The ultimate goal of the project is to develop sensors and sensor networks with as much (potential) functionality as possible. The project proposes to achieve this by making the hardware reconfigurable, which will involve mainly analogous front-ends (infrared, radar, etc.) and digital signal processing. We think the resulting range of range of possible reconfigurations will be rather limited, but as such, this will provide an interesting starting point. The system concepts and architecture have yet to be developed. Even so, methodological questions are raised by making parts of the architecture reconfigurable, such as those concerning testing procedures, software-hardware partitioning and composability (as pointed out for software architecture in [4]).

In our involvement in the STARS-project, we aim to identify specific ethical challenges related to the reconfigurability of technology, although we will also touch upon more general issues of multiple-functionality, with the goal of creating awareness and anticipating these challenges in the research and development phase of the technology. In this process, we will address the question whether *design for values* for reconfigurability related values asks for a different approach, and how *design for values* for reconfigurable technology relates to proposed approaches to the ethics of emerging technologies (like *Ethical Technology Assessment* [11] or *Anticipatory Technology Ethics* [2]).

4 Reconfigurability as a challenge for design for values

An important aspect of reconfigurability is that it challenges the type of stable, knowable, unambiguous function ascriptions to artifacts and systems. In that sense, it may ask for an extension of existing theories of technical functions. [5]

This bears on the principle of informed consent. A prerequisite of that principle is a knowable impression of what the system will do under which circumstances. One can argue that this prerequisite is hard to fulfill for many of today's (socio-technological) systems, as they are developed for a certain goal, but once in place, easily used for or combined with other functionalities. This is called *function creep*; a well known example is the use of cameras introduced to implement a road pricing system (also) for the detection of stolen cars, or tax evaders. But the issue is even more prominent if the system is *intended* to be reconfigurable to changing circumstances, and maybe even fit for yet unthought of functionalities. At what level of abstraction can the system's behaviour be specified for people subject to it, and is that enough of a basis for them to be able to consent or as a basis to justifiedly assume their consent?

The specification of the behaviour of the system requires a sophisticated and complex balancing of the different goals the different functionalities of the technology serves. Combining technology for multiple-functionality into one sensor, adds the restriction that only one functionality at a time can be actually used: as mentioned above, the functionality may not be usable concurrently. This means that more crucially than usual, priorities of the different functionalities must be assigned. This adds an extra dimension to the design process: the specification of priorities.

The observations above show that the reconfigurability leads to an increased range of choices that need to be made. These choices address not only practical aspects, but more essentially higher order choices: who will be in control of such (practical) choices? Who will bear responsibility for the different functionalities, or for the system as a whole? This indicates that the development of policies around reconfigurable systems will bring in new complexities. Such complexity may compromise the expected efficiency of reconfigurability.

A fundamental question that should be asked whether the (physical) reconfiguration of the technology is in fact essential for the issues we relate to reconfigurability. Without actually reconfiguring the technology, we can already conceive of certain technology to be used for something else. Think of a car or a plane that can be used for terrorist attacks rather than for transportation, or the use of nuclear technology for the development of weapons rather than for the generation of electricity (*dual use*). Sometimes it just takes another perspective towards the technology in order to enable different functionality. Can we distinguish between ethical issues related to the (intended) reconfiguration of technology and (unintended) (re)perception of the functionality of certain technology (without being reconfigured)?

Although the initial use case for the reconfigurable sensor networks is not primarily related to the observation of persons and their behaviour, we deem it useful to look at the ethical issue related to sensor networks like camera surveillance and RFID access control systems. There is extensive literature discussing how sensor networks for observation of individuals and their environment bring up issues concerning privacy and the protection of personal data, e.g. [3,12,6,13]. Despite the fact that the described use case for the reconfigurable sensor networks does not center around privacy, we expect that the technology may in the future be applied in privacy sensitive ways. But besides that, we argue that central notions from the discussion of privacy may be helpful in the analysis of reconfigurability.

Reconfigurability puts the context of use and control of information, captured in notions like ‘spheres of justice’/‘spheres of access’ [7,9] and ‘contextual integrity’

[1,10], even more crucially at the heart of the challenge put forward by privacy. For example, Nissenbaum understands privacy in terms of context-relative information norms, and distinguishes norms of appropriateness, and norms of distribution. She defines contexts as "*structured social settings, characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).*" Most relevant to the framework of Contextual Integrity are the roles, activities, norms and values. [10, p.132-134]. For reconfigurable systems there may be different roles, activities, norms and values that need to be combined in the design of one system. How to deal with the composition of these different contexts for one system is a particular challenge.

Reconfigurability involves applicability of one system with multiple functionality in possibly distinct contexts. In the case of reconfigurable sensor networks, the challenge will be to formulate requirements that are both general and specific enough to cover each possible use. For example, how to balance privacy issues if the sensor system monitors individuals only in very few of its configurations? And how to go about changes in this configuration?

Nissenbaum's framework for Contextual Integrity provides explanation, evaluation and prescription, and thereby contributes to the design process. However, it does not "*support substantive descriptions for general families of technologies*", and "*the most fruitful assessments take place within particular contexts*". [10, p.190] In the case of reconfigurable systems, the particular context may be underspecified, or only one of a vast number of possible contexts. Therefore, a specific challenge for design for values of reconfigurable technology, like the sensor networks, requires an analysis of the composition and interaction of different contexts.

5 Conclusion

Reconfigurability of sensors in networks seems to be an attractive answer to the increasing and unvariably changing demands in the security and crisis management domain, both in terms of economy and of effectivity. In this paper, we have presented an initial exploration of challenges reconfigurability may add in the ethical analysis of technology. In the coming years, we will develop a more thorough analysis of the concept. It will be interesting to see how reconfigurability can be analyzed from the perspective of the literature on function ascriptions and requirements engineering. Is (physical) reconfiguration essentially different from reconception of the possible use of a piece of technology (like in *dual use*)? We believe that a proper analysis and definition of context and spheres will be crucial in the 'design for values' of such technology, and essential for understanding its effect.

References

1. Ackerman, M., Darrell, T., & Weitzner, D. (2001). Privacy in context. *Human-Computer Interaction, 16*, 167-176.

2. Brey, P. (2011), *Anticipatory Ethics for New and Emerging Technologies*, Presidential address at the Society for Philosophy and Technology conference, Denton TX, USA, May 27, 2011 (https://spt2011.unt.edu/).
3. Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer, 36* (10), 103-105.
4. Guo, Y. (2006). Mapping applications to a coarse-grained reconfigurable architecture. PhD-thesis, University of Twente.
5. Houkes, W., and P.E. Vermaas (2010) Technical Functions: On the Use and Design of Artefacts, vol. 1 of *Philosophy of Engineering and Technology* (Dordrecht: Springer).
6. Hoven, J. v. (2008). Information Technology, Privacy, and the Protection of Personal Data. In J. v. Hoven, & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 301-321). Cambridge University Press.
7. Hoven, M. J. (1999). Privacy or informational injustice? In L. Pourcia (Ed.), *Ethics and information in the twenty-first century* (pp. 140-150). Purdue University Press.
8. Moore, J. (1985). What is computer ethics? *Metaphilosophy, 16(4): 266-275*. Retrieved from http://www.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html (June 16, 2011)
9. Nagenborg, M. (2009). Designing spheres of informational justice. *Ethics and Information Technology , 11* (3), 175-179.
10. Nissenbaum, H. (2010). *Privacy in Context*. Stanford University Press.
11. Palm, E. & Hansson, S.O. (2006), The case for ethical technology assessment (eTA), *Technological Forecasting and Social Change*, 73(5), 543-558.
12. Shi, E., & Perrig, A. (2004). Designing Secure Sensor Networks. *Wireless Communications, 11* (6), 38-43.
13. Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
14. STARS. (2010, July). Project Information. Retrieved from STARS-Project website: http://starsproject.nl/

Approximating user values to preserve privacy – a proposal

Sven H. Koch[1], Rumyana Proynova [2], Barbara Paech [2], Thomas Wetter [1,3]

[1] Institute of Medical Biometry and Informatics;
{Sven.Koch, Thomas.Wetter}@med.uni-heidelberg.de,
[2] Institute of Computer Science, Heidelberg University, Heidelberg, Germany
{Proynova, Paech}@informatik.uni-heidelberg.de
[3] Dept. of Biomedical and Health Informatics, U of Washington, Seattle, USA

Abstract. Users have different sets of personal values, such as benevolence, self-direction, and tradition. Among other factors, these personal values influence users' emotions, preferences, motivations, and ways of performing tasks - and hence, information needs. We sketch a method where, during software development, multiple value-dependent interface variants with different functions are created. When used the first time, personal values of the individual user are identified, and the software presents itself in the variant that best matches these values. In this paper we focus on identifying values when using software the first time. Currently used methods to identify values are work intensive and/or solicit personal user information. A method intended for routine use when a user starts using the interface, should require little effort and not intrude privacy. Instead of probing for user values directly, we propose to approximate users' personal values based on the users' preferences for work tasks and to neglect other factors influencing preferences. Questionnaires allow efficient data collection, and users have few issues sharing opinions about work. Inasmuch as this indirect querying of user values approximates underlying values, appropriate interfaces can be identified when using the software.

Keywords: personal values, elicitation, approximation, privacy, software tailoring, individualized interface

1 Introduction

Interfaces which are developed with values in mind are better suited for the user's needs, e.g. [1-4]. In general, values describe properties of the context and properties of the user. Among contextual values are ethical values, business values, quality properties of the system to be built, values of the system developers, as well as values of teams of users. Amid a user's values are his or her goals, motivation, emotions, preferences, and personal values or beliefs.

Personal values or beliefs are the concepts which guide individuals during their life and stay constant over time[5] e.g. the concepts of *benevolence*, *self-direction*, and *power*[6]. They are explained in further detail in Section 2.

Users' information needs are impacted by their specific personal values, so tailored interfaces might better support individual ways of working. Personal values influence users' goals, decisions, motivation, and preferences. Specific values therefore influence the tasks individual users see as essential to reach goals, and which information the individual user considers essential to perform these task. Tailored interfaces could show only relevant data and avoid cluttered displays which try to satisfy all information needs.

Consider the following examples of functions dependent on personal values: Imagine a physician whose personal values are predominantly *benevolent* compared to another physician who is rather guided by *power*. Both physicians would need to perform a similar set of basic tasks – however, the information they need, the way it is provided and the functions they can perform would differ according to their specific personal value. The *benevolent* physician may aim to detect a patient's problem before it becomes a threat and may want to plan the least harmful therapy personally. Possibly preferred functions for benevolence include information about the burden of treatment options on the patient and his/her quality of life, and leaving comments to coworkers to ensure continuity of treatment and prevent possible harm. The physician for whom *power* is essential might in the same situation instead want to delegate the task of treatment to co-workers and/or order procedures the patient needs to follow. Possibly preferred functions for power include adding tasks to others to-do lists and seeing their workloads.

However, it is not easy to measure personal values. Approved questionnaires are work intensive and use items that users feel concerned to answer in a work context because they are related to their private lives (Section 2). Software tailoring based on approximated personal values comes with the benefits of individualized information without the privacy concerns of directly measured values. Therefore, we propose a method to approximate personal values without users' privacy concerns.

Requirements for a method to approximate values are that it should have a low workload and a low impact on users' privacy. After determining user interface (UI) variants during development, every user would perform the method once when starting to use the software. Therefore, it should be efficient with many users by requiring low workload on UI practitioners who tailor interfaces to individual users' needs. Furthermore, a method should take into account the user's privacy related concerns. If methods don't respect privacy needs, users might plainly refuse to participate. The approximation of personal values should rely on information people are willing to talk about instead of very personal ("secret") information.

We propose to approximate values through attitudes towards work for situations where it is not feasible to directly measure personal values. Furthermore, we suggest that multiple value dependent interface variants are developed and each user, when using the software, sees the variant appropriate for his or her specific personal values.

Our research focuses on constructing a method to approximate the individual personal values of many users. In the following, we first describe what we mean by the user's personal values, and review currently used approaches to elicit user values. In the Section 3 we explain our proposal of a method to approximate user's personal values - exemplified with a case study. In the last section, we discuss possible implications and limitations of the method.

2 Background

Personal values describe an individual's basic concepts and beliefs which guide the individual through life. We center our research on the validated personal values theory of Shalom Schwartz [6]. Schwartz' value theory provides us with verified questionnaires for value measurement and specific descriptions of each value concept [5]. We expect that using this theory will make our research reproducible.

Schwartz is one of the leading researchers in psychological analysis of personal values and found that the values of individuals stay constant over time and are present in individuals of different races, nationalities, and social or cultural background.

Schwartz' personal values theory was verified through broad empirical research in many countries and individuals with a wide range of different demographics. His value system is commonly used and differentiates between ten personal values.

Table 1 lists the ten personal values which were determined by Schwartz and short descriptions for each. The Schwartz value system is based on two dimensions: 1) focus on the self or not (self-enhancement vs. self-transcendence) and 2) seeking stability or change (openness to change vs. conservation). The category self-enhancement (focus on self) includes the values *achievement*, *power* and *hedonism*, contrasted by the category self-transcendence (not-self) with the values *universalism* and *benevolence*. The category conservation (stability) has the values *security*, *tradition*, and *conformity*, contrasted by the category (openness to change) with *stimulation*, *self-direction*, and *hedonism* (which belongs to two categories).

Table 2 shows an overview of methods which are currently used or proposed to elicit user values and properties. We included requirements elicitation methods that identify properties of users outside of the very strict definitions of the Schwartz value method because we are interested in properties related to IT.

Table 1. Personal values determined by Schwartz [5, 6] and short descriptions for each.

Value	Description
Achievement	Personal success through demonstrating competence according to social standards
Benevolence	Preservation and enhancement of the welfare of people with whom one is in frequent personal contact.
Conformity	Restriction of actions, inclinations and impulses likely to accept or harm

	others and violate social norms or standards.
Hedonism	Pleasure and sensuous gratification to oneself.
Power	Social status and prestige, control and dominance over people and resources.
Security	Safety, harmony and stability of society, of relationship, and of self.
Self-direction	Independent thought and action-choosing, creating, exploring.
Stimulation	Excitement, novelty and challenge in life.
Tradition	Respect, commitment and acceptance of the customs and ideas that traditional culture or religion provide the self.
Universalism	Understanding, appreciation, tolerance and protection for the welfare of all people and for nature.

Table 2. Examples of currently used methods to approximate user values and needs, their estimated impact on privacy, and estimated workload on UI practitioners who tailor the interface to individual user, in case values for many users have to be determined.

Method	**Impact on users' privacy**	**UI practitioners workload with many users**	**Proposed or used e.g. by**
Ethnographic observation	Medium	High	[1, 4, 7, 8]
User review of scenarios and storyboards	Low	High	[1]
User evaluation of prototypes	Low	High	[1]
Discussing users' needs in the design team	Low	High	[4]
Personal informatics	Medium	High	[2]
Interviews	Medium	High	[1, 9]
Questionnaires	High	Low	[5, 10]

Dealing with privacy concerns is important to make eliciting of personal values feasible. Our rating about the impact of methods on privacy in Table 2 is based on how much personal information the user needs to reveal and how. During ethnographic observation, participants are followed by an observer who notes e.g. actions and goals. Some participants might feel they are assessed, which could result in a feeling of uneasiness concerning privacy. During user review of scenarios and storyboards, as well as when reviewing prototypes, participants' comments and feedback can be used to reveal to what extent the system reflects their values or motivation. If used correctly, these review methods should have a low impact on participants' privacy: users only share opinions. If the design team needs to discuss many users' needs this results in a high workload. When using personal informatics systems [2], participants collect personally relevant information, for the purpose of self-reflection and gaining self-knowledge about their personal values without directly talking to the developers. Interviews are time intensive and dependent on the questions require users to directly reveal private information. Users found filling questionnaire about personal values was difficult [10] – but researchers workload is low due to automated evaluation.

Our assumptions about workload on the UI practitioner in Table 2 distinguish between direct and indirect methods. Methods where direct, time intensive one-to-one contact between UI developer and user is required were assumed to have a high workload when used with many users. Questionnaires, which can be completed without UI practitioner-user contact and which can be evaluated automatically, were assumed to have a low workload.

In conclusion, a method which requires a low workload and has a low impact on user's privacy when approximating personal values of many users is currently missing. In the following, we describe our approach to approximate personal values through a low impact – low effort questionnaire presentation.

3 Method proposal

Our method to approximate users' personal values targets concepts which are influenced by the user's personal values and can be easily obtained from the user. In the following, we describe the method to approximate values based on preferences for work tasks and exemplify it with a case study.

3.1. Description of our proposed method

Values influence behavior indirectly through attitudes. While individuals are seldom aware of their values, they are aware of their attitudes and use them as rationales for decisions [11, 12]. As such, attitudes are one of the values-related concepts which can influence users' preferences and expectations about software. An attitude can be expressed as a single statement of the type "I like X" (a positive attitude) or "I don't like Y" (a negative attitude). Attitudes are formed, among other factors, based on values. For example, if the value *tradition* is very strong in a particular individual, there is a high probability that this individual has a positive attitude towards things considered traditional.

Users are rather more willing to share their attitude towards work tasks than their personal values. Although the preference for sharing personal information varies from user to user, the willingness or reluctance to reveal personal information depends on the type of information to be shared. During preliminary interviews we found users to be very reluctant to reveal personal information such as personal values. However, they were openly talking about what they liked and what they didn't like about their work and their attitude towards individual tasks.

Approximating personal values through attitudes towards work tasks might be feasible without strong privacy concerns but not as accurate as directly measuring values. Figure 1 exemplifies this relationship in a simplified conceptual model. It shows how we plan to approximate personal values based on preferences towards work tasks. Although attitudes towards work tasks are influenced by other factors, such as the nature of tasks or devices a task is performed with, we believe that attitudes allow value approximation.

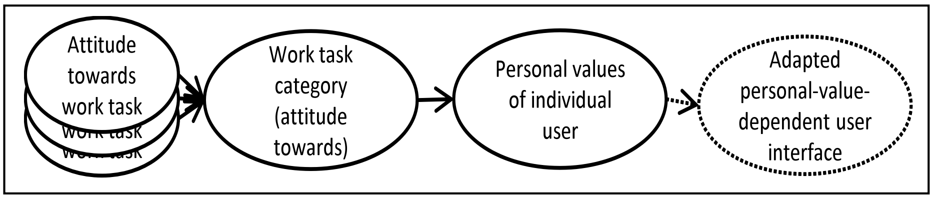

Attitude towards work task
work task
work task
Work task category (attitude towards)
Personal values of individual user
Adapted personal-value-dependent user interface

Figure 1 If during development several personal value specific interface variants were developed, then we could display the appropriate variant to each user – dependent on his/her personal values. Our method proposes to approximate users' personal values based on individual attitudes towards (work) tasks for situations where privacy concerns prevent direct value measurement.

Questionnaires suggest themselves as a method for data collection. They can be employed without personal contact between the users or software engineers and can be automatically evaluated, and are less intrusive or intimidating to users compared to revealing personal information in a one-to-one conversation.

We propose to use lists of work tasks, to ask users about their attitudes towards these tasks and to infer their personal values based on value-dependent properties of these tasks. Such task lists can be based on canonical work descriptions. For further streamlining, these tasks can be grouped in work task categories, and questionnaires can be shortened by only asking for tasks that each represent a task category. The correlation between personal values and task preferences would be determined prior to the study based on a reference model with task categories and associated values (e.g. Table 3) which we are currently developing. In the following we explain how we used our method in a case study.

3.2 Pilot study: Approximating personal values of nurses and physicians

A pilot study was conducted with a total of seven participants working at two university hospitals in Germany - three physicians and four nurses. The pilot study covered multiple aspects of our research in several parts. In this paper we report the two parts related to value approximation.

Our research question was: does our proposed method allow to select tasks or task categories appropriate for routine use? By routine use we mean that they approximate user values with enough precision to inform provision of user individualized interfaces?

The first part for personal value approximation was a list of users' work tasks which were typical for their respective professions. Our task selection included different kinds of tasks such as delegation tasks, decision support tasks, and patient centered tasks (see Table 3 for examples), and was based on medical literature and preliminary observations. Physicians received a questionnaire of 43 physician tasks, and nurses got 45 nursing tasks. For each task, participants indicated their attitude on a Likert scale ranging from 1 (strongly dislike task) to 9 (favorite task).

Table 3. Attitudes towards work task categories and associated values as examples. The table shows task categories which correlated with individual users' personal values. For each task category example tasks are given, followed by the correlated values with positive or negative correlation. For example, we found that communication tasks were liked by 2 users with the value self-direction, and 1 user with the value stimulation and 1 with hedonism.

Task category	**Example tasks**	**Personal value (attitude towards task category)**
Communication with co-workers	Ask for second opinion, ask for advice	*self-direction* (likes, 2), *stimulation* (likes), *hedonism* (likes)
Documentation	Document patient data, write a discharge letter	*self-direction* (dislikes, 2), *benevolence* (dislikes, 2)
Manual tasks	Patient examination, drug administration	*hedonism*(likes), *benevolence* (likes)

The second part of the questionnaire consisted of the Schwartz Value Survey[6], a standardized instrument for identifying personal values. The survey asked participants to assess the importance of 56 items in their life and values. Items include human properties such as successful, polite, daring, and healthy. Participants rated each item on Likert scales ranging from "This item is opposed to my personal values" … "very important to my personal values".

Response rates were 100% (physicians) and from the initially invited six nurses, only four replied (67%). We identified task categories in which individual users liked or disliked most tasks. Table 3 shows examples of the findings in our pilot study. Our participants predominantly exhibited the values *self-direction*, *benevolence*, *hedonism*, and *stimulation*. We found that a positive attitude towards communication tasks correlated with *self-direction*, *stimulation*, and *hedonism*. Documentation tasks showed a negative correlation towards *self-direction* and *benevolence*, and liking manual tasks correlated with *hedonism* and *benevolence*.

4 Discussion and Conclusion

We propose to use the attitudes towards work tasks to approximate personal values. We have applied and evaluated our method in a small scale case study, and found a correlation between attitudes towards some task categories and personal values.

Our proposed method is a compromise between workload, accuracy, and the protection of privacy: during pilot interviews, users only took 10 minutes to complete questions about attitudes towards tasks, did not have to reveal very private information, but accuracy might be limited. Therefore, our method might be more feasible in everyday situations than directly measuring values.

Limitations of the case study include the sample size being too small in order to identify significant correlations between values and tasks categories. It also was too small to allow conclusions whether the four values found in our subjects are prevailing in healthcare professionals or just a selection artifact. The validity of the questionnaires was not verified; therefore, our preliminary results might lack reliability.

Our ongoing work focuses on the correlation between values, attitudes towards tasks and software requirements [13]. We aim to create a reference model for the development of personalized value specific software requirements which shows value-task group relationships and value specific software requirements. Developers should be able to use the reference model to identify which type of information would be particularly useful for users with specific personal values. Finally, we plan to investigate the relationship between personal values and specific interface features.

Future work will aim to evaluate our proposed method and its accuracy to approximate personal values based on attitudes on a large sample of users. Furthermore, studies could explore the relationship between personal values and other soft issues. If successful, our method will make the detection of personal values easier and contribute a step towards value specific personalized interfaces.

References

1. Thew, S., Sutcliffe, A.: Value-based requirements engineering. REFSQ 2008, Barcelona (2008)
2. Detweiler, C., Pommeranz, A., Jonker, C.: Personal Informatics for Reflection on Personal Values. CHI'11 workshop on "Personal Informatics & HCI: Design, Theory, & Social Implications, Toronto (May 2011)
3. Nissenbaum, H.: Values in technical design. Encyclopedia of Science, Technology and Society, ed. by C. Mitcham, MacMillan, New York (2005)
4. Flanagan, M., Howe, D., Nissenbaum, H.: Embodying values in technology: Theory and practice. In: Hoven, J.v.d. (ed.) Information technology and moral philosophy, pp. 322-353. Cambridge University Press, Cambridge (2008)
5. Schwartz, S., Melech, G., Lehmann, A.: Extending the Cross-Cultural Validity of the Theory of Basic Human Values with a Different Method of Measurement. Journal of Cross-Cultural Psychology 32, 519-542 (2001)
6. Schwartz, S. (ed.): Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. Academic Press, San Diego (1992)
7. Ramos, I., Berry, D.M.: Is emotion relevant to requirements engineering? Requirements Engineering 10, 238-242 (2005)
8. Ramos, I., Berry, D.M., Carvalho, J.: Requirements engineering for organizational transformation. Information and Software Technology 47, 479-495 (2005)
9. Friedman, B.: Social judgments and technological innovation: Adolescents' understanding of property, privacy, and electronic information. Computers in Human Behavior 13, 327-351 (1997)
10. Pommeranz, A., Detweiler, C., Wiggers, P., Jonker, C.M.: Self-Reflection on Personal Values to support Value-Sensitive Design. In: Conference Self-Reflection on Personal Values to support Value-Sensitive Design. (Year)

11. Tesser, A., Schwarz, N. (eds.): Intraindividual process, Vol. 1. Blackwell publishers, Malden (2003)
12. Fishbein, M.: The influence of attitudes on behavior. The Handbook of Attitudes 173 (2005)
13. Proynova, R., Paech, B., Koch, S.H., Wicht, A., Wetter, T.: Investigating the influence of personal values on requirements for health care information systems. SEHC '11 Proceeding of the 3rd workshop on Software engineering in health care pp. 48-55. ACM (2011)

Exploring Norm-Critical Design in Online Youth Counseling

Sofia Lundmark[1,2], Maria Normark[1,3], Minna Räsänen[1]

[1] Södertörn University, 141 89 Huddinge, Sweden
[2] Uppsala University Box 256, 751 05 Uppsala, Sweden
[3] Mobile Life Centre, DSV, Forum 100,164 40 Kista, Sweden
sofia.lundmark, maria.normark, minna.rasanen @sh.se

Abstract. Although digital artefacts constitute a fundamental part of the contemporary lifestyle it is seldom discussed how the use of such objects affect the way we understand the world. We propose a new concept, *norm-critical design*, in which the unit of analysis is the interaction design consisting of technology, interaction, images, sounds, text and how they together construct meaning. We argue that there is a need to unpack how digital design embeds norms and to examine how the relationship between norms and design can be critically examined. We base our discussion on studies of online youth counseling.

Keywords: norm-critical design, values for youth counseling, values-in-design, critical perspectives in design

1 Introduction

A little more than a decade ago the influential book 'Sorting Things Out: Classification and Its Consequence' came out [7]. It discussed the way that classification schemes are organized and embedded into objects that gives shape to the categories that people make. An example showed a number of objects that were developed to perform these classifications of races. By embedding the classifications in objects, Bowker and Star argued that the classification became *invisible* (in the sense of taken for granted) in the standards that were developed in the arrangements for upholding a certain classification. Following this argument, we have developed a research interest during the last couple of years that we have termed *norm-critical design* (see also [15]).

The object of our research is the values and norms in the interface; the way that functions are making sense to the users and the way that e.g. navigation creates meaning. We have found that the way that the interface design presents itself to the user largely affects the way the user interpret the normative meaning of the activities that go on there. As in the examples in Bowker and Star, the implicit values embedded in the interface design is invisible in the sense that we do not think about how it structures our actions and interpretations of the online setting.

We argue that interface design create normative understandings that goes beyond the more common analysis in the HCI field of ‘usability’ or ‘aesthetics’ or ‘effectivity’. By viewing the construction of norms in interface design, we want to continue the corpus of examples that make it possible to critically examine the way that interface design provides a structural pattern that many of us come in contact with daily.

By the term norm-critical we mean to investigate the norms and normative assumptions that a certain object generates. Norms refer to the ‘normal’, the implicit expectations of what one should act, feel or experience in a certain situation. The focus of a norm-critical perspective is to make norms that affects and dominates our beliefs and values, more visible. To visualize and shed light on those norms also means to question the norms and to be able to challenge them. In a norm-critical perspective one makes the privileges visible and examine one’s own position (see [8]). The positions and relations to power are something that differ and are changeable within different contexts, For example, discussing norm-critical design quality is both a part of the designer’s agenda; the intentional norm-critical design of an artefact; and also as user experience of use, form and relevant values.

2 Theoretical Points of Departure

STS research

Norms, values and/or meaning making actions are made up of humans and other actors acting in the world. As we see it, the technology is co-constructing norms and values, both in a social context in interaction, and as inhabitants of norms and values. We also view design as a carrier of norms. According to Berg and Lie (1995) “artifacts do have gender and gender politics in the sense that they are designed and used in gendered contexts” [5].

Technology and digital artefacts are developed and constructed in social and cultural contexts [4]. This, from a social constructivism perspective that has a focus on how social forces influences the invention of new technologies. Even though, when bringing societal and culture structures into the understanding of the design of technology and digital artefacts/spaces, the process becomes more then the design of the specific artefact/space (see [16], [17]).

Technology creates rules and possibilities from the terms of production, which in turn leads to the impact of use, and the possibilities provided to, and created by, the users. This is of importance in relation to norm-critical design processes. Barad’s [1] concept of ”agential intra-actions”, critize the dualism between human and for example technology. Human action is inseparable from the context of the culture and the technology. Agency is intertwined and something that is created in-between human actions and technological artifacts. The users are often active intentional agents in their inter- and intra-actions within different digital environments and/or arenas, and not at least in relation to the digital technology. Moser [13] use Haraway’s notion of *interference* to create a bridge between how differences are made, interacted, and come to matter in people's lives and how science, medicine, and technologies are involved and parts in such processes. Interference was used to create a metaphor for critical notions of academic work and it was argued that realities are not given, but rather created in material practices and locations. The practices are to be seen as reflexive, critical and enacted versions of the reality that interfere. "They are "in action", in the "belly of the beast" [13]. Moser claims that this perspective can show how realities and interpretations emerge and are effects of relations that go beyond the traditional interest of semiotic approaches. This way of exploring materials, practices, technology and artefacts also goes beyond the studies of traditional texts and discourses. The focus is rather how objects, interpretations and social orders are made, emerged and sustained in relation to their materialities and how these come to matter [13]. This perspective can be a starting point in relation to norm-critical perspectives of design and design processes.

Critical perspectives in HCI

Critical theory and critical perspectives is often used as term to include a number of terms and fields and has traditionally aimed to understand, explicate, evaluate and critique cultural phenomena [6]. In many design disciplines a critical frame of reference is present in the interplay between the creative practice and the critical perspectives. Critical approaches have accordingly to some extent been developed in HCI and design research and it has become more important in HCI to become more concerned with critical theory (see [6]). Some of these critical perspectives are the Value Sensitive Design ([10]; [11]; [14]), Interaction criticism framework (that is suggested in e.g. [2] and [9]), research on Reflective and critical HCI (see [6]; [9]) or Reflective Design (see e.g. [18]) and research on Aesthetics [2]. Other interesting critical perspectives on artifacts are perspectives and research by [20] and by [7]. Previous research has argued for an expert perspective that critically examines the qualities of the interaction design and the way the design is modelled to fit its context. The purpose of this activity is to contribute to a corpus and knowledge of what is good interaction design. [9] suggests that there are three programs or concerns for how digital artefacts can be critically examined.

3. Case studies: online youth counseling

The national Swedish web-based youth counselling, umo.se (umo), propose is to make it easier for young people in the ages 13-25 to find relevant, updated and quality assured information about sex, health and relationships. Obviously, this movement from communication with a real person, either face-to-face at the healthcare centre or through telephone services, towards more generic self-diagnosing and information acquirement raises a large number of questions. Besides from different user experiences, there are a number of issues related to power and emancipation as well as the medical consequences. Design in the healthcare genre therefore, we argue, requires a specific rhetoric and/or approach. Responding to the users' expectations on trustworthiness and reliable information is guiding the umo design. It is not unexpected that the concept of norm-critical design is highly relevant and studied in the context of healthcare information services, though these are one of the fields that have to deal with questions about equality, emancipation, diversity and empowerment.

Umo.se work with this ambition in different ways during the work process of the content and the development of the site. Norms are questioned, discussed and debated through the whole working process with the site and throughout the content of the whole site. Regarding content umo.se use quality assurance processes that involves different examinations; the external expert fact-reviewers, the umo.se editorial board, the medical director and an editorial board consisting of people representing youth clinics and experts on human rights and discrimination.

At the umo editorial board, being critical towards norms means:

- Avoid reproducing norms and also question norms and standards.
- To show both people and groups of people that can be placed within and outside the norms. This inclusion is intended to be without focusing on problems or discrepancies.
- Address differences in conditions for different people or groups where they are relevant.
- Always has a human rights perspective.
- Actively promote equality through a respectful attitude towards the target group.
- To allow other types of sources and knowledge than the traditional scientific ones, such as personal experiences and everyday knowledge to be visible.
- Invite users to engage and submit comments and criticism on the content and the design of the site.

On the umo site, the content is based on factual information that aims to be visible all through the site and the material. The texts are often short and with everyday language. The information is also visible through images, illustrations, movies and other visuals to include as many users as possible. Text, images and illustrations have a shared design and approach to attract users. The website has a lot of functions where the user can interact with the content, through games, questionnaires, slideshows, moving images, “Ask Umo”, etc. The design and layout of the images and illustrations are cartoon-like; distinct and colourful. These features and ambitions aim to have an inclusive approach. The material should be easy to access and possible to use in several different ways. The website and the material that umo.se provide is also developed to be able to use for different users and in different ways, for example for young people, educators, youth clinics etc.

Umo.se has defined five different areas that they especially aim to work with from a norm-critical perspective. The five different areas are: content, information structure and interaction design, external communication, co-operations and the working force. With information structure and interaction design umo aim for prioritizing of subjects, how the users are expected to search and find their way on the site etc. The external communication illustrates whom umo.se chooses to communicate with, in which way, where and how the information is visible. Also co-operations includes who umo.se choose to work with, who they hire for assignments, who’s knowledge and who’s perspective that is prioritized etc. The staff at umo.se consists of persons who have an awareness about issues like different groups' superior power and others lack of it, in order to be able to fulfil the above engagements. Umo.se also have an ambition to show transparency by encouraging users to help developing the site by submitting comments and criticisms about the contents of the site.

Reflections on norm-critical design work

In our analysis we have explored what design elements that contributes to the message in the design work at umo. We have also analyzed how the elements interplay to create the intended effect. Two important documents are *the image policy* and *the text policy* that is used. Quality in these two policies is highly focused on empowerment, equality and emancipation. Understanding what design quality means in this context is closely related to understanding what message the designers/editors want to convey. Drawing on the observations we made during the study at umo.se, we have made an initial organization of the different aspects of norm-critical elements in four categories:

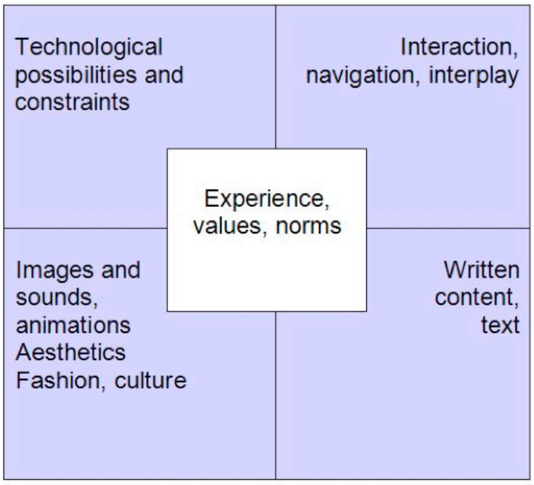

Technological possibilities and constraints
Interaction, navigation, interplay
Experience, values, norms
Images and sounds, animations Aesthetics Fashion, culture
Written content, text

Figure 1: ***Unpacking norm-critical design elements***

It is a rough division of elements but our main point here is that they all constitute and affect the norm-critical design. All four needs to be considered to unpack how normative meaning is embedded. The focus in the design process at umo is on the experience of the web site. The central intention is to design an experience that is value sensitive and norm-critical. In order to design the intended consistent message, umo uses a number of documents that states the requirements and restrictions in the design work. It is not only norm-critical aspects that are stated, there should also be a consistent "umo-style" (colours, fonts, etc.). The two policy documents (text and image policies) are important. This way of organizing what constitutes the general message is probably inherited from other older media forms. But there are also interaction possibilities and navigation, as well as technological constraints that affect the message. In this sense, texts and images should not be treated in isolation, because it is likely to weaken the intended norm-critical effect.

4. Conclusions

Critical perspectives are emerging in HCI research. Although digital artefacts constitute a fundamental part of the contemporary lifestyle it is seldom discussed how the use of such objects affect the way we understand the world. We propose a new concept, *norm-critical design*, in which the unit of analysis is the interaction design consisting of technology, interaction, images, sounds, text and how they together construct meaning. We argue that there is a need to unpack how digital design embeds norms and to examine how the relationship between norms and design can be critically examined. Based on our studies of the role of norms in design we argue that

- Digital design is not a neutral platform: digital design reformulates norms and power perspectives; the way that interaction, navigation, text, images, etc. interplay is manifesting norms.
- The design/form/*gestalt* affect the message, shape the understanding and creates normative expectations of how to act and interpret the digital context.

5. References

1. Barad, Karen (2007) Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning. Durham: Duke University Press.

2. Bardzell, J., & Bardzell, S. (2010) “Interaction Criticism: Three Readings of an Interaction Design, and What they Get Us” In Interactions, March+April 2010

3. Bardzell, Shaowen (2010) “Feminist HCI: Taking Stock and Outlining an Agenda for Design” Paper presented in CHI 2010: HCI For All, April 10–15, 2010, Atlanta, GA, USA

4. Baym, Nancy K. (2010) *Personal Connections in a Digital Age*. Polity Press.

5. Berg, Anne-Jorunn & Lie, Merete (1995) Feminism and Constructivism: Do Artifacts Have Gender? *Science, Technology, & Human Values*, Vol. 20, No. 3, Special Issue: Feminist and Constructivist Perspectives on New Technology, (Summer, 1995), pp. 332-351

6. Blythe, Mark, Bardzell, Jeffrey, Bardzell, Shaowen, Blackwell, Alan (2007) “Critical Issues in Interaction Design” BCS-HCI '08 Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 2

7. Bowker, G., Star, S. L. (2000) ”Sorting things out: Classification and Its Consequences”, The MIT Press.

8. Bromseth, Janne & Darj, Frida (ed.) (2010) Normkritisk pedagogik. Makt lärande och strategier för förändring. Uppsala: Centrum för genusvetenskap.

9. Dourish, P. (2007) “Seeing Like an Interface”, Paper presented at OzCHI 2007, Adelaide, Australia

10. Friedman, B. (1996) *Value-Sensitive Design* In Interactions, Vol 3 Issue 6

11. Le Dantec, C. A., Poole, E. S. & Wyche, S. P. (2009) Values as Lived Experience: Evolving Value Sensitive Design in Support of Value Discovery. In the proceedings of CHI 2009

12. Lundmark, Sofia & Normark, Maria (work in progress) “Digital Arenas for Intra-Active Performances: On doing Gender Online”

13. Moser, Ingunn (2006) ”Sociotechnical Practices and Difference: On the Interferences Between Disability, Gender and Class” In: Science, Technology & Human Values, Sep 2006; vol. 31: pp. 537 - 564

14. Nathan, L. P., Friedman, B., Klasnja, P., Kane, S. K., Miller, J. K. (2008) Envisioning Systemic Effects on Persons and Society Throughout Interactive System Design. In the proceedings of DIS 2008, Cape Town, South Africa.

15. Normark, Maria & Lundmark, Sofia (2011; work-in-progress) “Experiences of Norm-Critical Design”

16. Satchell, Christine (2008) ”Cultural Theory and Design: Identifying Trends by Looking at the Action in the Periphery” In: *Interactions* November + December 2008

17. Sefyrin, Johanna (2010) “Entanglements of Participation, Gender, Power and Knowledge in IT Design” Proceedings of the 11th Biennial Participatory Design Conference ACM New York, NY, USA ©2010

18. Sengers, P., Boehner, K., David, S., Kaye, J. (2005) ”Reflective Design” Paper presented at the Critical Computing Conference, Aarhus, Denmark

19. Stokoe, Elisabeth (2006) ”Analyzing gender categories in action: Feminism, etnomethodology and membership categorization analysis”. In: Sociological Review, 54(3): 467-494

20. Suchman, Lucy (2007) Human-Machine Reconfigurations Plans and Situated Actions, 2nd Edition. Cambridge: University Press

Designing and Evaluating for Trust: A Perspective from the New Practitioners

Aisling Ann O'Kane [1], Christian Detweiler [2], Alina Pommeranz [2]

[1] Royal Institute of Technology, Forum 105, 164 40 Kista, Sweden
aisling@kth.se
[2] Delft Technical University, Mekelweg 4, 2628 CD Delft, The Netherlands.
{c.deweiler, a.pommeranz}@tudelft.nl

Abstract. Trust as a factor in the design of interactive technologies is a relatively new research subject, and this paper provides the perspective from new interaction designers and developers on their views and experience with the use of trust in the design and evaluation of technology. A survey was sent out and answered by participants in their early careers and education as interaction designers and developers about designing and evaluating trust in technology. The results show that overall, the new practitioners queried believed that designing for trust is important, but in their experience it is not accounted for adequately in practice. The survey also showed that qualitative methods were the most popular to identify trust issues in new technology, but perhaps the concept of trust as used for the design of interactive systems is still very new.

1 Introduction

There is an emerging trend in Human Computer Interaction (HCI) and Human Factors Engineering (HFE) research to accept that new complex systems will never be perfect. In the HCI community, researchers such as Stewart and Williams [1] believe that the trend towards domestication and user-led creation of technologies originates from the unlikelihood that designers can entirely match user needs. In addition, new technologies are becoming more complex in the HFE domain, not allowing for comprehensive testing of all components particularly for finding interaction issues according to Parasuraman [2]. Although designers can strive for perfection and engineers try to design for complete reliability, "there will always be a set of conditions under which the automation will reach an incorrect decision" [2, p. 293]. Trust in technology is important not only for system efficiency and user experience, but designing for trust comes with ethical concerns for designers as well.

These are important considerations for the design of interactive systems, regardless of the type of system. According to Lee and See, trust has been linked to people's reliance and adoption of technology and "trust plays a critical role in people's ability to accommodate the cognitive complexity and uncertainty that accompanies the move away from highly structured organizations and simple technology" [3, p. 52].

As the study of trust in relation to technology is a new trend, it is of interest to see how new practitioners of interaction design view the importance of user trust in interactive technology and how they evaluate for trust issues with technology. This paper gives background on the research involving trust in technology, details the survey filled out by new practitioners, presents the results and analysis of the responses, and provides some discussion around trust in interactive technology design.

2 Background

In the HFE domain, Lee and See's [3] oft cited “Trust in Automation: Designing for Appropriate Reliance” presents substantial evidence pointing to the connection between trust and people’s reliance on technology. They also suggest the similarities between the factors that influence both human-human and human-automation relationships, and they define trust, a social psychological concept, as an attitude that an agent will help achieve a person's goals, and that agent could be the automation. It is a very important concept when related to automation as it influences their adoption and reliance on it: “people tend to rely on automation they trust and tend to reject automation they do not” [3, p. 51]. Corritore [4] argues that in order to be trusted, computers or technology do not need to be shown as moral agents capable of acting with reference to right and wrong, but rather being portrayed as social actors will suffice. People can enter into relationships with technology and respond to them according to rules that apply in trusting social relationships, as technology has a social presence.

In the HCI domain, Experience-Oriented and Value Sensitive Design are emerging trends. To design for experience is important for the success of the design, as it needs to be useful in a person's life and McCarthy and Wright [5] stress that feelings, cultures and values must be designed for. This view aligns with Value Sensitive Design, a framework where the resulting technology accounts for human values in a principled and comprehensive manner [7]. Friedman, Kahn, and Borning [6] in their VSD overview conclude trust “refers to expectations that exist between people who can experience good will, extend good will toward others, feel vulnerable, and experience betrayal” [p. 17]. The methodology for exploring human values such as trust through VSD consists of conceptual, empirical, and technical investigations that are performed iteratively and integrated throughout the design process. Friedman, Kahn, and Borning caution the ethics involves in this type of design because “unlike with people with whom we can disagree about values, we cannot easily negotiate with the technology. Although inattention to moral values in any enterprise is disturbing, it is particularly so in the design of computer technology” [p. 21].

Beyond HCI and HFE, research on trust can be found in a variety of literature, spanning the fields of philosophy, sociology, psychology, management, marketing, ergonomics, industrial psychology and electronic commerce [4]. Looking at the variety of fields, it is no surprise that “as a result of both the range of disciplinary lenses used to study trust and the inherent ambiguity of the trust construct, there is currently a confusing assortment of conceptual perspectives on trust” [8, p. 143]. In summary, trust involves aspects of expectation, vulnerability, and risk regarding the likelihood of a favourable response, but this is not easily articulated. Trust is an attitude towards something and that experience is something that can be hard to describe, let alone design for.

Although definitions of trust can vary significantly between disciplines, and between people in general, the emerging trends in HCI and HFE research show the importance of trust in technology and this research should influence the new generation of interaction designers and developers. Given these new trends in trust research from the HCI and HFE domains, it is of interest to see how new practitioners view the importance of trust in the design of technology and how they identify trust issues through different evaluation strategies.

2 Method

A Google Docs form was piloted with 6 test users before the link to the survey was sent through Facebook to 57 personal contacts known to have experience in the HFE or HCI domain in Canada, Sweden, and the Netherlands. The message introduced the survey as a way to gain perspective on design practices around trust, and invited those who had experience as interaction designers or developers to fill it out and spread it to their respective interaction design networks. Although the use of personal contacts and introducing the survey as a means to investigate designing for trust introduced bias into the results as personal relationships and intrinsic interest in the topic of trust would effect response rate, the survey was merely a means of probing practices of new HCI and HFE practitioners so the results were not meant to be statistically significant.

The aim of the survey was to compare new practitioners' perceived importance of trust versus their actual experience of accounting for trust in interaction design, and also to compare the popularity of different evaluation techniques for finding trust issues. The first two statements aim to shed light on if the participants have found trust issues to be important in their past work experience and if they believe that user trust is important. The third and forth statements aim to shed light on if trust issues have been raised in their design experience and if they believe that trust should be brought into the design process. The last three questions aim to shed light on which evaluation methodologies are the most popular for finding trust issues. These statements were piloted with 6 participants and the language was modified slightly before the survey was sent to the large sample.

The first seven statements were based on participants' level of agreement on a seven point Likert scale which ranged from low agreement 1 ('not at all') to high agreement 7 ('very much'). The last item was an open ended question which welcomed general comments on the design and evaluation of trust.

In addition, further statements on the connections between affective experience and trust were queried, but the above statements on designing and evaluating for trust are the focus of this paper.

4 Results and Analysis

Of the 57 new practitioners contacted and not including the six test pilots of the survey, 20 participants (14 male) responded. As listed in Table 1 below, the average age was just under 26.5 (median = 26, mode = 26) with respondents ranging from 24 to 32 and their self-identified nationalities showed 11 of the participants identified themselves as from Europe, 5 were from Asia, and 3 were from North America. With regards to education, 7 had achieved their Bachelor's degree, 10 had received a Master's degree, and 3 were at a Post-Graduate level. Regarding work experience, the average experience obtained was just over 3.2 years (median = 3, mode = 3). Although they split on whether they considered themselves a technical designer (9 participants) or an interaction designer (10 participants) with one business analyst, their descriptions of a typical role they would play in a project showed that most had experience in various aspects of technology design. When asked about a typical design projects they were involved in, Human Factors Engineering and Human Computer Interaction domains were mentioned with roles ranging from interaction design research to nuclear safety consulting.

Table 1. Demographic information for the surveyed participants

	Gender	Age	Nationality	Education	Experience
P1	Male	27	German	Bachelor	Interaction Design
P2	Female	25	Kosovar Albanian	Master	Technical Design
P3	Male	24	Pakistani	Master	Interaction Design
P4	Male	28	Mexican	Master	Technical Design
P5	Female	24	U.S.	Bachelor	Interaction Design
P6	Male	26	Greek	Bachelor	Technical Design
P7	Male	25	Italian	Master	Technical Design
P8	Female	28	Iranian	Master	Interaction Design
P9	Female	26	Greek	Master	Technical Design
P10	Female	28	Korean	Bachelor	Interaction Design
P11	Male	26	Canadian	Bachelor	Technical Design
P12	Male	32	Swedish	Master	Technical Design
P13	Male	25	Bulgarian	Master	Technical Design
P14	Male	25	Turkish	Master	Technical Design
P15	Male	26	Greek	Bachelor	Interaction Design
P16	Male	25	Belgian	Master	Interaction Design
P17	Female	28	Nepalese	Post-Grad	Interaction Design
P18	Male	28	Greek	Post-Grad	Interaction Design
P19	Male	26	Canadian-Chinese	Bachelor	Business Analyst
P20	Male	27	Spanish	Post-Grad	Interaction Design

Although statistical analysis of a small sample size with a biased response rate will not be very accurate, Wilcoxon Signed-Rank Tests were conducted to show any statistical differences between the statements. This analysis showed significant statistical differences between S1 and S2 (Z=-3.220, P=0.001), between S3 and S4 (Z=-3.845, P=0.000), between S5 and S6 (Z=-2.506, P=0.012), and between S6 and S7 (Z=-2.209, P=0.027).

Table 2. Statement agreement averages and standard deviations

Statement	Mean	Std Dev
S1. In my past work experience, user trust issues have influenced user acceptance of the design.	4.85	1.496
S2. I believe user trust in the system is a crucial part of its acceptance.	6.00	1.076
S3. In my past work experience, user trust is discussed and accounted for in the design process.	3.90	1.373
S4. Ideally, user trust in the system should be discussed and accounted for during the design process.	6.10	0.788
S5. In my past work experience, personally testing the system or having the design team test the system has pinpointed issues with trust in the design.	4.55	1.468
S6. In my past work experience, having users test the system and conducting interviews, observations, and other qualitative measures have pinpointed issues with trust in the design.	5.55	1.638
S7. In my past work experience, having users test the system and collecting error rates, questionnaires, and other quantitative measures have pinpointed issues with trust in the design.	4.70	1.625

The first four statements' averages point to the differences between the participants' opinions on the importance of trust in the design of interactive systems versus their past work experience as interaction designers and developers. Although these new practitioners believe user trust is a crucial part of interactive technology's acceptance (S2), fewer have seen the result of this in practice (S1). Also, the participants believed that user trust ideally should be accounted for and discussed (S4), but found that in their past work experience it was not as highly regarded during the design process (S3). P12 works in software design and implementation and explains that “'Trust' has never been explicitly addressed in any work I've done before, neither by me or others”. P7 explains his experience in web design as such: “In my experience there hasn't been as much attention on user's trust as on user's satisfaction [...] More attention and stress on trust might and should be put in other areas, which for instance require a more complicated and [thorough] design process, or a closer user interaction, etc”. There is a high positive correlation (0.683) between the participants who agreed with the two belief questions (S2 and S4) about trust's importance in user acceptance of technology and its importance in the design process for interactive technology.

The statements about evaluation methods used in the participants’ design experiences (S5, S6, and S7) did not show strong results, but did point to qualitative methods as being the most popular to test trust issues. P5 mentions that she tends to use qualitative methods, but “Theoretically, I think experts can do a decent job of finding trust issues if they have a lot of experience in designing certain systems. Choice of users is also very influential, because some are more adept with technology than others. (So a perceptive expert review could give more than a tech-savvy user.)”. Many participants chose the neutral level of agreement, indicating no agreement nor disagreement. This could be caused by the lack of attention on trust during the design process mentioned above, and therefore they did not have experience with using any evaluation methods for finding trust issues.

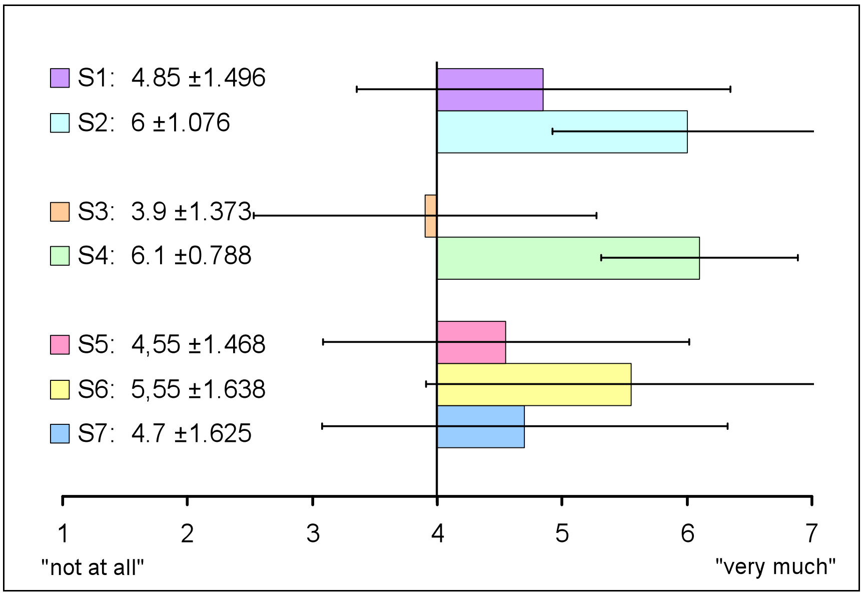


Fig. 1. Statement averages shown graphically with error bars representing standard deviation.

The neutral level of agreement to the survey statements by participants may have also be caused by the ambiguity of the trust construct itself. In the design of this survey, no definitions of trust were made nor was there any reference to trust literature for participants that have not been exposed to this research. P12 made reference to this lack of direction in the survey: “Before taking this [survey], there should probably have been a definition of what 'trust' and 'user trust' etc is, my feeling for what it is doesn't really feel like it fits in the questions above”. P13 also suggested that the design of the survey should have included definitions of trust.

5 Discussion

Despite the lack of experience in designing for trust, participants generally agreed that trust is an important concept in interaction design and development. Although many of the participants may not have thought about trust as related to the way users accept the technology they design, they have a general concept that it should be accounted for in the design process. These results perhaps do not point to HCI and HFE trust literature filtering down to the new practitioners, but could point to a general understanding of trust as a social issue that effects technology that has a social presence, as per Corritore [4] mentioned above. The participants could have been keeping the “enduring human value of trust” [7, p. 40] in their minds during the design processes that they have been involved with without explicitly mentioning the term trust: essentially conducting value conscious design, without knowing or using the framework of Value Sensitive Design to describe their activities.

The lack of experience evaluating for trust is clear from the results of this survey. But even with the very neutral results of the evaluation statements, the participants still indicated that qualitative methods of user evaluation were the most popular for potentially identifying trust issues with the design. Perhaps because of the lack of experience with using the word trust explicitly during their experiences in design, they may have been evaluating for issues with user trust in their system without actually calling it such. Much like evaluation follows design in the interactive technology design process, perhaps evaluating for trust will follow a trend towards designing for trust.

The word trust is something that is basically understood by anyone, but is very hard to define for everyone. Trust is a hard concept to define and definitions not only vary between disciplines, but also between people. This is apparent in the results of this survey about designing and evaluating for trust in the interaction design process through the neutral results as well as feedback about the survey. This perhaps points to trust not being brought up in these new practitioners' education or practical experience. This might be the result of the recent trust research in the HCI and HFE disciplines not reaching them yet in education or experience, or perhaps designing for trust has not been prioritized.

6 Conclusion

The results of this survey show that new practitioners of interaction design and development believe that user trust is an important concept to discuss and include in the design process, but they have not seen this type of focus on user trust in their experience. The neutral answers to questions point to this lack of experience in designing and evaluating for trust, and therefore lack of focus on designing for trust in their education and professional experience. Their neutral answers also show the new practitioners were unsure of what was meant by "trust" or "user trust", perhaps because they have never experienced these words being linked to design or technology, but rather human relationships. Although this survey shows that there is not a lot of familiarity with designing and evaluating for trust among the new practitioners, the results show the potential for a shift towards accounting for trust in future design processes of interactive systems.

As technologies become more and more complex, the relationships between these technologies and their users will change. The complexities seen in autonomous and adaptive systems will push our relationships with these technologies closer to social human-human relationships, and just as human relationships are not perfect, technology will not be perfect. It is up to designers from all fields to account for user trust in an ethical manner, balancing designing to promote trust without engendering over trust in a system.

Trust is an important concept when it comes to the adoption and reliance on technology, and even one breach of trust can highly influence user perception of that technology. It will become increasingly important to account for trust in the design process of interactive systems and this is seen in recent research in both the HCI and HFE domains. As this survey shows, the existing research on trust from both the HCI and HFE fields trickling down to interaction design education and professional practice is too slow. Design for trust should be emphasized in interaction designers' education and work experience, and frameworks such as Value Sensitive Design and other methods that take trust into account should be further disseminated in both the HCI and HFE communities.

References

1. Stewart, J., Williams R.: "The Wrong Trousers? Beyond the Design Fallacy: Social Learning and the User". In: User involvement in innovation processes. Strategies and limitations from a socio-technical perspective. Profil-Verlag, Munich (2005).
2. Parasuraman, R., Sheridan, T.B., Wickens, C.D.: A model for types and levels of human interaction with automation. In: IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 30, no. 3, pp. 286-297 (2000).
3. Lee, J.D., See, K.A.: Trust in Automation: Designing for Appropriate Reliance. In: Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 46, no. 1, pp. 50 (2004).
4. Corritore, C.L., Kracher, B., Wiedenbeck, S.: On-line trust: concepts, evolving themes, a model. In: International Journal of Human-Computer Studies, vol. 58, no. 6, pp. 737-758 (2003).
5. McCarthy, J., Wright, P.: Technology as Experience. The MIT Press, Cambridge, (2004).
6. Friedman, B., Khan Jr, P.H., Borning, A.: Value Sensitive Design and Information Systems. In: Human-Computer Interaction in Management Information Systems: Foundations, vol. 6, pp. 348-372 (2006).
7. Friedman, B., Khan Jr, P.H., Howe, D.C.: Trust Online. In: Communications of the ACM, vol. 43, no. 12, pp. 34-40 (2000).
8. Zaheer, A., McEvily, B., Perrone, V.: Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. In: Organization Science, vol. 9, no. 2, pp. 141-159 (1998).

Experiencing mobility data

Pedro Sanches[1], Markus Bylund [1]

[1]SICS, Box 1263,SE-164 29 Kista, Sweden
{sanches, bylund}@sics.se

Abstract. Mobility data, collected during normal functioning of mobile networks, is to most phone users an abstract and invisible entity. In this position paper, we describe our method based on research through design, for involving users when designing with that intangible data. Our goal is to explore the design space of applications that can emerge if this data is made public and engage users in a process of grounded discovery of societal and ethical consequences.

Keywords: Probe, research through design, mobility data, tracking

1 Introduction

Location based services are increasingly common in today's developed societies. Thousands of smartphone applications take advantage of the users' location data to recommend restaurants, forecast traffic congestions, or locate friends. Existing popular location based social networks, such as Gowalla, Foursquare and Facebook Places, use a "check-in" system, that allows users to tag places where they are at the moment, and share it with groups of friends. As more people get access to Internet through their phones, the amount of data collected in these handsets will likely increase rapidly in the near future.

But even before access to Internet through cell phones, handsets already had to communicate with nearby cell towers to make the telephony service possible. At the moment, there is a wealth of mobility data safely stored behind the firewalls of each cell phone provider, for each customer. Every time the phone is switched on, the nearest cell tower is logged in the provider's data center. Also, each phone is requested by the protocol to update their location in the network at a set time interval, or whenever it changes a pre-defined location area. Whenever a call is active, the network knows exactly which cell tower is to take responsibility for that call, in order to provide roaming – otherwise, it would not be possible to place a call while on the move.

The data generated in the network is, in most cases, not being stored for anything else than for operational purposes. Recently, however, operators started to realize the potential of the data they have been storing. The Japanese Docomo has recently announced a project [3] where it would use aggregated mobility data from their cell phone customers in Tokyo for purposes of urban planning and earthquake preparation. Also, companies like SkyHook [15] have started their own mobility mining projects, relying on their own sets of anonymized data, for research and marketing purposes.

We are at the brink of a major shift in how communication mobility data is handled. The quality of the first systems making use of data of this kind will likely drive public acceptance of future systems and influence restrictions and legislations on how this data is to be used – see the recent case of Apple secretly storing a positioning log file in the device of each user and how will that likely influence laws dealing with positioning data [2]. At the moment, there is an open design space for systems of this kind and we, as designers of new technology, have the opportunity to map the ethical and societal consequences of using this data, engage users in ideation and co-creation of new systems and services and negotiate relationships between stakeholders.

Privacy and more

Location privacy has been appointed as one of the future main concerns for law and policy makers. Especially in the case of mobile network data, where the data already exists and is heavily regulated, there will be a need for new laws if this data is to be released for a purpose that was not originally intended for. There is a concern that disclosing location to strangers and third parties, especially if combined with diverse other sources of personal information, can pose a threat risk for citizens, consumers and society as a whole because of its implications for security, personal integrity and freedom. But privacy is far from a simple concept and there are several stances one can take.

The surveillance model, present in Foucault's work [17], has been the most dominant discourse about privacy in the new media field. It is very useful in describing how power can be exerted over a subject under a constant state of observation. The observed subject internalizes the relentless surveillance by a hidden observer, ending up reducing herself as a political entity, with reduced free action. This model has produced many dystopian visions of future society. One of the most notable is Dobson and Fisher's "geoslavery" concept [18], which describes a sophisticated form of slavery where a master can track the whereabouts of a slave using current state-of-the-art positioning technology.

As the surveillance model tends to assign a negative connotation to all data gathering activities, Agres has proposed another model, the capture model [23]. Unlike the surveillance model which assumes, at its extreme, a centralized all-knowing entity, the capture model contributes with a more dynamic view on the dialogue between development of new technology and its acceptance by society. It acknowledges that distributed computer systems still potentially have the capability of establishing a regime of total visibility over human activities but that does not need to be viewed as utopian or anti-utopian. The capture model is more in line with the recent trend of wearable sensors and the rise of self-monitoring tools [7] as well as tools for parental monitoring over their children. As surveillance technology is developed, and as it is incorporated and accepted into our everyday lives, it slowly changes social norms and people adapt – cope or react - to those systems.

Besides privacy of location data, one can have other ethical concerns on the use and application of network mobility data. Simply by having a crude idea of how a large group of individuals move - without necessarily invading personal privacy by getting to the identity of the individuals – one could potentially enable more effective exertion of crowd control, if the data was to be used for that purpose [18]. Also, since public infrastructure planning is one of the possible applications of this information – as in Docomo's project - one must also consider how the system can introduce bias on that planning, by disregarding users who have chosen to opt out of the data collection, or simply were given no means to participate in it.

Our goal is to contribute to the ongoing dialogue between social norms and introduction of new technology. In the case we describe in this paper, we want to discuss with mobile phone users about the possibilities and consequences of using network mobility data. However, we are left with a problem of engaging users. A generalized dystopic surveillance critique makes the current public debate about privacy, or the limits for what is right or wrong in respect to data, quite polarized. Typically it boils down to either "if you have nothing to hide you have nothing to fear" or "the rapid development in information or communicating technology is creating an Orwellian society". We argue that the debate is in urgent need of more nuances in order to guide policy makers and designers of new technology. For that, we need methods and tools to engage users in novel ways. Our stance on surveillance technology and pervasive data collection is, rather than critical, exploratory. Our interest is to define ethical limits and opportunities for design of new systems or services that might use mobile network data in the near future.

2 Engaging users with the pervasive data collection landscape

The first problem with engaging users with the mobile network data is that this data is already being collected invisibly in the existing infrastructure of mobile network providers. This invisibility of the infrastructure may cause problems with users understanding its complexity and appropriating it, as pointed by Chalmers [10], which can in turn limit the responses and the engagement of the users when confronted with it. Added to this is the commonly observed mismatch between a high level of moral concern with privacy stated by users in polls, and the actual measures taken by users to ensure and protect their personal data – a phenomenon known as privacy paradox [19]. For these reasons, in order to obtain rich and grounded feedback from users, we have opted not to do any polls, questionnaires or scenarios and instead adopt a research through design approach, where the research will mainly be driven by design artifacts.

Zimmerman introduced research through design [20] as an approach that follows a process of design inquiry – i.e. designing artifacts - where the goal is production of knowledge, rather than obtaining commercially successful products. In his words, the goal is to:

"…make prototypes, products, and models to codify their understanding of a particular situation and to provide a concrete framing of the problem […] Design researchers can explore new materials and actively participate in intentionally constructing the future, in the form of disciplined imagination, instead of limiting their research to an analysis of the present and the past."[20]

In the case presented here, our goal is to bring up the mobility data into the attention of the users, making them experience it, rather than conceptualizing it as an abstract entity stored away in a distant database. As such, we will build on our own previous work [9,16] where we have developed systems intended to provoke users into reflecting on the consequences of technology. We are inspired by the work of Paulos with sustainability [6], where he and his team have designed critical artifacts that enable users to hold energy in their hands – such as a Light Jar, that stores solar light and releases it as a glowing light when the lid is open – in order to explore how making energy tangible, visible and limited would change would change users' attitudes towards it. Also inspiring is the work of Petra Sundström [5] with an exploration of the physical properties of intangible digital material – such as the Bluetooth protocol. Sundström's method allows multi-disciplinary design teams to get acquainted with properties of a material by engaging playfully with artifacts designed to expose those properties. Likewise, the prototyping approach of Lim [8] puts do-it-yourself user friendly sensor kits in the homes of users and lets them explore the properties and potential of ubiquitous computing, allowing users to design their own systems at home by combining sensors.

3 Artifacts

Our approach to research through design will make use of two kinds of artifacts: 1) a package of open-ended materials called Cultural Probe [21] and 2) our artifact for mobility data. Cultural Probes consists of packages of various objects such as disposable cameras, maps, postcards, diaries and scrapbooks. Users are asked to record specific events, feelings or interactions with their environment, anonymously. Included in the package are sometimes ambiguous instructions such as "photograph the spiritual center of your home". The purpose is to get to know better the users' context and culture, rather than look for solutions for specific needs. Designers then interpret the probe returns and use those insights to create further design artifacts, in a manner of conversation with the users.

For this application we are interested in getting to know how users experience their own travel habits. The way we will use the results is similar to the way the original creators intended, i.e. as inspiration for the design of the artifact for mobility data.

Our probe might then include instructions such as “put an X on the most public place you usually frequent on a weekday”. Our interpretation of the probe results will be crucial when designing the mobility data artifact.

Mobility data artifact

We have been previously exploring the properties of network and terminal positioning data, in an attempt to determine the technological constraints that this kind of data poses. Some of our work is publicly available [14]. There are many methods to estimate the location of the user within the network. The accuracy of the location information varies greatly based on which method is used to estimate the location of the user. It depends on the positioning method used, the layout of the network, and the surroundings of the subscriber that is being located. Depending on the combination of these factors the location information can have anywhere between 5m to 30km of uncertainty.

As it will, most likely, not be possible to have access to real network data – as it is heavily regulated and operators do not easily release it – we envision our artifact to run on the mobile phone, logging nearby cell towers. The data will then have to be reduced in order to mimic the behavior of the network protocols and enriched with geographical coordinates of the cell towers. The simplest interface possible with the data would be a map shown in the mobile phone, with an approximate trace of the user’s path. However, in order to get rich feedback, we intend to integrate a critical edge to the artifact, much like the work of Paulos or our own, mentioned before. As such, the final artifact could take any shape such as a game, a social network, a personal assistant, etc. In order to get inspiration for the design we will use the returned packages from the Cultural Probes.

We will distribute the resulting artifact – most likely an app for a smartphone –to a small group of users (<10) for a period of two weeks, where it will collect the data and possibly show it, in some form, in real-time. After that period of time we will conduct semi-structured interviews where we will follow a similar model to the ones used by Bowen [22] for his critical artifact methodology. Users will engage in a dialogue with the designers, with the artifact as a catalyst, and will be prompted to manifest their reactions to the artifact and to their own data.

4 Conclusion

We expect the resulting knowledge from our process to be a rich qualitative account of user experiences on mobility – from the Cultural Probes – and on data collection through the mobile phone. Our hypothesis is that by following an artifact-driven research through design, using Zimmerman’s framework, we can tap into feelings and concerns from users that we wouldn’t be able to reach with conventional methods, such as polls.

References

1. Hincapié, J.D., Tabard, A., Alt, F., Computing, P.: Contextual-Analysis for Infrastructure Awareness Systems.

2. FT.com / Technology - Apple and Android phones face tighter laws in Europe, http://www.ft.com/cms/s/2/b7d304b6-8174-11e0-9c83-00144feabdc0.html#axzz1MmU8R7o4.

3. How Docomo Plans To Use Mobile Data For City Planning & Earthquake Preparation | Penn Olson, http://www.penn-olson.com/2011/06/04/docomo-japan-mobile-spatial/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PennOlson+%28Penn+Olson%29.

4. Bennett, C.J.: In Defence of Privacy. Surveillance & Society. 8, 486 (2011).

5. Sundström, P., Taylor, A., Grufberg, K., Wirström, N., Solsona Belenguer, J., Lundén, M.: Inspirational bits: towards a shared understanding of the digital material. Proceedings of the 2011 annual conference on Human factors in computing systems. pp. 1561–1570 (2011).

6. Kuznetsov, S., Paulos, E.: Participatory sensing in public spaces: activating urban surfaces with sensor probes. Proceedings of the 8th ACM Conference on Designing Interactive Systems. pp. 21–30 (2010).

7. Li, I., Dey, A., Forlizzi, J., Höök, K., Medynskiy, Y.: Personal informatics and HCI: design, theory, and social implications. Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems. pp. 2417–2420. ACM, Vancouver, BC, Canada (2011).

8. Lim, Y.-kyung, Nam, T.-jin, Oh, A., Kim, K.-E.: Personal Informatics for Discovering Human-centered Lifecare System Opportunities. Personal Informatics Workshop. ACM, Atlanta, Georgia, USA.

9. Bylund, M., Höök, K., Pommeranz, A.: Pieces of identity. Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges. pp. 427–430 (2008).

10. Chalmers, M., Galani, A.: Seamful interweaving: heterogeneity in the theory and design of interactive systems. Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. pp. 243–252 (2004).

11. Kim, M.-C.: Surveillance Technology, Privacy and Social Control. int sociol. 19, 193-213 (2004).

12. Chandrasekaran, S., Cooper, O., Deshpande, A., Franklin, M.J., Hellerstein, J.M., Hong, W., Krishnamurthy, S., Madden, S.R., Reiss, F., Shah, M.A.: TelegraphCQ: continuous dataflow processing. Proceedings of the 2003 ACM SIGMOD international conference on Management of data. pp. 668–668 (2003).

13. Halloran, J., Hornecker, E., Stringer, M., Harris, E., Fitzpatrick, G.: The value of values: Resourcing co-design of ubiquitous computing. NCDN. 5, 245-273 (2009).

14. Svee, E.O., Sanches, P., Bylund, M.: Time geography rediscovered: a common language for location-oriented services. Proceedings of the 2nd International Workshop on Location and the Web. p. 11 (2009)

15. Why "Human Density Data" Is a Big Deal - O'Reilly Media - O'Reilly Insights - Forbes, http://blogs.forbes.com/oreillymedia/2011/06/06/why-human-density-data-is-a-big-deal/.

16. Nordström, M., Pyy, J. and Salo, L. . Qualitative analysis of Hot Potato. TKK / SICS / University of Helsinki, T-121.5900 (2007)

17. Foucault, M., Sheridan, A.: Discipline and punish: The birth of the prison. Penguin Books New York (1991).

18. Dobson, J.E., Fisher, P.F.: Geoslavery. Technology and Society Magazine, IEEE. 22, 47–52 (2003).

19. Norberg, P.A., Horne, D.R., Horne, D.A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs. 41, 100-126 (2007).

20. Zimmerman, J., Forlizzi, J., Evenson, S.: Research through design as a method for interaction design research in HCI. Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 493–502. ACM, San Jose, California, USA (2007).

21. Gaver, B., Dunne, T., Pacenti, E.: Design: Cultural probes. interactions. 6, 21–29 (1999).

22. Bowen, S.: A Critical Artefact Methodology: Using Provocative Conceptual Designs to Foster Human-centred Innovation, http://www.simon-bowen.com/downloads/research/aCriticalArtefactMethodology.pdf, (2009).

23. Agre, P., Surveillance and capture: Two models of privacy. The Information Society 10, 2, 101-127 (1994)

Lockbox: Applying the Value of Privacy to Cloud Storage

Luke Stark[1] , Matt Tierney[2]

[1] Media, Culture, and Communication, New York University [2] Computer Science, New York University
luke.stark@nyu.edu, tierney@cs.nyu.edu

Abstract. This paper examines one particular problem in cloud computing: how users can take advantage of the cloud to store data without compromising their autonomy and individual empowerment, giving up control of the appropriate flows of their personal data --- in other words, how users can maintain privacy and security in the cloud without sacrificing data availability.

Keywords: privacy, cloud computing, human-computer interaction (HCI), Values-Sensitive Design, security, cryptography, trust, user empowerment

1 Introduction

1.1 Values in Cloud Computing

Context. Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access" to a shared collection of information systems such as "networks, servers, storage, applications, and services" [1]. One appealing feature of cloud computing is its possibilities for data storage; data stored in the "cloud" of a networked server is, in theory, ubiquitously available where and when a user needs it. However, the market leader in cloud storage, file synching, sharing, and versioning —Dropbox—has come under increasing scrutiny for its weak privacy policies [2]. Moreover, as some tech commentators have noted, Dropbox's uncomplicated reliance on Amazon's Simple Storage Service makes the scope of Dropbox's own *Terms of Service,* and its own security mechanisms, secondary to a more general problem: the vulnerability of user data stored in the cloud to privacy breaches, unauthorized or unanticipated access and circulation outside the control of the individual [3].

Application. Lockbox is a secure, built-from-scratch, cloud storage application that seeks to preserve certain values expressed in conventional cloud storage systems—namely, usability and data availability—while radically improving technical expression of the values of privacy and security for its users. As such, Lockbox is a privacy/security-aware alternative to popular systems like Dropbox. As Deborah Johnson observes, "computer systems cannot *by themselves* be moral agents, but they can be components of moral agency" [4]. The initial impetuses behind the creation of Lockbox were the realizations that (a) from an empirical and technical standpoint, individual data storage in the "cloud" was not as secure as it might be, and (b) from a conceptual standpoint Dropbox's standing in the burgeoning field of cloud storage should be critically assessed from a values perspective.

Competing Models. A number of consumer applications currently provide user storage in the "cloud": these include SugarSync, Mozy and market leader Dropbox. While these applications do claim to encrypt user data, they do so only external to the applications themselves: the data is still vulnerable to inadvertent or deliberate access by employees of the companies involved, or to malicious actors hacking into the system. A number of consumer applications featuring enhanced security are also available, some of which are similar conceptually to Lockbox: these include Wuala, Tahoe-LAFS, Lockify, and SpiderOak. Arguably, these systems sacrifice the convenience of a single folder abstraction (e.g., Wuala) or demand extraordinary expertise and confidence from end-users (e.g., installing a new file system). As such, the Lockbox team determined that a new application build specifically with privacy values in mind was an appropriate project.

Conceptual Frames. This case study builds primarily on the framework of Value Sensitive Design (VSD) [5] [6]. As Flanagan, Howe and Nissenbaum observe, "the study of human and social dimensions of technology is so demanding [because] the areas of knowledge and the methodologies it straddles are traditionally both far-flung and self-contained" [7]. Given the challenges inherent in drawing together even as proximate a pair of disciplines as media criticism and computer science, Value Sensitive Design, "a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" [8], seems the most practical system at hand. While acknowledging similar schema for evaluating human values within technological systems, such as reflective design [9], and incorporating some of these methods' key insights into our analysis, we believe VSD provides a robust and flexible framework within which to conduct our assessment of values designed into distributed systems.

1.2 Discovering Values in the Cloud

User Empowerment. In preliminary discussions, the design team identified the concept of individual online autonomy—what David Clark and his co-authors term "user empowerment"—as an important value underpinning both the team's general critique of Dropbox's shortcomings, and its intuitions for improvements. According to Clark et al., user empowerment is " the preference that the user, rather than the service provider or the software provider, be able to pick what applications to run, what servers and services to use, and so on." Clark and his co-authors suggest that user empowerment is a basic principle of the Internet itself: it is "the manifestation of the right to choose—to drive competition, and thus drive change" [10]. In the distributed system context, we take "user empowerment" to mean accentuating the autonomy promoted by the cloud while diminishing the prospects for data to go astray beyond the user's contextualized choices or permissions.

Availability. User empowerment or autonomy in cloud computing is defined by the cloud's model of data availability. The user model for cloud storage presumes that the physical mobility of individuals (across cities, borders, access terminals, or mobile devices) matches data flows, and that people desire a virtual place to store data without requiring the end-user to update or duplicate files constantly, or worry about leaving a particular file on a particular piece of hardware (e.g., a USB flash drive); in other words, a place accessible from anywhere with network access. In practical terms, Amazon Web Services' Simple Storage Service (S3) provides this virtual location for both Dropbox and Lockbox.

Tradeoffs. In light of the design team's decision to highlight user autonomy as a key value in distributed systems, the team came to view autonomy as the correlation between the lived decisions and choices of a user and the synchronous availability of data within the cloud *solely to that particular user*. Data in the cloud is conveniently accessible from multiple points, matching a user's mobility; however, when a user is not accessing data, that user's autonomy is preserved if the data is inert, inaccessible. The team therefore decided to turn to cryptography as a technical system through which the value of user empowerment could be actualized, paradoxically by binding the user—and arguable reducing autonomy—to his or her data through knowledge of an encryption key.

Any digitally encoded data is evidently not materially "inert" — it can be moved or copied easily, including between different servers or terminals networked to the cloud. Cryptography permits data to persist in the cloud, but be separated from their legibility, and therefore their practical utility for users without the code: while the quantity of data is still discernible, its significance is, to most, only so much "noise." Flows of information persist, but their contents are blocked from those without the decryption key. The Lockbox user views her data as cleartext, while unauthorized actors peering at data within the cloud storage server or network would perceive a user's data as ciphertext. Thinking of "user empowerment" and "availability" together allowed the design team to consider what design tradeoffs were truly necessary in order to ensure the values of privacy and security could be built into a cloud storage system; the decision to limit the legibility of data through encryption to the user "in the know" trades global availability of data for enhanced privacy for both any one user and that user's data.

2 Designing Values in the Cloud: Lockbox

Application Specifics. The Lockbox application operates as a background user program, synchronizing contents from user-specified directories to a cloud storage service. Data is encrypted in transit to and in storage on the cloud service provider's servers. Lockbox also enables users to share encrypted data with friends who use the Lockbox program, and makes secure file sharing private and always available. In conceptualizing and creating Lockbox, the design team was inspired to consider user empowerment in the cloud in several novel ways, particularly in regards to the role of encryption in enhancing online autonomy. Lockbox's encrypted storage is prototypical of a new approach to cloud storage: by setting the parameters for online data to be protected within a particular encrypted "slice" of the "cloud" controlled by a particular user, Lockbox begins to carve out autonomous spaces legible to particular individuals within servers protected by encryption, within which data is preserved until needed. Thus, it was also important to the design team that Lockbox be portable across platforms and operating systems in order to preserve a high degree of user choice. As such, Lockbox was written using the versatile Python programming language, licensed under a Sleepycat License (Open Source Initiative), and designed so that its configuration by end users could be accomplished through a web browser (a standard artifact and mostly homogeneous rendering engine across common contemporary desktop operating systems). In accord with the essence of the Sleepycat License, Lockbox also consists of bundle open source libraries for Amazon Web Service APIs, OpenSSL (implements stream and block ciphers), and GNU Privacy Guard (implements OpenPGP protocol).

Privacy. There is a voluminous literature available on the subject of online privacy, here defined as the "appropriate flow of information" [12]. A number of authors have suggested that informational or data privacy is a vital means to foster individual freedom in the face of institutions equipped with ever-more sophisticated systems for data harvesting, mining, retrieval and analysis [13] [14] [15] [16] [17]. Others have argued that technology has changed little in terms of the balance between a need to protect individual rights online versus the prerogatives of law enforcement and commerce [18] [19]. More nuanced empirical analysis has examined the ways in which everyday users of technology craft strategies for privacy in online situations which are less than amenable [20]. Though Lockbox's mission is not identical to that of those espousing information privacy in general, we are evidently sympathetic to the criticisms espoused by the former view, namely that the promiscuity and recombinability of data requires close attention to empowering users to make "appropriate" choices themselves.

As Brian Whitworth and Aldo de More suggest, "Internet privacy concerns seem essentially a conflict between a social requirement (privacy) and current Internet system design"; this conflict represents a "social-technical gap...the degree software fails to meet social requirements" [21]. Siani Pearson observes that, "The privacy challenge for software engineers is to design cloud services in such a way as to decrease privacy risk, and to ensure legal compliance" [22]. With Lockbox, the challenge with designing privacy affordances lacking in other cloud-based storage services that rely on a "middleman" hinges on balancing the convenience of the end user with a robust encryption regime enabling privacy.

Along with its mobilization for industrial and military applications, cryptography has a long history of association with user empowerment movements online [23]. In existing cloud storage systems, one of the most common and practical methods for securely storing data is using a *symmetric key* encryption method known as the AES-256 block cipher. Symmetric key cryptography is very similar to the everyday use of passwords to log into computers, email services, etc.; to access a password-encrypted document simply requires the correct password. However, this password, or “key,” must be shared between all parties who the owner wants to grant access to the data. The privacy practices of services like Dropbox raise concerns surrounding middleman companies that use symmetric key encryption, since the organization stores the password that is used to encrypt the stored data. The middleman can see the data and can release the cleartext data when pressured by an outside agency, at their employees’ whim, or when their security services are compromised.[4]

Lockbox uses a cryptographic system based on the primitives of symmetric key and public key cryptography. Public key cryptographic techniques are used to sign and encrypt data for two purposes: first, signing data (with the private key) guarantees that the recipient knows that sender of the data is who the sender claims to be; second, encrypting data (with the public key) guarantees that only the corresponding private key owner can decrypt the data. (Notably, the public key cannot be used to decrypt the public key encrypted data.) Lockbox uses a hybrid cryptosystem, a well-known combination of symmetric key and public key cryptography, to ensure privacy for user’s files. A randomly generated 32 character password is generated per file; this password is used to AES-256 encrypt a file. The password is then encrypted with the public key of whomever the file owner wants to share the file with; the public key-encrypted password files (more than one, since there are multiple users to share the file with) and the symmetric key encrypted file are then uploaded to the cloud service. The symmetric key encrypted file and the corresponding public key encrypted password file are made accessible to the user the file owner wants to share the original data with. Lockbox manages these operations in an opaque manner. A user is only required to drop files into her Lockbox directory, specify with whom she wants to share the file from the Lockbox address book; the application manages the rest of the transaction. However, managing public keys remains a hard problem for security and privacy.[5]

[4] The current practice for users who desire to combine the convenience of Dropbox with some type of encryption system involves an application called TrueCrypt, a free and open source disk encryption system. On a user’s file system, TrueCrypt creates block cipher-encrypted “volumes,” which are password-encrypted directories. Challenges arise for end-users, however, with respect to user experience details such as the order in which the TrueCrypt and Dropbox are started (or stopped) when a computer boots (or shuts down). Moreover, the trouble with this method of sharing is that security hinges on sharing a password with another user (recall the difficulty with symmetric key encryption techniques, in general). A single password that must be shared remains a dubious mechanism to protect secrets especially since the compromise of the password compromises the secrecy of the entire Dropbox volume undetectably.

[5] For instance, the design team must solidify the design for how to appropriately handle access revocation. Do we retroactively apply the revocation to all previous versions of a file? Other concerns include how do we want to store public keys and access control lists on the cloud. We may risk revealing information about users (therefore compromising privacy) with a bad design of key and ACL management. At the time of writing, the initial Lockbox prototype implemented a naive, proof-of-concept privacy, key management, and access control story. For every file and file update, a new password key is generated. Revocation is simple by changing permissions to the corresponding object in an S3 bucket as well as removing the revoked user’s keys from the list of keys with which to encrypt the files. The choice to implement a simple yet

Deploying a hybrid cryptosystem within the cloud allows Lockbox to operationalize a view of privacy based on contextual access and flow of data to a particular user: Lockbox therefore qualifies as a privacy-enhancing technology (PET). Herbert Buckert has defined PETs as technologies that “seek to eliminate the use of personal data altogether or...give direct control over revelation of personal information to the person concerned” [24]. Buckert’s taxonomy of PETs includes subject-oriented, object-oriented, transaction-oriented and system-oriented technical concepts; Lockbox operates primarily as a subject-oriented PET, by aiming to “eliminate or substantially reduce the capability to personally identify the acting subject” through hybrid cryptography [25]. The design team is cognizant of Buckert’s critiques of PETs, particularly that the values underpinning the design of such technologies must be carefully though through.

Security. Lockbox assures users that through its algorithm they are secure and free from harm in their data storage privacy. While security is not zero sum, the data that is secured sometimes is: the secure and encrypted nature of Lockbox’s service may prompt care and attention from lawmakers and regulators with an interest in tracking and classifying in the “cloud.” Moreover, Lockbox obviously does not protect side-channel or covert channel attacks, such as screen shots or password copying --- threats which are predicated on a breakdown of trust offline.

Cost. One final value the design team engaged with in the creation of Lockbox was of low cost, both financially and in terms of computer resources: given that the political economy of distributed systems ties the latter to the former for users, the design goal was to limit both. Using a service like Amazon S3 costs fractions of pennies to store and retrieve gigabytes of data. However, a user modifying an already-stored file on her laptop should not require her to upload the entire file again to the cloud (this would be a costly, repetitive operation for most of the file). The process of applying *delta encoding* for incremental modifications is easy on cleartext files; however, encrypted files make this process more difficult. Finding the right design to enable delta updates without revealing information about the files to the cloud will be important for future versions of Lockbox.

To address the value of minimizing costs, the design team has begun implementing a more cost effective design that leverages the rsync algorithm in addition to Amazon Web Services’ Simple Queue Service (SQS) and SimpleDB [26]. rsync is a well-known algorithm designed to quickly compute differences between files and quickly apply delta updates to files. SQS is designed to store messages as they travel between computers. SimpleDB is designed as a (optionally, strongly consistent) database optimized for efficient index and select queries (non-relational queries). By combining the affordances of delta encoding (to minimize bandwidth and storage costs), messaging (to send notices easily between machines that share files), and

inefficient design was made by the design team for the purpose of demonstrating a working proof-of-concept prototype. Nevertheless, the design team has debated the “correct” design of the key management and access control story; we expand on this point in the “Cost” section.

strong consistency (to ensure total ordering of updates), the design team will maintain the original vision of a correctly-implemented file sharing, syncing, and versioning while minimizing costs to end-users and trusted computation in the cloud.

3 Conclusion

3.1 Discovering Users

As Lockbox has yet to go through alpha testing by users, more empirical research and feedback is needed to assess the degree to which the design team has been successful in programming for "user empowerment," enabled by cryptographically ensured privacy. We are mindful of Sengers et al.'s six strategies for putting reflective design into practice, particularly that of using technical design to "probe" for un-assumed user needs and the exploration of previously overlooked concepts and metaphors brought forward by the user" [27]. Further empirical work is also necessary to systematically identify the design choices made by other secure cloud storage services: whether these applications have made similar or divergent design choices from those of the Lockbox team, and how design choices have affected expressed values in the use of the application.

More broadly, interactions with prospective users continue to influence future design considerations of Lockbox. While the design team is aware that new technologies will inevitably breed new uses and new users, specific user constituencies have already been identified. In particular, discussions with technologists who work with human rights workers have yielded valuable insight into needs that Dropbox fails to meet. Human rights activists who must share large videos with individuals outside of a country of interest require bandwidth-shaping features to avoid detection by governments who censor network activity. Without bandwidth shaping to limit the amount of traffic uploaded or downloaded through a file sharing service, giant bursts of traffic could raise red flags for censoring governments. These interviews have prompted the design team to consider ways to extend Lockbox's privacy-enhancing functions in future iterations of the product. At this point, further research and testing is a necessary compliment to the theoretical and technical work already accomplished. Ideally, the Lockbox project will not only stimulate further conceptual and theoretical work on the status of the individual and her privacy in the "cloud," but also lead to a product useful to these groups whose design reflects attention to the values at play within it.

References

1. Mell, P. & Grance, T.: The NIST Definition of Cloud Computing (Draft). National Institute of Standards and Technology Special Publication 800-145 (Draft) (January 2011)
2. Gain, B.: Why Dropbox's Privacy Policy Is OK (Just Proceed Carefully) PCWorld, http://www.pcworld.com/printable/article/id,226080/printable.html

3. Matthews, L. “Dropbox responds to privacy outrage.” Geek.com, http://www.geek.com/articles/news/dropbox-responds-to-privacy-outrage-20110421/
4. Johnson, D.G.: Computer Systems: Moral Entities but not Moral Agents. In: Ethics and Information Technology 8, 195-204 (2006)
5. Friedman, B. & Nissenbaum, H.: Bias in Computer Systems. In: ACM Transactions on Information Systems 14(3), 330-347 (1996)
6. Friedman, B., Kahn, P. and Borning, A.: Value Sensitive Design and Information Systems. In: Schneiderman, B., Zhang, P., & Galletta, D. (eds) Human-Computer Interaction in Management Information Systems: Foundations, pp. 348--372. M.E. Sharpe, New York (2006)
7. Flanagan, M., Howe, D., & Nissenbaum, H.: Embodying Values in Technology: Theory and Practice. In: van den Hoven, J., Weckert, J. (eds) Information Technology and Moral Philosophy, pp. 322—353. Cambridge University Press, Cambridge (2008), 324
8. Friedman, B., Kahn, P. and Borning, A.: Value Sensitive Design and Information Systems. In: Schneiderman, B., Zhang, P., & Galletta, D. (eds) Human-Computer Interaction in Management Information Systems: Foundations, pp. 348—372. M.E. Sharpe, New York (2006), 350
9. Sengers, P., Boehner, K., David, S. & Kaye, J.: Reflective Design. In: Culturally Embedded Computing Group, pp. 49--58. Cornell Information Science, Ithaca (2005)
10. Clark, D. D., Wroclawski, J., Sollins, K. R., & Braden, R.: Tussle in Cyberspace: Defining Tomorrow's Internet. IEEE/ACM Transactions on Networking 13(3), 462-475 (2005), 473
11. Brewer, E.: Towards Robust Distributed Systems. Principles on Distributed Computing (2000)
12. Nissenbaum, H.: Privacy in Context. Stanford University Press, Stanford (2010), 127
13. Cohen, J.: Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review 52, 1373--1438 (2000)
14. Kerr, I. & McGill, J.: Emanations, Snoop Dogs and Reasonable Expectations of Privacy. Criminal Law Quarterly 52(3), 392--432 (2007)
15. Ohm, P.: The Fourth Amendment Right to Delete. Harvard Law Review 119, 10--18, Gannett House, Cambridge (2005)
16. Solove, D.: A Taxonomy of Privacy. University of Pennsylvania Law Review 154(3), 477--564 (2006)
17. Lyon, D.: Data, Discrimination, Dignity. In: Surveillance Studies: An Overview, pp. 179--197. Polity Press, Malden, MA (2007)
18. Kerr, O.: Searches and Seizures in a Digital World. Harvard Law Review 119, 531--585, Gannett House, Cambridge (2006)
19. Posner, R. A.: An Economic Theory of Privacy. Regulation 2(3), 19--26 (1978)
20. boyd, danah: Making Sense of Privacy and Publicity. SXSW. Austin, Texas, March 13 (2010)
21. Whitworth, B. and Moor, A.: Legitimate By Design: Towards Trusted Socio-Technical Systems. Behavior and Information Technology 22(1), 31-51 (2003), 33
22. Pearson, S.: Taking Account of Privacy when Designing Cloud Computing Services. Proc. ICSE-Cloud09, Vancouver, IEEE (May 2009)
23. Levy, S.: Crypto Rebels. In: Ludlow, P. (ed) High Noon on the Electronic Frontier, pp. 185--205. The MIT Press, Cambridge (1996)
24. Burkert, H.: Privacy-Enhancing Technologies: Typology, Critique, Vision. In: Agre, P. & Rotenberg, M. (eds) Technology and Privacy: The New Landscape, pp. 125-142. The MIT Press, Cambridge (1997), 127
25. Burkert, H.: Privacy-Enhancing Technologies: Typology, Critique, Vision. In: Agre, P. & Rotenberg, M. (eds) Technology and Privacy: The New Landscape, pp. 125-142. The MIT Press, Cambridge (1997), 125
26. Tridgell, A. & Mackerras, P.: The rsync algorithm. The Australian National University (1996)
27. Sengers, P., Boehner, K., David, S. & Kaye, J.: Reflective Design. In: Culturally Embedded Computing Group, pp. 49—58. Cornell Information Science, Ithaca (2005), 56-57.

Elicitation of Values, Motivations and Emotions: The VBRE Method

Sarah Thew[1], Alistair Sutcliffe[2]

[1] Northwest e-Health, University of Manchester, UK
[2] Manchester Business School, University of Manchester, UK
(sarah.thew, alistair.sutcliffe)@manchester.ac.uk

Abstract. Soft issues, such as emotions, motivations and values are often cited as problems in the RE process. A method is presented for analysing such issues. The method includes a taxonomy of users' values, motivations and emotions, with guidance for eliciting and analysing these issues during the RE process. Two method evaluation studies are described: a questionnaire evaluation of the website and method by novice and RE experts, and preliminary results from a series of three industry based case studies making use of the method during software development projects. The validation studies demonstrate the utility and acceptability of the method by industrial practitioners.

Keywords: Requirements elicitation, values, motivations, emotions.

1 Introduction

Soft issues, such as politics and people's feelings are often cited as problems in the RE process, although there is little advice about how to deal with these issues. Few studies have directly considered stakeholders' emotions during the analysis phase, although there have been numerous studies which report the impact of negative user emotions after implementation e.g. [1, 2]. Gowler [3] observed that systems must fit with stakeholders' values and beliefs to be successful. However, it is not easy to gain insight into personal values or emotions, since people rarely directly express such information. Experienced analysts may develop the ability to understand users' values, motivations and emotions; however, this knowledge is tacit and rarely articulated. In this paper we attempt to make such knowledge explicit and propose a method for analysis of users' 'soft' issues in RE.

Values are beliefs and attitudes held by people about other people, organisations or artefacts. Kluckhohn's definition of values [4]:

"a conception explicit or implicit, distinctive or an individual or characteristic of a group, of the desirable which influences the selection from available modes, means and of action"

has been adopted by studies into values in the context of software development[5, 6]. Values are complex concepts or knowledge schema, related to our beliefs and attitudes, which shape our response to events.

Motivations are long-lasting, high-level behavioural drivers, the strength with which a motivation is held will influence the intensity and persistence of behaviour. An understanding of motivation can be helpful in interpreting stakeholder behaviours during software design and development [7].

Emotions are reactive responses to events, objects and artefacts. Software developments have the potential to change working circumstances and therefore to have an emotional effect. Understanding values, motivations and emotions helps requirements engineers interpret stakeholder concerns and behaviours, the VBRE (Value Based Requirements Elicitation) method aims to facilitate this process.

2. The VBRE Method

Questionnaires are effective for surveying values, motivations or emotions within a population; however, they restrict investigations to a pre-defined set of responses. Elaboration and exploration are desirable when considering subjective concepts, since one person's understanding of a value such as 'equality' may well manifest itself with a meaning quite different from someone else's. Furthermore, our research with practicing analysts indicated that they did not feel questionnaires were an appropriate or acceptable tool for exploring what might be sensitive or difficult subjects [8]. Hence the VBRE method aims to encourage a rich, qualitative understanding of the meaning of values, motivations and emotions within the context of individual projects and stakeholders.

The method integrates into the analysts' usual elicitation activities, making use of the outputs of standard techniques such as interviews and workshops. The method can be used in two modes to suit novice or expert analysts and the time resources available.

In novice mode (summarised in figure 1), preliminary analysis of the known project circumstances and the VBRE taxonomies leads to identification of key issues or 'hunches', i.e. a sub-set of the users' values, motivations or emotions considered relevant to the project. Making these intuitions explicit encourages gathering evidence to support or challenge initial hunches.

The analyst then begins their standard requirements elicitation work: interviews, workshops etc., the elicitation advice provided by the VBRE website (see below) can be used to support this work, e.g. a list of questions that can be used to explore 'trust'.

At regular intervals the analyst will review elicitation outputs for evidence of the expression of values, emotions or motivations. This involves reviewing interview/meeting notes for evidence of the expression of values, emotions or motivations. Novice analysts may wish to transcribe sections of text from audio recordings, if time resources are constrained an alternative is to simply listen to audio recordings and make notes.

These reviews are inspected for frequently expressed value, motivation and emotions and possible causations thereof. The hunch list is modified following each cycle of reflection, and develops incrementally into a rich picture of the stakeholders' values, motivations and emotions. Finally the implications of the analysis for both the project process and the design are reviewed. These may be functional and non-functional requirements, but also recommendations for project procedures, functional allocation and work design.

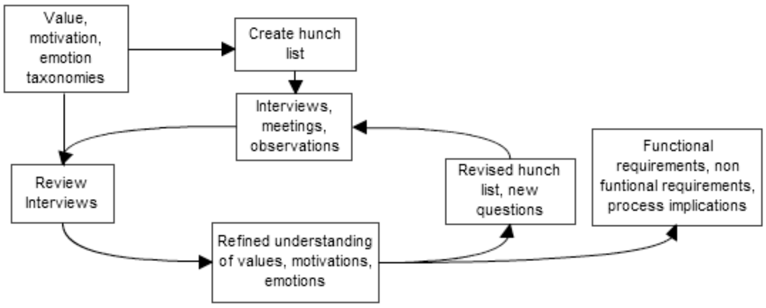

Value, motivation, emotion taxonomies
Create hunch list
Interviews, meetings, observations
Review Interviews
Revised hunch list, new questions
Functional requirements, non funtional requirements, process implications
Refined understanding of values, motivations, emotions

Figure 1. The novice pathway through the VBRE method.

In expert mode, the method knowledge is internalised so it can be used to formulate appropriate questions framed by the analyst's understanding of the application domain. The method becomes part of the expert's battery of techniques in scenario analysis, questioning using storyboard and prototype probes; as well as informing review of interview notes, using Tables 1-3 as aide-memoires and prompts for wider thinking about values, motivations and emotions.

2.1 VBRE Taxonomies

The taxonomy of values and their consequences for process guidance are illustrated in Table 1. Eight upper-level value categories are proposed based on existing analyses of value theory [5, 9] and our own investigations from card sort experiments and expert interviews. The process implications in column 4 vary from organising the team composition in response to aesthetic needs, specialisation of the RE process to include safety and risk analysis, to more general heuristics for project team management.

Table 1. Values: potential sources and implications for RE

Value concept	Related terms	Potential sources	Process implications
Trust	openness integrity responsibility,	Relationships with other individuals /groups. Privacy policies	less control, improved confidence
Collaboration	cooperation friendship altruism	Relationships with others Awareness of others – office politics	improved cooperation shared awareness
Morals/ Ethics	Justice, fairness equality tolerance	Behaviour towards others Opinions of others' behaviours	openness and honesty in team
Creativity Innovation	Originality, adventure	Work processes, problem solving	Creativity workshops, brainstorming
Aesthetics	Beauty nature, art, design	Self appearance reaction to images, shapes, art and design	Design as a priority, storyboards

Security	safety privacy, risk	Data management policies Attitudes towards change	hazard / threat analysis
Personal characteristics	serious/playful introvert/extrovert; systematic/ opportunistic	Self image, personae scenarios, psychological questionnaires	Customisation analysis for personal RE. team conflict management
Beliefs & Attitudes	cultural, political, religious topics	Leisure interests, user background, reaction to news events	Team composition, incentives

Motivations are important for understanding the behaviour of stakeholder groups as well as for individual-level requirements, some motivations may also be important as properties of organisations. Table 2 summarises the more important motivations for requirements analysis, synthesised from existing theories of motivation [10][11].

Table 2. Motivations and their implications

Motivation	Description	Implications
Power	need to control others, authority, command	Work organisation, responsibility, control Hierarchy
Possession	desire for material goods, wealth	resource control, monetary incentives, marketing,
Achievement	need to design, construct, organise	goal oriented, need to align users with project aims
Self-esteem	need to feel satisfied with oneself	link personal & project goals, praise personal achievement
Peer-esteem	need to feel valued by others	team composition social feedback & rewards
Self-efficacy	confidence in own capabilities	confidence building, training, skill matching
Curiosity, learning	desire to discover, understand world	extensible systems, self tutoring
Sociability	desire to be part of a group	collaboration in work organisation
Altruism	desire to help others	cooperation in work organisation

Emotions can give useful feedback about reactions to project plans and designs, especially since emotional responses are stronger than ordinary opinions and may therefore indicate significant problems leading to user dissatisfaction or system rejection. The principle emotions and their consequences are given in Table 3. These emotions are based on the classification of emotions as responses (positive or negative) to events, people or artefacts by Ortony et al [12]

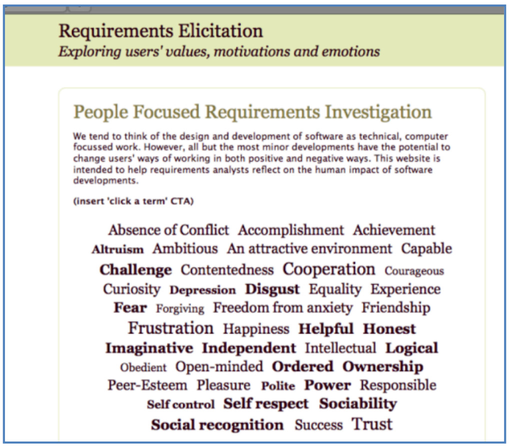
Table 3. Emotions and their potential causes

Emotion	**Related feelings**	**Possible causes**	**Remedial action**
Fear	fright, worry threat	Design is threatening, negative consequences	Review/ameliorate threats
Pleasure	joy, happiness	Design is rewarding, positive	None; note for future reference

Anxiety	Uncertainty worry	Specification may be confusing, consequences not clear, little involvement	Explain specification, use scenarios, reassure users
Frustration	annoyance, anger	Irreconcilable conflict, barriers, value-interest clashes, values ignored	Revisit stakeholder analysis
Disgust	revulsion, horror	Design has clash with values/culture	Radical design review
Depression	withdrawn, isolated, alone	Lack of involvement in process, values ignored	Re-engage users, improve communication & motivation

2.2 Initial Method Evaluation and Development of the VBRE Method Support Website

A preliminary evaluation of the method was carried out by the first author, during two software projects. The method was trialled across several interviews and outputs reviewed with other project team members. The process of structured, guided reflection was considered valuable. However, it was also felt that some concepts in the taxonomy required additional explanation; that further elicitation advice was useful, and that paper tables were difficult to work with. To make the taxonomies more accessible a website was developed (http://www.vbre.org.uk), structured around a table of values, motivations and emotions, with content drawn from the taxonomies (figure 2).



Requirements Elicitation
Exploring users' values, motivations and emotions

People Focused Requirements Investigation

We tend to think of the design and development of software as technical, computer focussed work. However, all but the most minor developments have the potential to change users' ways of working in both positive and negative ways. This website is intended to help requirements analysts reflect on the human impact of software developments.

(insert 'click a term' CTA)

Absence of Conflict Accomplishment Achievement
Altruism Ambitious An attractive environment Capable
Challenge Contentedness Cooperation Courageous
Curiosity Depression Disgust Equality Experience
Fear Forgiving Freedom from anxiety Friendship
Frustration Happiness Helpful Honest
Imaginative Independent Intellectual Logical
Obedient Open-minded Ordered Ownership
Peer-Esteem Pleasure Polite Power Responsible
Self control Self respect Sociability
Social recognition Success Trust

Figure 2. Screenshot of the main values, motivations and emotions navigation table from the VBRE website.

Each term has a page of detailed content, including example interview questions, scenarios to help the analyst consider how values, motivations or emotions might be important to their project, advice about its potential impact on the requirements process or software design.

3. Method Validation

Two approaches have been used to evaluate the VBRE method. Below we present a short summary of results from (i) a questionnaire to evaluate the website with RE students and professional analysts, and preliminary findings from (ii) an on-going series of case studies investigating use of the VBRE method and website by practising requirements analysts.

3.1 Questionnaire Evaluation of the website

A questionnaire was used to gather feedback about the website. Respondents were asked to explore the website and then rate its utility and comprehensibility on a 7 point Likert scale. Respondents could also supply free text comments. The first group of respondents were final year undergraduate students (n=12, 9 male 3 female) who had just completed a course in requirements engineering. The second group were professional requirements engineers recruited by a 'snowball' approach (n=6, 4 male, 2 female), by email with a short description of the purpose of the website, and links to the website and the questionnaire.

Both the students and RE experts rated all aspects of the website positively, see table 4, in particular both groups felt the scenarios and associated lists of related values, motivations and emotions were very useful. The experts were slightly more critical of comprehension of the concepts and design advice, which is not surprising given their more extensive experience; however even these lower ratings were well above the mean.

Table 4. Students and expert ratings of the VBRE website based on a 7 point Likert scale.

	Students **Mean (SD)**	**Experts** **Mean (SD)**
Content Quality	5.5 (0.85)	6.33 (0.85)
Comprehensibility – contents clear?	6.45 (0.52)	5.66 (0.85)
Comprehensibility - easy to understand?	6.08 (1.03)	4.5(1.76)
Utility - scenarios	6.17 (0.63)	6.17(0.98)
Utility – design advice	5.75 (0.75)	4.83(1.94)
Utility - overall	6.33 (0.84)	6 (1.26)

3.2 Case Study Evaluation

Whilst results from this initial questionnaire based study were encouraging, this approach was unable to tell us anything about the utility of the method in practice. We are running a series of case studies working with practising analysts who are using the VBRE method and website in their own projects. We are using the case studies to explore a number of questions:

- The impact (if any) of the method in the projects under study.
- Whether the method and website are used in the same way by novice and expert analysts?

- How the method is adapted for use in ‘real-life’

Three volunteers were recruited by advertising within local requirements and usability groups:

Analyst 1 (A1) has a background in nursing and health informatics, but little formal requirements analysis training and has only worked as an analyst on one previous project.

Analyst 2 (A2) has a background in bioinformatics and has worked as a requirements analyst for 5 years on a series of large European projects around the sharing of scientific methods and results. She is testing the VBRE method within one of these projects, currently in a state of flux as new partners join the established project team.

Analyst 3 (A3) has a degree in Computer Science and has worked as a requirements analyst for over 10 years. He is a contractor working in a wide variety of industries, and is testing the VBRE method within a project to allow users from multiple health organisations to share sensitive patient information.

We are using interviews and diary keeping to collect data about analyst experiences of working with the VBRE method. An initial introductory interview captured information about analysts’ background, past project experiences and upcoming project work. This introductory meeting also included a tutorial describing the VBRE method and website. The analysts have kept an on-going diary of their experiences of using the method. We will shortly be carrying out final interviews during which we will review the content of the diary. All interviews and meetings have been audio-recorded and described, and we are in the process of thematic coding the content. Completed diaries will also be coded.

3.3 Preliminary Case Study Results and Discussion

Our preliminary results have shown the three analysts making use of the method and website in ways which vary with their levels of experience and the demands of their projects.

Thus far, A1 has used the method and the website in a manner that closely mirrors the novice approach as laid out in figure 1. He has frequently used the interview questions on the VBRE website, and has identified ownership, power and trust as particular issues within his project.

A2 ‘s users are spread across many European countries so rather than regular small individual meetings she holds larger workshops every 6 months. Her main use of the VBRE method has been in preparing for these workshops – in particular thinking about the motivations of new users joining these workshops, and the potential reactions of existing user group members to new team members. She perceives the usefulness of the method lies in encouraging her to make a point of taking the time to anticipate and reflect on soft issues within her projects.

A3’s use of the method has focussed on the website, in particular the list of values, motivations and emotions which he finds very useful when reflecting on the outcomes of interviews. He has identified a strong value clash between medical staff who are keen to share information and collaborate, and the IT team who are extremely anxious about information security and afraid that they will be held responsible for any breaches of patient confidentiality.

4. Conclusions

The VBRE method introduces new considerations into the RE process by drawing attention to individual stakeholders' values, motivations and emotions. The framework advances previous elicitation techniques around 'soft issues' by providing explicit taxonomies of values and motivations to guide discovery. The VBRE framework accommodates novice and expert practice, by describing different pathways for the method knowledge to be used directly as aide-memoires or learned and used directly. This flexibility was well received in the initial industrial trials, and early results from our case studies would also indicate that novice and expert analysts are making use of the method and website in different ways. Future work will focus on analysing the completed case studies, in particular identifying the impact of the VBRE method within the case study projects.

REFERENCES

[1] A. C. W. Finkelstein and J. Dowell, "A Comedy of Errors: The London Ambulance Service Case Study," in *8th International Workshop on Software Specification and Design*, Schloss Velen, Germany, 1996.

[2] K. Breitman, J. C. S. do Prado Leite, and A. Finkelstein, "The World's a stage: a survey on requirements engineering using a real-life case study.," *Journal of the Brazilian Computer Society,* vol. 6, pp. 13-37, 199.

[3] D. Gowler, "Values, Contracts and Job Satisfaction," *Personnel Review,* vol. 3, pp. 4-14, 1974.

[4] C. Kluckhohn, "Value and value-orientations in the theory of action," in *Towards a General Theory of Action*, T. Parsons and E. Shil, Eds.: Harvard University Press, 1951.

[5] E. Mumford, *Values, Technology and Work*: Martinus Nijhoff Publishers, 1981.

[6] Bjorn-Andersen, Hedberg, Mercer, E. Mumford, and Sole, *The Impact of Systems Change in Organisations*: Sijthoff & Noordhoff, 1979.

[7] R. J. Boland and W. F. Day, "The experience of system design: A hermeneutic of organizational action," *Scandinavian Journal of Management,* vol. 5, pp. 87-104, 1989.

[8] S. Thew and A. Sutcliffe, "Requirements Elicitation: Understanding Users' Values and Emotions," in *NordiCHI 2008 Workshop on New Approaches to Requirements Elicitation*, Lund, Sweden, 2008.

[9] N. Rescher, *Introduction to Value Theory*: Prentice-Hall Inc, 1969.

[10] A. H. Maslow, R. Frager, C. McReynolds, R. Cox, and J. Fadiman, *Motivation and Personality*. New York: Addison Wesley-Longman, 1987.

[11] A. Bandura, *Social Cognitive Theory of Mass Communication*: Lawrence Erlbaum Associates, 2001.

[12] A. Ortony, C. G, and C. A, *The Cognitive Structure of Emotions*: Cambridge University Press, 1990.