UNIVERSITÄT
KOBLENZ · LANDAU
Institut für
Computervisualistik

FB 4
Informatik

Extension of a didactic media competence model by privacy risk

Alexander Hug
Rüdiger Grimm

Nr. 5/2016

Arbeitsberichte aus dem Fachbereich Informatik

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Lämmel

Kontaktdaten der Verfasser

Alexander Hug, Rüdiger Grimm
Institut für Computervisualistik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
E-Mail : hug@uni-koblenz.de, grimm@uni-koblenz.de

Extension of a didactic media competence model by privacy risk

ABSTRACT

Six and Gimmler have identified concrete capabilities that enable users to use the Internet in a competent way [6]. Their media competence model can be used for the didactical design of media usage in secondary schools. However, the special challenge of security awareness is not addressed by the model. In this paper, the important dimension of risk and risk assessment will be introduced into the model. This is especially relevant for the risk of the protection of personal data and privacy. This paper will apply the method of IT risk analysis in order to select those dimensions of the Six/Gimmler media competence model that are appropriate to describe privacy aware Internet usage. Privacy risk aware decisions for or against the Internet usage is made visible by the trust model of Mayer et al. [4]. The privacy extension of the competence model will lead to a measurement of the existing privacy awareness in secondary schools, which, in turn, can serve as a didactically well-reasoned design of Informatics modules in secondary schools. This paper will provide the privacy-extended competence model, while empirical measurement and module design is planned for further research activities.

Keywords

- privacy competence model
- media competence model
- privacy and personal data
- security awareness
- risk
- trust
- Internet usage

1. INTRODUCTION: THE NECESSITY OF ADDRESSING THE TOPIC OF DATA PROTECTION IN CS EDUCATION

Today's world, in which students need to find their way, is marked by the consistent use of information technology in both educational and private contexts. The independence from a fixed time and place raises the frequency of usage of such systems. The usage of systems which allow for internet usage and online communication does not necessarily show how these systems treat personal data, which is why their protection needs to be given a high priority. Thus, data protection is a very important topic of contemporary computer science education.

If one takes a look at computer science education syllabi and educational standards in Germany, the topic of data protection is explicitly mentioned. However, press reports on misconduct by young people on the internet and results of certain studies suggest that data protection is not sufficiently dealt with in computer science education and other school subjects.

One instance where pupils face data protection risks are social networks. Here, it is possible to reveal too much personal data. Faulty or insufficient data protection settings lead to unintended publication and transfer of data. Moreover, studies show that students are rarely aware of the consequences of their postings. Often, they also do not know which kind of data are not necessary by online shopping. In order to strengthen their conscious handling of their own personal data, this competence needs to be developed and supported in computer science education.

Internet usage always includes an interplay between self-regulation concerning the doings of a user and the tools he or she uses, and the trust which is put in the technical system, their developers and the service providers. It is only in this way that internet usage is truly possible, as it is shown in the following section 2. Thereafter in section 3 we will point out that trust is a prerequisite for taking the risk after assessing it, and we will show how it can be assessed by applying techniques of IT security theory. The correlation between trust and risk is revealed by Mayer, Davis and Schoorman's trust model [4]. In order to carry out a risk evaluation (in this case with respect to the internet with its applications), IT-security methods are executed, as they are described in the IT security analysis reference model [3].

In the consecutive section 4, a media competence model is introduced. This model is capable of measuring students' competences. It is shown that aspects belonging to the topic of data protection can be described by the model. Data protection competence is also significantly characterized by the ability of risk recognition, risk assessment and the differentiation of action strategies such as avoidance or the use of tools and basic settings. This ability, however, is not depicted in the present media competence model. Thus, this model is to be applied and expanded accordingly by choosing and interpreting available competences. This way, a manner of risk evaluation and its embedding into cooperations which include a risk for data protection is carried out. We describe such an approach as a „data protection competence model".

Section 5 will finally draw conclusions of our work and open a perspective for further research. Our data protection competence model serves as a template which – for further research – allows quantitative examinations of the ability of students' risk assessment. The results can be used to derive insights into the organization of teaching contents aiming at the improvement of data protection competence. The protection of one's own privacy is supposed to be paramount.

2. INTERNET USAGE AS AN INTERPLAY BETWEEN SELF-CONTROL AND TRUST

Internet usage is impossible without a trusting cooperation with different parties. In [2], trust is defined „as a willingness on the part of the trustor to undertake a risky action, which he is not in complete control of, in the expectation that the context is controlled by the trustee, thus protecting the trustor.“[1] The interplay between trustor and trustee is described by Mayer, Davis and Schoorman's model [4], which is contemplated in the following section.

The different parties which a user faces when surfing the internet are the software manufacturers (of operating systems, browsers, plug-ins etc.), the internet provider enabling the user to access the web and saving connection details and also other providers offering services which the user wishes to use. Overall, this cooperation is a risky one since the user can only control his or her data to a certain degree. Complete control exists if a user makes a conscious decision for or against passing on personal data in a social network or to a provider (when shopping online, for example). Encryption also offers an option of controlling ones data. This option ends, however, at the point where the trusted partner decrypts the data. Such protective mechanisms, which are controlled by users, count as self data protection mechanisms.

When the user exposes his data, he trusts the other side to handle it appropriately. This use is regulated by privacy statements based on data protection laws. At this point, the user (as the trustor) passes control to the other parties (trustees). It must be considered that the different groups involved (internet provider, software providers, service providers) pursue different targets.

Users can also improve self data protection by means of appropriate tools. This, however, does not change the fact that the user needs to put his trust into a tool which he normally has not programmed himself and expect it to serve its purpose with goodwill and integrity. It needs to be considered how much trust is to be put in the opposite, in this case the infrastructure bearing these tools.

Self data protection control and trust are mutually dependent and closely linked in the risky situation. In this case, the risk needs to be estimated in order to derive an action strategy. If the cooperation puts the user in charge of self data protection control, there is no risk. If, however, there should be some remaining risk present, the user has two options: removing himself or herself from the situation or taking the remaining risk by placing his or her trust in the cooperation. This decision requires knowledge and awareness and thus accounts for a major part of data protection competence. This line of thought is more closely examined in the following section.

3. TRUST AND RISK ASSESSMENT

Drawing on Mayer, Davis and Schoorman's model [4] describing the relationship of trust between trustee and trustor, the user (i.e. the trustor) puts his trust in the providers (i.e. the trustees) because of their competence, their benevolence and their integrity. If there is a risk to be expected, this risk is incorporated into the relationship of trust. The results of this relationship cause the trust to grow or fall, since the results represent the perceived trustworthiness of the trustee. This constitutes a feedback element.

[1] All German quotations in this text are translated by the authors.

Actions which are administered in connection with internet usage are risky because in such a complex structure, a user cannot control all processes and steps. Before putting trust into the trustees, the user must first perceive and subsequently assess the risk, which constitutes a product of amount of damage and probability of occurrence.

By means of the reference model for IT security analysis [3], an assessment can be carried out (see Figure 1). It is intended to primarily serve developers of security systems. A modified version of this model can be used to assess a usage risk.

Within the first step, the *actual state analysis*, an "inventory of the world including the identification of goods to be protected, of weaknesses in the system, of the involved stakeholders, the underlying conflicts of interest and the interplay of the world's elements among each other" needs to be carried out [3]. In the context at hand the goods are the personal data, the IT systems are the user's devices, the routers and the servers, the stakeholders are the user, the administrators of the networks which host the data traffic, the service providers and also the people unwarrantedly interfering with the process of data exchange (attackers). Conflicts of interest can emerge between what the user expects and what other stakeholders hope for. For example, while the user wants a social network to connect him to other people, the provider hopes that the user reveals as much personal data as possible so that it can be used to present personalized advertisements from the providers partners. Weaknesses in the system can result from faulty hardware and software configuration, from software errors, but also from a disregard of the underlying rules of conduct. These weak points result from human error.

The second step constitutes the *potential assessment*. This is a matter of "listing all threat with their risk, [of] assigning threats to goods worth protecting and exploited weaknesses, and also [of] IT system safety requirements associated with the threats" [3]. Threats as possible results of attacks (e.g. on a users terminal device and the communication process or in the form of a man-in-the-middle-attack) are, for example, external control over the device, data loss through credit card data theft, the unauthorized surveillance of communication or a usage of data published in social networks for initially unintended purposes. The risk always needs to be assessed in relation to the goods which are threatened. In the case of personal data, their threat level depends on the nature of the data and cannot always be quantified. The amount of damage resulting from credit card data theft is more easily quantifiable than the harm done by the involuntary publication of one's relationship status. Weaknesses which can be exploited here are too simple ways of accessing the server (e.g. through weak passwords), insufficiently protected data (open networks) and user behavior (e.g. avoidance of cryptographic procedures). The requirements of privacy protection can be broken down into the following functional safety requirements: confidentiality (i.e. access only for authorized communication partners), earmarking (from appropriate data usage), other parties' trustworthiness and functionally integrated data availability.

The next step is *developing a security concept*, in which „any identified threats are counteracted by sufficiently effective security measures and […] all specified safety requirements are implemented in the form of adequate security measures" [3]. A first security measure is the use of strong passwords, of encryption of e-mail or chat correspondence and the consideration of an encrypted internet communication, whereas this is done with trust in the provider. Furthermore, a user should acquire knowledge of data protection principles and use it to only communicate selected contents and transmit them with caution. This possibility of making security settings and using protective mechanisms is a further security measure, just as the use of alternative search engines or regularly

deleting ones cookies and browser history. The development of a security concept for protecting ones privacy requires explicit data protection competence, i.e. knowledge and experience in relation to dealing with personalized data.

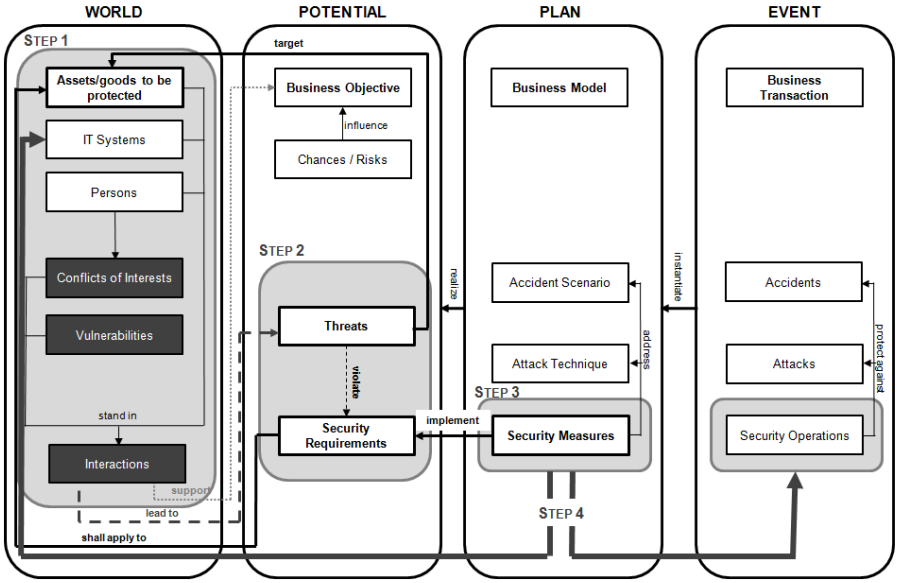

Figure 1. Reference model and taxonomy for conducting an IT security analysis [3]

The last step is *installing a security concept*. Developers can use this as a template for their development project. It serves the user inasmuch as he or she can decide which safety mechanisms of self data protection are present in order to fulfill an adequate security concept and to what extent he is put at risk and whether he can trust the partners he still depends on that point. Here, his or her data protection competence, and particularly the ability to act comes into play.

This enables a user to assess the present risk, to employ adequate protective mechanisms and to evaluate their trustworthiness. This is the data protection competence required to make a decision for or against their use and to shape these, if necessary.

4. FROM RISK EVALUATION IN THE MEDIA COMPETENCE MODEL TO A DATA PROTECTION COMPETENCE MODEL

In [6] and [5], Six and Gimmler introduce a media competence model which, as Gimmler already shows in [1], suitably describes data protection competence to a certain degree. However, a risk evaluation for internet usage is absent. This shall be made up for in the following.

According to [6], media competence describes “the ability to critically, self-determinedly, creatively and responsibly deal with media […]. Competent media behavior needs to be self-determined, reflected upon and self-controlled; moreover, it needs to be oriented towards one’s own issues, purposeful and functional at the same time, but also compatible and appropriate in a personal and social way.” [6] The media competence model characterizes a field of knowledge and a field of abilities and skills, which are summarized as dimensions. The field of knowledge is comprised of the following competences: *orientation knowledge*, *background knowledge*, *conceptual knowledge* and *procedural*

knowledge. The second sector is comprised of the *ability to judge*, *reception and processing competence*, *selection and usage competence and communication competence*.

The following competences from the media competence model play a role in risk assessment (the short definitions by Gimmler in relation to media competence are given in brackets):

Background knowledge ("knowledge of general conditions as well as social and individual importance and effect of media and media use" [1]) is necessary, as each form of internet use is associated with a certain risk. This risk needs to be estimated in order to prevent damage. Data protection measures available to the user are, for example, use of alternative software, alternative search engines, the use of data protection software tools and the personal decision about the disclosure of personal data. This dimension further complemented by knowledge about data protection principles and their importance as well as their application, since they play a role in risk assessment. Thus, background knowledge is required for the actual state analysis, the potential assessment and the development of the security concept based on the reference model.

Self data protection requires *orientation knowledge* ("knowledge of media and media services, their functional usability, technical requirements and the specific requirements for the users" [1]), because on the one hand, knowledge of the services and their functional usability is required (e.g. software tools which prevent tracking through third party cookies) and on the other hand, the technical requirements and specific requirements are specified for the user. The user knows the services and employs them according to the situation at hand. Furthermore, he or she knows of ways to make new information accessible. This orientation knowledge is required to move from the actual state analysis to the development of the security concept.

The *ability to judge* („ability and skill to form an opinion about media services and their development as well as one's own way of use" [1]) is a very important ability. In the definition given above, however, it is too narrowly defined. Knowing and following the development of services is important, but a user involved in risk assessment must be able to form an opinion without any such services at hand. The formation of trust plays a decisive role here. Based on the verdict, the user either accepts of rejects the service. According to the reference model, the ability to judge is incorporated into the actual state analysis, the potential assessment and the development of the security concept.

Through *selection and usage competence* ("the ability to choose and use media services in a self-determined, goal-oriented and reflected way" [1]), the user achieves a self-determined, goal-oriented and reflected choice and usage of internet services. In risky situations the user decides whether or not to take certain risk (based on his or her ability to judge). By making suitable choices concerning protective mechanisms, he or she can minimize the risk. Thus, he or she requires selection and usage competence in the development phases of a security concept and finally in the application phases.

Table 1. Comparison of media competence and reference model

Competence	Steps in reference model for IT security analysis
background knowledge and orientation knowledge and ability to judge	• actual state analysis • potential assessment • development of the security concept
selection and usage competence	• development of the security concept • application phases

When applied to the selected dimensions of the media competence model, the risk interpretation leads to an extension of the model, which can be regarded as a data protection competence model. Data protection competence can be understood as the ability to recognize and assess present risks and to derive action strategies and protective mechanisms. This can take the form of an application or an avoidance of tools and basic settings.

An important application of the data protection competence model will be, for further research, the measurement of students' competence and, as a result of such a survey, didactically justified recommendations for education on internet privacy in school.

Here are examples for questions to measure existing competences of students with attribution to the four relevant dimensions of the data protection competence model. *Background knowledge* will be surveyed by testing factual knowledge about legal requirements, about the existence and functioning of tools and about the technical behavior of laptops and mobiles that are connected to the internet. *Orientation knowledge* will be identified by questions on the availability of tools and settings, by prompting the ability to install tools, to define settings and to be aware of data that users should not publish. The *ability to judge* will be enquired by asking for arguments about the balance of privacy versus security, about the balance between privacy and social publicity, about the political dimension of whistle blowing, and about the opinion on illegal and legal data retrieval. The *selection and usage competence* can be identified by questions about action alternatives, such as the choice between different mobile operation systems ("advantages and disadvantages of Android versus iOS"), the alternative of using extra tools (like cookies and script blockers) or better only application settings (as those offered by Firefox, for example), as well as about the alternative between publication in social media or keeping certain data silent.

All questions will have a meaning for more than only one dimension, like, for example, the question about the refraining from data publication, which has a meaning for the *orientation knowledge* and for the *selection and usage competence*. Therefore, it will be important for the quality of the survey, to give the questions appropriate weights for the dimensions in order to achieve a didactically well-structured picture of the status of data protection competences in our schools.

5. SUMMARY: OUTLOOK FOR AN EMPIRICAL STUDY

In conjunction with data protection, internet use is always characterized by the conscious application of self data protection within the realms of consciously applied system data protection, as well as the competent consideration of remaining risks. This consideration is never simple since many parties (internet provider, software producer, service providers) contribute to the process and the user needs to put his trust in them, based on parties' competence, benevolence and integrity.

Six and Gimmler's media competence model provides partial competences demonstrating aspects of data protection. However, considerations concerning risk assessment are not included. Thus, the model was expanded to a data protection competence model including risk assessment through selected dimensions.

This model's validity is to be examined and applied by further research. The plan is to conduct a survey on risk assessment (with emphasis on privacy protection) amongst students, based on a template of the model. The survey will reveal deficiencies in the current curricula in schools, most probably with respect to all competence dimensions. However, the survey shall show which dimensions have the greatest need for improvement. Therefore, the data thus acquired is then used to develop concrete recommendations for lesson contents.

6. REFERENCES

[1] Gimmler, R. 2012. Medienkompetenz und Datenschutzkompetenz in der Schule. *DuD* 36, 2, 110–116.

[2] Grimm, R. and Bräunlich, K. 2015. Vertrauen und Privatheit. Anwendung des Referenzmodells für Vertrauen auf die Prinzipien des Datenschutzes. *DuD* 39, 5, 289–294.

[3] Grimm, R., Simić-Draws, D., Bräunlich, K., Kasten, A., and Meletiadou, A. 2016. Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. *Informatik Spektrum* 39, 1, 2–20.

[4] Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. An Integrative Model of Organizational Trust. *Academy of Management Review* 20, 3, 709–734.

[5] Six, U. and Gimmler, R. 2013. Medienkompetenz im schulischen Kontext. In *Kommunikation in der Schule*, I. Vogel, Ed. UTB 3649 : Schulpädagogik. UTB, Stuttgart, 96–117.

[6] Six, U., Gleich, U., and Gimmler, R., Eds. 2007. *Kommunikationspsychologie -- Medienpsychologie*. *Lehrbuch*. BeltzPVU, Weinheim.

7. ACKNOWLEDGEMENT

Thanks to Johannes Thielen, student of the CS faculty, for his profitable discussions while writing this paper.

Bisher erschienen (seit 2012)

Davor erschienene Arbeitsberichte, siehe

http://www.uni-koblenz-landau.de/koblenz/fb4/forschung/publications/Reports

Arbeitsberichte aus dem Fachbereich Informatik

Alexander Hug, Rüdiger Grimm, Extension of a didactic competence model by privacy risk, Arbeitsberichte aus dem Fachbereich Informatik 5/2016

Rebecca Bindarra, Lara Fiedler, Nico Merten, Sara West, Paulina Wojciechowska, IT-Sicherheitsanalyse von Geschäftsprozessen am Beispiel der Anwendungen „Kommunalwahlen“ und „Geldauszahlung am Geldautomaten“, Arbeitsberichte aus dem Fachbereich Informatik 4/2016

Heinrich Hartmann, Tim Wambach, Maximilian Meffert, Rüdiger Grimm, A Privacy Aware Mobile Sensor Application, Arbeitsberichte aus dem Fachbereich Informatik 3/2016

Katharina Bräunlich, Rüdiger Grimm, Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl, Arbeitsberichte aus dem Fachbereich Informatik 2/2016

Sebastian Eberz, Mario Schaarschmidt, Stefan Ivens, Harald von Korflesch, Arbeitgeberreputation und Mitarbeiterverhalten in sozialen Netzwerken: Was treibt Social Media Nutzerverhalten im Unternehmenskontext? Arbeitsberichte aus dem Fachbereich Informatik 1/2016

Mario Schaarschmidt, Stefan Ivens, Dirk Homscheid, Pascal Bilo, Crowdsourcing for Survey Research: Where Amazon Mechanical Turks deviates from conventional survey methods, Arbeitsberichte aus dem Fachbereich Informatik 1/2015

Verena Hausmann, Susan P. Williams, Categorising Social Media Business, Arbeitsberichte aus dem Fachbereich Informatik 4/2014

Christian Meininger, Dorothée Zerwas, Harald von Korflesch, Matthias Bertram, Entwicklung eines ganzheitlichen Modells der Absorptive Capacity, Arbeitsberichte aus dem Fachbereich Informatik 3/2014

Felix Schwagereit, Thomas Gottron, Steffen Staab, Micro Modelling of User Perception and Generation Processes for Macro Level Predictions in Online Communities, Arbeitsberichte aus dem Fachbereich Informatik 2/2014

Johann Schaible, Thomas Gottron, Ansgar Scherp, Extended Description oft he Survey on Common Strategies of Vocabulary Reuse in Linked Open Data Modelling, Arbeitsberichte aus dem Fachbereich Informatik 1/2014

Ulrich Furbach, Claudia Schon, Sementically Guided Evolution of SHI ABoxes, Arbeitsberichte aus dem Fachbereich Informatik 4/2013

Andreas Kasten, Ansgar Scherp, Iterative Signing of RDF(S) Graphs, Named Graphs, and OWL Graphs: Formalization and Application, Arbeitsberichte aus dem Fachbereich Informatik 3/2013

Thomas Gottron, Johann Schaible, Stefan Scheglmann, Ansgar Scherp, LOVER: Support for Modeling Data Using Linked Open Vocabularies, Arbeitsberichte aus dem Fachbereich Informatik 2/2013

Markus Bender, E-Hyper Tableaux with Distinct Objects Identifiers, Arbeitsberichte aus dem Fachbereich Informatik 1/2013

Kurt Lautenbach, Kerstin Susewind, Probability Propagation Nets and Duality, Arbeitsberichte aus dem Fachbereich Informatik 11/2012

Kurt Lautenbach, Kerstin Susewind, Applying Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 10/2012

Kurt Lautenbach, The Quaternality of Simulation: An Event/Non-Event Approach, Arbeitsberichte aus dem Fachbereich Informatik 9/2012

Horst Kutsch, Matthias Bertram, Harald F.O. von Kortzfleisch, Entwicklung eines Dienstleistungsproduktivitätsmodells (DLPMM) am Beispiel von B2b Software-Customizing, Fachbereich Informatik 8/2012

Rüdiger Grimm, Jean-Noël Colin, Virtual Goods + ODRL 2012, Arbeitsberichte aus dem Fachbereich Informatik 7/2012

Ansgar Scherp, Thomas Gottron, Malte Knauf, Stefan Scheglmann, Explicit and Implicit Schema Information on the Linked Open Data Cloud: Joined Forces or Antagonists? Arbeitsberichte aus dem Fachbereich Informatik 6/2012

Harald von Kortzfleisch, Ilias Mokanis, Dorothée Zerwas, Introducing Entrepreneurial Design Thinking, Arbeitsberichte aus dem Fachbereich Informatik 5/2012

Ansgar Scherp, Daniel Eißing, Carsten Saathoff, Integrating Multimedia Metadata Standarts and Metadata Formats with the Multimedia Metadata Ontology: Method and Examples, Arbeitsberichte aus dem Fachbereich Informatik 4/2012

Martin Surrey,Björn Lilge, Ludwig Paulsen, Marco Wolf, Markus Aldenhövel, Mike Reuthel, Roland Diehl, Integration von CRM-Systemen mit Kollaborations-Systemen am Beispiel von DocHouse und Lotus Quickr, Arbeitsberichte aus dem Fachbereich Informatik 3/2012

Martin Surrey, Roland Diehl, DOCHOUSE: Opportunity Management im Partnerkanal (IBM Lotus Quickr), Arbeitsberichte aus dem Fachbereich Informatik 2/2012

Mark Schneider, Ansgar Scherp, Comparing a Grid-based vs. List-based Approach for Faceted Search of Social Media Data on Mobile Devices, Arbeitsberichte aus dem Fachbereich Informatik 1/2012