Understanding Users' Perception Toward Sharing Personal Health Information

Sadegh Torabi
University of British Columbia
Vancouver, BC
sadeq@ece.ubc.ca

ABSTRACT

Sharing personal information in general and health related information in specific has been a topic of discussion for the past years. While sharing information could have its benefits, people have shown different levels of concern when it comes to sharing their personal health information (PHI) with others. For example, someone might be willing to hand over personal information such as name, age, and place of birth to an online blogging website, while showing much more concerns when it comes to others. Interestingly, some sensitive health related information might be easily shared with an unknown doctor at a hospital, whereas not shared with the person's closest friend or even parents. In this survey research paper, we aim to investigate existing literature to better understand the different aspects related to users' perception toward sharing personal health information, specially on online platforms such as web pages and online social networks. We will eventually point out main findings and provide suggestion that could be used to fill existing gaps.

Keywords

Online social networks, personal health information, information de-anonymization, illusion of control, privacy enhancement tools

1. INTRODUCTION

Personal health information (PHI), also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a health care professional to identify an individual and determine appropriate care [4]. Also, any oral or recorded form of identifying information relating mental or physical health of individuals, healthcare service plan and payments, organ donations, and individual identifying health numbers are all considered as PHI [2]. Personal health information is different from personal health record (PHR), which is usually defined as records of health related data that are stored and maintained by the patient himself [30, 3].

Sharing health related information is a subset of sharing personal information. Many studies have been conducted toward identifying concerns related to sharing personal data and protecting them, specially on online websites and social networks. In general, when considering health related information as a subset of personal information, findings from literature could be applied to the context of protecting health related information as well. However, users have shown different behaviour and concerns regarding sharing their health related information with others. For example, sharing a sexual related disease on a public forum for the sake of getting answers or with the family doctor might be totally accepted by some people while being considered awkward if shared with friends or family members. Therefore, we believe that health related information must be treated with extra caution, considering both security aspects along with users' privacy related concerns before being shared.

Different rules and legislation formed by governments to protect individual and their PHI. For example, under the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) [1], covered entities, which include health care providers, insurers and their business associates, are limited in the types of PHI they can collect from individuals, share with other organizations or use in marketing communications. In addition, PHI must be provided to patients if requested, preferably in an electronic format, and cannot be sold unless it is being used for public health activities, research, treatment, services rendered or the merger/acquisition of a HIPAA covered entity. Similarly, the Canadian Personal Health Information Protection Act, 2004 (PHIPA), controls the collection and disclosure of PHI by forcing physician to explicitly get the consent of the individual unless otherwise stated by law [2]. In specific circumstances, a "circle of care" is defined, which is defined by a number of involved parties such as caregivers and physicians that could assume the individual's implicit consent in specific cases and therefore share his information without direct consent [11]. This process must be carefully considered and could be only approved under circumstances mentioned in PHIPA. It is clearly observed that rules and regulations are established for protecting users' data, yet when it comes to practice, specially when using online services, users may face different set of challenges toward maintaining their information privacy.

In this study, we identify some of the research points and

try to classify existing literature respectively. Due to the complexity and variety of existing threats and issues related to sharing personal data and PHI, we do look specifically after studies related to sharing data on online platforms such as websites and online social networks. The study is aimed to provide a clear understanding about the current level of knowledge in regard with sharing users' PHI and maintaining its privacy. The study is also made mainly to investigate existing literature to understand users' perception toward sharing PHI and understanding privacy related issues.

The rest of the paper is designed as following: in section 2, main research points in regard to sharing PHI is going to be presented and discussed in details. In sections 3, future work and suggested studies will be proposed, followed by the conclusion section at the end.

2. DISCUSSION

In the following sections, we will present in more details results of the applied broad literature survey by classifying the research to main points. These points are classified considering the main stakeholders of the study: individual PHI owners, involved organizations and individual professionals such as doctors and hospitals, governments and law enforcements, online system designers and operators. We did have this specific classification due to the wide use of online systems such as websites and online social networks and their emerging role in the users' PHI sharing process. Also, we consider personal health information as important as other personally identifiable information, and therefore, any concern would be applied to both PHI and PII. We specified 5 research points as following: *Health Related Data Protection and Information De-anonymization*, *Privacy and Sharing Information in Online Platforms*, *User Control Over Publication*, *Privacy Enhancement Tools*, and finally *User Attitude and Behaviour*.

2.1 Health Related Data Protection and Information De-anonymization

Health related data protection is a subset of the overall data protection theme. Due to the significant value and importance of health related data, along with users concerns about who gets access to the data and how, protecting health related data and records agains various threats has been a hot topic in the past decade. Several threats exists when it comes to data protection, starting with physical threats to data centers, storage media and connected devices, to all other different cyber attacks. Data protection in general, and personal health related data in specific tend to have significant importance for individuals and organization and therefore, protecting them must be a priority. When it comes to publishing users' data for the purpose of research, information privacy is considered as a main concern. Although it is essential for researchers to use these information to enhance knowledge and possibly produce benefits for the health care society, information privacy must not be sacrificed with. Therefore, it has been assured that users' information privacy must be considered and as a result, related data must not be published unless anonymized under a set of standards.

Information de-anonymization is a well addressed issue when it comes to personal data anonymization. Data anonymization is the process of manipulating PII and replacing them with some identifiers for the sake of preserving privacy. Many attacks have been identified and discussed toward reverse engineering the anonymized data. In these attacks, researchers have shown that information could be de-anonymized by several means specially when some parts of the actual data is known to an adversary.

A number of de-identification or anonymization techniques have been applied by well known health care organization toward making anonymized copies of patients data that would be publicly available for researchers. El-emam and his colleagues at the "Electronic Health Information Laboratory[1]" have published a number of studies that aim toward large dataset de-identification (anonymization) and re-identification (de-anonymization), and described attacks and counter attacks, and showed how each one could be effective in certain situations [25, 20, 15]. He recently published an article that shows how large sets of medical records could be anonymized and publicly available for research purposes by achieving some level of anonymization acceptable by US Health Insurance Portability and Accountability (HIPPA) [14]. However, he also described attacks that could reveal approximately 5.8% of the latest published long term dataset by Heritage Health Prize (HHP)[2], even when these data sets were claimed to meet the HIPPA requirements that specifies the risks of re-identification to be less than 0.05% [14].

Another set of de-anonymization attacks have been implemented on anonymized copies of online social networks. Again, and for the sake of research and its significant benefits, some online social networks would try to anonymize subsets of its existing data represented by its users and their interpersonal ties, communication, demographics and etc. and provide the anonymized copy to researchers. These online social network de-anonymization have proven to be weak and therefore, several attacks have been proposed to provide insight about existing threats and suggest solutions [7, 34]. For example, in online social networks such as Twitter, attackers where able to de-anonymize a copy of the network by creating few known links that could be identified after the network was anonymized. Other attacks only relied on the network topology without the need to create dummy nodes and sybil with an error rate of 12% only [26]. Wondracek et al have shown in [33] that online social network users could be identified by knowing their group memberships (groups they belong to), simply by exploiting these data from the online social network website.

Many studies have been published to prove that information de-anonymization is not a feasible technique. In fact, some studies where even more pessimistic [27], requiring governments to immediately act and save the broken promises by means of new privacy protecting rules and regulations. In reality, we notice an accumulative amount of attention toward preserving users' information privacy by several means. Although information anonymization was proved to be not completely effective (100% anonymization), it has been ar-

[1]University of Ottawa, http://www.ehealthinformation.ca

[2]HHP is a global data mining competition to predict, by using claims data, the number of days patients will be hospitalized in a subsequent year

gued that the newly applied standards and techniques would assure an acceptable level of information anonymization specially in large scale data sets. In case of online social network anonymization, so much has to be done. It might be due to the ungoverned operations and structure of the existing social networks, or due to the lack of related rules and legislations. The future is promising and people are becoming more aware about their privacy and therefore, we suspect that within the coming years, this issue would get more attention and reaches its equilibrium state.

2.2 Privacy and Sharing Information in Online Platforms

This section is related to users' perception toward sharing and publishing health related information. Sharing health related data is considered as a subset of sharing personal data issues. Personal data may include Personal Identifying Information PII and other types of information such as personal health information PHI. Users have shown concerns about how private would they like to have their PHI to be and from whom they are more likely to hide these data. Also, with the large set of online databases and online social networks, the leakage of personal data on online platforms are of users' concern. The question is "does existing online systems appropriately maintain users' information privacy when sharing personal data online?". To answer this question, we will assume that online systems do maintains an adequate level of users information privacy, regardless of the individual practices. This means that users' privacy will be maintained when using these online systems and their personal data will be safe against possible leakage, even if they were benign users with minimum knowledge about privacy related settings (if any). In reality, several attacks have been proposed on a number of online systems, most of them showing privacy breaches existing in the design and structure of used online systems, leading to information leakage. in the following paragraph, we will present a number of these studies briefly without going into details of the implemented attacks since our objective here is to prove that attacks are possible and information leakage is happening rather than how it happens.

Krishnamurthy and Wills have shown that popular online social networks implement default privacy settings that are more likely to be used by most users and which will publicly reveals most of the users' information [21]. They also discussed different means of leakage of PII on online social networks in their later study in 2010 [22]. In another study, the authors have found that while privacy concerns are not clearly presented in the users' ephemeral online activities such as posting and commenting on posts, awareness and familiarity with privacy controls is being observed, which suggests that existing online social networks might have failed in transferring users' privacy concerns into the technical boundary control mechanism [28].

A set of privacy breaches and information leakage on online systems have been identified as a result of the operations of third-party applications, who may implicitly grant access to users' personal data for the purpose of providing a free service or playing an online game [10, 16]. More over, a number of utilization techniques used on some online social networks such as friends suggestion, users' similarity projection, and targeted adds, would result leakage of personal information as described in [24, 29]. Finally, in a totally different study than what mentioned before, Turow et al have showed that the commercial use of the term "Privacy Policy" has strong implications on users' perception toward their privacy protection, leading them to think that the platform would keep their data private [31]. The existence of the legal term would not guarantee any privacy protection and its misleading use should be legally regulated by responsible authorities to avoid privacy leakage.

In a nutshell, it has been shown that online collaboration systems, specially online social networks have not met users' concerns when it comes to privacy control and information leakage prevention [18]. They tend to operate under a certain level of pragmatic and vague privacy controlling mechanism that is insufficient to preserve users' data when connected to online social sites. On the other hand, users' either have little knowledge, or wrong perception about existing threats to their personal data on online social network. More importantly, the free service providers such as online social networks heavily rely in their core structure on gathering and analyzing their users' data and making use of them in targeted adds and other monetary services!

2.3 User Control Over Publication

With the fast growth of online systems, users' information and data are gathered, stored and maintained online through different platforms, and have been available for authorized use in order to facilitate sharing and transferring information in a timely manner. Whether if it is a governmental agency, an educational institute, a physician or simply an online social network, some personally identifiable information (PII) is usually required to maintain user records. Users must provide these information in order to facilitate the use of these online systems and possibly let them create profiles and records for each individual user. At the receiving end, these parties must maintain the security and privacy of the stored data and prevent such information from been disclosed by unauthorized users.

Some service providers require users to have public online profiles that contain some information about the users. These public profiles could be created either by the users or by the online service provider. In both cases, the users only have control over what data to give to the service provider and no control over the published data as soon as it has been publicly available (i.e. they can not control who can see and use their published data and where it could be used). With the existence of mixed public and private profiles, it is difficult to manage anonymity of users data, specially on online social networks, where boundaries are not well defined or understood by the average users and information anonymity could be easily revealed by exploring users' surrounding space in the network [35]. Moreover, researchers have shown that users have misunderstanding about how things work. They think that others are prevented from unauthorized access or usage of their publicly available data simply because they only provided these data to some known service providers and not to the public. Therefore they establish this "illusion of control" over the availability of their published data to third parties, where in fact, these data was collected to create a public profile in the first place!

To conform the "illusion of control" hypothesis, some experiment where implemented and the results showed that users are more concerned to provide their personal data to online service providers when the public profile creation and publishing involves a third party [9]. In the experiments, users where told to provide personal data for the purpose of creating an online public profile for them by their university website. Two conditions existed, both have same outcomes, which is creating and publishing a public profile for the university website. In the first experiment, users have been told that the university will create and publish the data where in the second identical experiment, users have been told that a third party would create the profile on behalf of the university. Results have shown that users show less trust by providing fewer personal information when a third party is involved [9]. They actually feel more compromised with the existence of a third party, confusing the accessibility and publishing of their personal data. In both experiments, accessibility of published data is not controlled by the users, yet the users think they may prevent unauthorized access simply by providing less information.

Another issue regarding control over publication of public profile is raised when dealing with different online social networking platforms, which in some cases have transferred the privacy control fully to the users. On the other hand, the privacy control mechanism implementation is not logically feasible due to the network structure and the utilization techniques used by the network operators, which mainly focus on sharing information. Therefore, users might think that they are tuning their privacy while in fact, what is being published could be indirectly seen and accessed by others. To overcome such dilemma, and as a result of their study in [23], they suggested a collaborative boundary regulation framework for managing privacy on online social networks by means of group negotiation and discussion and then making decisions about managing group privacy. They also classified existing strategies implemented by their participants to and identified the following strategies: Individual and Collaborative, Preventive and Corrective, Mental and Behavioural [23].

People have shown higher level of privacy concern regarding sharing their information with strangers in real life and online social networks. Meanwhile, users have shown less care and sensitivity toward preserving their privacy when captured in the wild, sharing almost everything on online social networks such as Facebook, starting with their PII, and not ending at their physical location, romantic status, personal believes and etc. Why this contradicting behaviour and saying something and doing another thing? Researchers have tried, and still trying to find explanation for this phenomena. Some refer this behaviour to the lack of awareness of privacy implications of sharing personal data on online networks, while others refer to the illusion of control over publication issue [23]. Some explain it as the trade off that leads users to choose between the benefits of using a service over their personal privacy implications. In their study [6], *Acquisti and Gross* have showed that a significant majority of Facebook users are not aware of their profile visibility, or even if they are, they tend to have the ability of control over their privacy by self maintaining their privacy setting, and not considering the actual visibility of their profiles. Also, participants have shown less knowledge about how Facebook is treating their stored data, which could be a sign of overall blindfold trust in the network operators.

2.4 Privacy Enhancement Tools

Several privacy technology tools have been developed and tested for the sake of preserving users' privacy on online platforms. These tools where seeded by works of computer security and cryptography experts. Different tools with different goals have been developed, some used for securing users' stored data, others help securing transferring data, and finally, preserving users private data from unauthorized access when partially published on shared online platforms. These tools are so called "Privacy Enhancement Tools" or PET, which usually aim to preserve users' data privacy with different means [12, 8].

Another set of tools, which are called "Transparency Enhancement Tools" or TET, which are introduced to preserve users' data privacy by evaluating possible threats to users' data on an online system and informing the user about them [32, 19]. TETs might also suggest preemptive moves toward data privacy preserving when it comes to sharing data on online platforms. For example, TET might be used to help users understand how their data would be shared on specific websites, or who would be able to see which part of the data and how would this effect the privacy of the users. Both PETs and TETs are important nowadays specially with the growth of online social networks and the huge number of users who sometimes tend to unconsciously publish their personal data on online networks while not considering the subsequences of their actions.

At the end, one must not think that tools such as PETs and TETs are going to fill the existing privacy protection gap of the online social networks and other online systems. They aim at providing different means of enhancing privacy protection and leveraging current user practices on online collaborative systems and would not guarantee protection of users' data and privacy.

2.5 Users Attitude and Behaviour

In this section, we will go through a number of studies that have been made on users in order to understand their behaviour and attitude toward sharing health related information online. The *Pew Internet and American Life Project* [5], which is a project of the "Pew Research Center", is considered as a reliable source for latest statistics regarding the impact of internet on individuals, communities and healthcare practices (they would also produce statistics in other fields that is not of our interest for this specific study). Based on a survey in September 2010, they specified that 80% of U.S. internet users, whom represent 59% of U.S. adults, look online for health information, while 15% of U.S. adults use their mobile phones to look for health related information [17]. When people have health related questions, the default answer is : "I don't know, but I can try to find out", according to [17]. This implies that people most likely would go and search the internet to get quick answers to their health related questions. Table 1 shows a summery of the finding and statistics stated by Pew Internet [17].

On the other hand, studies have shown that an increasing

Table 1: Users online behaviour with respect to health related information

% of U.S. Adults	Online Behaviour
15%	used the internet to look for health related information
15%	used their mobiles to look for health related information online
25%	read someone else's comments or experience about health related information on online websites, news groups, or blogs
18%	consulted online reviews of particular drugs or medical treatments
13%	went online to search for others who share similar chronic and rare condition disease
20%	tracked their weight, diet and exercise routine or other health indicators online
4%	posted comments, questions or information regarding their health online
3%	posted their experience with a particular drug or medical treatment

Table 2: Online social network users behaviour with respect to sharing health related information

% Online Social Network Users	Online Behaviour
23%	have followed their friends' personal health experience or updates on site
17%	have used social networking sites to remember or memorialize other people who suffered from a certain health condition
15%	have got any health information on the sites

number of users are using Emails and online social networks such as Facebook to share their health experience [13]. They study made by Lucid Marketing and HeardItFromAMom.com have shown that 84% of Moms often share health related information via email and 69% often share via Facebook. Email and Facebook are also the places where they most often hear recent news (email 83% and Facebook 76%). As shown in Table 2, similar results have published by Pew research that confirms the importance of social media in healthcare.

Using online websites, blogs and online social networks for the purpose of gathering and sharing health related information has been significantly increased during the past years, and yet does not seem to stop. This could be a result of the fast and on click access to a bank of online information, that in many cases would help the users find their answers in a timely manner. It has become more than sharing information, it turned to an educational process. People go online, share information, discuss with others, compare to their experience, and possibly post their own experience, whether negative or positive. Availability of a variety of resources, instant access, and daily use of online social networks could be other reasons behind the emerging number of users that would share or surf health related information on online platforms.

3. FUTURE WORK

The study has resulted pointing out several points related to sharing health related data on online platforms. These points have been discussed and presented in the previous sections. However, a number of important aspects have been missing from the literature or been weakly addressed. For example, the lack of understanding about what users actually would like to experience when sharing their data on an online social network or website. Other examples could be listed as following: users information privacy concerns when sharing data online; how and by whom would users want their data to be viewed, processed and gathered; what level of anonymity is required by the users; how usable and secure is the online platform and etc.

We suggest a large scale user study to be done in order to identify users' actual privacy concerns when it comes to sharing health related information online. Staring by interviewing users to identify their needs and requirements, both in terms of privacy and usability issues. We believe that it is not right to transfer the privacy protection process to the user side rather than to be maintained by the online systems themselves. Users are not designers of the system and therefore, they will never fully understand the implementation and possibly make wrong assumptions as well. To avoid that, the system must be design around the user, considering all (most) of his needs, concerns and limitations. Next step is designing low fidelity prototypes and testing it on users to get feedback and then move to higher fidelity prototypes. System evaluation is an essential step that must be considered all the way while doing this user study. Finally, the prototype must be tested on a broader range of people in order to validate its usefulness and effectiveness in terms meeting users' requirements and needs.

4. CONCLUSIONS

In this study, we have shown that online platforms that are widely used by people to share their personal health information are vulnerable toward several types of attacks. These online websites and social networks suffer from the following vulnerabilities: Information de-anonymization, information leakage through privacy breaches, information harvesting by third-party application, and lack of proper privacy controls. Although some technical aspects like data anonymizations have been addressed in more detail, other technical and privacy related aspects have not reached an acceptable level in practice. It might be due to the commercial nature and collaborative structure of the free service providers such as online social networks, or due to the loose boundary regulation mechanism provided by online application developers.

However, the fact is that online platform users' needs and concerns are ignored when designing such online collaborative systems. Now, online social networks and websites have

millions of users in some cases, and when privacy concerns arise, the system developers will possibly look for patching solutions, that would not be helpful in most cases. On the other hand, because of the high demand and daily use of its participants, it is difficult for the system operators to drop their services and redesign the whole system, due to the reputation and commercial damage that they would receive. Therefore, we observe clearly how privacy concerns are sacrificed for the purpose of other benefits.

At the end, we suggest that users' needs must be considered and their privacy concerns must be used as the basis for designing any collaborative online system that will be used to share personal information in the future. The result must be a user friendly system, that could be used by different people with different capabilities, with a user centric design that meets the users' needs and requirements.

5. REFERENCES

[1] Health insurance portability and accountability act of 1996. US PUBLIC LAW 104 - 191, 1996.

[2] Confidentiality of personal health information. COLLEGE OF PHYSICIANS AND SURGEONS OF ONTARIO, POLICY STATEMENT 8-05, April 2006.

[3] Defining key health information technology terms. The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology, April 2008.

[4] Personal health information (phi), September 2010.

[5] www.pewinternet.org.

[6] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Proceedings from Privacy Enhancing Technologies Workshop*, 2006.

[7] L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography. In *WWW 2007*, Banf, ALberta, Canada, May 2007. ACM.

[8] J. Becker and H. Chen. Measuring privacy risk in online social networks. In *Web 2.0 Security and Privacy 2009*, 2009.

[9] L. Brandimarte. Privacy concerns and information disclosure: An illusion of control hypothesis. Draft - H. John Heinz III College – School of Public Policy and Management Carnegie Mellon University, April 2009.

[10] J. Calandrino, A. Kilzer, A. Narayanan, E. Felten, and V. Shmatikov. "you might also like:" privacy risks of collaborative filtering. In *2011 IEEE Symposium on Security and Privacy*, pages 231–246, 2011.

[11] A. Cavoukian. Circle of care: Sharing personal health information for health-care purposes. Information and Privacy Commissioner, Ontario, Canada, September 2009.

[12] G. Danezis and S. Gurses. A critical review of 10 years of privacy technology. In *Proceedings of Surveillance Cultures: A Global Surveillance Society*, April 2010.

[13] J. Dunham. Marketing to moms: Sharing healthcare info on facebook. The Lipstick Economy, August 2011.

[14] K. El Emam, L. Arbuckle, G. Koru, B. Eze, L. Gaudette, E. Neri, S. Rose, J. Howard, and J. Gluck. De-identification methods for open health data: The case of the heritage health prize claims dataset. *Journal of Medical Internet Research*, 14(1), 2012.

[15] K. El Emam, E. Jonker, L. Arbuckle, and B. Malin. A systematic review of re-identification attacks on health data. *PLoS ONE*, 6(12), 2011.

[16] A. Felt and D. Evans. Privacy protection for social networking platforms. Workshop on Web 2.0 Security and Privacy. Oakland, CA, May 2008.

[17] S. Fox. Pew internet: Health. Highlights of the Pew Internet Project's research related to health and health care, March 2012.

[18] R. Gross and A. Acquisti. Information revelation and privacy in online social networks (the facebook case). In *In Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 2005.

[19] P. I. A. W. Group. Managing information privacy and security in healthcare privacy impact assessment guide. Healthcare Information and Management Systems Society, July 2008.

[20] P. Kosseim and K. El Emam. Privacy interests in prescription data. *IEEE Security and Privacy*, 2009.

[21] B. Krishnamurthi and C. E. Wills. Characterizing privacy in online social networks. 2008.

[22] B. Krishnamurthi and C. E. Wills. On the leakage of personally identifiable information via online social networks. 2010.

[23] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen. We're in it together: Interpersonal management of disclosure in social network services. In *CHI 2011 session privacy*, Vancouver BC, 2011.

[24] A. Lipowicz. Facebook timeline could reveal your hidden connections.

[25] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008.

[26] A. Narayanan and V. Shmatikov. De-anonymizing social networks. IEEE Security and Privacy '09, 2009.

[27] P. Ohm. Broken promises of privacy: Responding to the surprising failure of anonymization. Technical report, University of Colorado Law School, 2009.

[28] B. Reynolds, J. Venkatanathan, J. Gonçalves, and V. Kostakos. Sharing ephemeral information in online social networks: Privacy perceptions and behaviours. In *INTERACT (3)*, volume 6948, pages 204–215, 2011.

[29] J. Staddon. Finding "hidden" connections on linkedin an argument for more pragmatic social network privacy, Novemer 2009.

[30] P. Tang, J. Ash, D. Bates, M. Overhage, and D. Sands. Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, 13(2):121–126, April 2006.

[31] J. Turow, C. Hoofnagle, D. Mulligan, N. Good, and J. Grossklags. The federal trade commission and consumer privacy in the coming decade, 2007.

[32] E. Wästlund and S. Fischer-Hübner. End user transparency tools: Ui prototypes. Unabhängiges Landeszentrum für Datenschutz, Karlstads Universitet, and Center for Usability Research and Engineering, June 2010.

[33] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 223 – 238, Oakland, CA, USA, May 2010.

[34] WP7. Behavioural biometric profiling and transparency enhancing tools. Technical report, Future of Identity in the Information Society, 2004.

[35] E. Zheleva and L. Getoor. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In *18th International World Wide Web Conference*, 2009.