Computer security

Did you change your social network setting after these readings? How can social networks disclose health information? What are the possible negativeconsequences of this? With the review of the provided literature the fact that social networking and the pleasure that one derives from being a part of a virtual community might come at a price is brought to light. To update your privacy settings or to at the very least review the privacy policies of social communities that you are members of is a necessary precaution. This is mainly due to the fact that although online social networks offer exciting new opportunities for interaction and communication but due to their vast membership and easily identifiable data they open up a window of highly personal information revelation behavior of millions of people to friends as well as complete strangers. Millions of people around the world use social networks like Friendster, MySpace, Facebook to communicate, find friends, dates and jobs – and in doing so they wittingly reveal highly personal information about themselves to everyone. With the burst in advertising of these social networks most of them now days encourage users to reveal highly personal information. This includes their dates of birth, cell phone numbers, addresses and highly confidential health information. The weak structural design of social networks in terms of security and access controls is cleverly concealed by a false sense of security which is aided by the current changing cultural trends; familiarity and confidence in digital technologies, lack o f exposure of personal data by others, all play a unprecedented phenomenon of information revelation. Research reveals that a majority of users of these networks are not particularly concerned for their privacy and this is largely due to their lack of awareness of the actual exposure and visibility of information that they so

comfortably publish their personal data on working profiles that center around key questions regarding a person’s views, current health and perceptions on various issues. The reader’s willingness to share this information on networks like facebook is highly dependant on supposedly granular and powerful control on privacy which is in reality very permeable and easily accessible. These varying levels of privacy related advertising that social networks target by taking into account heterogeneous privacy preferences in the user population, and the temporal dynamics of privacy concerns all fall into the proposed model the privacy communication game. This brings to our attention the obvious privacy concerns of members of various social networks and the social network’s strategy that attempts to overcome these concerns and optimize interaction within the group. Privacy policy, a basic legally binding contract between the social network operator and its users, is the only primary source that a prospective user can rely on to give informed consent for data collection as is required by the EU; which makes a posting and access of these documents both technically and linguistically critical. Also Security Measure such as the use of TLS Encryption and authentication that aims to enforce these privacy concerns is critical for the functioning of these social networks. However an evaluation of the adoption of policies conforming to enable these measures through a P3P format shows a significantly low adoption of an implementation of these policies. The basic infrastructure of these policies exists but the implementation is weak and highly flawed with sites like Facebook consisting of an incorrect policy element name ‘ HONK’ crafted specifically to mock P3P displaying browsers. Furthermore the fact that experimental economics has long suggested that user’s privacy related decision making is systematically

distorted because of limited information provided to them which leads them to display private information without really knowing its easy access implications. The incentive here for social networks to limit privacy salience as part of their privacy communication game to combat aggressive existing competition. The negative consequences are, besides having a lot of strangers as well as friends know intimate details of your life, health and daily schedule, the fact that these social networks store vast amount of detailed information about millions of users. This combined with the fact that their privacy controls are structurally flawed and costs of mining and storing data are declining which makes the information provided on these ostensibly private social networks, effectively, public data. That could interest marketers, employers, national and foreign security agencies that have incentives and the ability to seek out these confidential details.