Assignment 1 - Social Web

Arthur-Ervin Avramiea
2517642
a.e.avramiea@student.vu.nl

Mihnea Dobrescu-Balaur

Mihai Gramada

1. MAIN ISSUES RELATED TO PRIVACY ON THE SOCIAL WEB

One of the main advantages of allowing an online entity to store personal information is web personalization. Access to a person's interests allows the website to provide useful recommendations, while information about how an individual uses an website may help the service provider to tune the website behavior for the individuals' needs. Nonetheless, users are concerned about their own privacy, and the ways in which their personal information is used. The users' privacy concerns have an impact on how do individuals utilize website which personalize their content, and what information do they share[3]. Fig. 1 reflects the concepts which revolve around the idea of privacy-enhanced personalization.

The status of an individual was shown to have an influence on his privacy concerns. As he advances in age,

Website trust

Privacy-enhancing technologies

Rules

—-

The main concern of todays Social Web users is the fear of third parties accessing their data. To avoid this, users tend to falsify their data and reduce the amount of information they share online. Besides data leaks, users are also afraid of third party cookies that help build targeted ad profiles and spam e-mail. While falsifying online data or not sharing any at all can work for some people, this is not a productive solution for the future of the Social Web, since false data or no data at all are no good.

To improve this situation, Web properties have to address concerns about data misuse. The most common way to do this for a website, is to have a privacy policy - a document that states what can the people running the website do with the users data and what they cant do. Many websites have adopted this approach, but it turns out that while the idea is good, the implementation could be improved.

Studies[4] have shown that the language used in current privacy policies is rather targeted at lawyers than at laymen. More so, the words used are chosen in such a way that the policies state that third parties will have access to the users data, without raising any alarms. This is accomplished through the use of negations and modal verbs. Also, all the implications described are shown in a way that implies that all happens based on the users choice (not without your permission).

Irene Pollach notes[5] that it seems that the real goal of privacy policies is to mitigate privacy litigations in court, rather than expressing clearly to the users what happens with their data. In order for privacy policies to ease the users worries, they have to be expressed in a more easy to understand, succinct way - less lawyer-specific words, less sugarcoating and less uncertainty (we occasionally []).

Another way to build[2] user trust is to use opt-in/out facilities. This gives users the thought that they are in control of of what they share or not. Even more, some websites allow users to completely delete their user profile, which increases the level of trust even more. However, privacy policies sometimes state that deleting an user profile just means that it wont be publicly accessible anymore, the data remaining available to the Web property owner.

2. INITIATIVES INTENTIONS

The Anti-Counterfeiting Trade Agreement (ACTA) is a multinational treaty which consists of a body of regulations built with the purpose of enforcing intellectual property(IP) rights [7]. It establishes cooperation mech-

anisms between the adhering countries, that facilitate the enforcement of IP rights across borders. In this process, law enforcement authorities act on behalf of the IP right holders, and cooperate with them in securing IP, and hence protecting the profits of private businesses, at the expense of taxpayer money[1]. However, the disadvantages for the general public are not limited to this financial aspect.

Although the stated aim of ACTA is to regulate large-scale counterfeiting and piracy activities done for commercial purposes, it also criminalizes IP rights infringements of regular citizens, even when the infringement did not involve any financial gain.

In what involves copyright infringement on the online medium, it requires online service providers - be it ISPs, search engines, websites, to take down infringing content and provide the law enforcement agencies with the personal details of the infringer. First of all, this opens the door to abuses of the privacy rights of individuals, within the legislation of one country. Second of all, personal information may be sent across the border, at the request of an IP rights holder. Privacy legislation differs between countries and the personal information may not be treated with the same protection as the information crosses the borders.

Due to pressure from some of the parties involved, and from the general public, ACTA was modified so as to allow countries to protect its citizens. However, these stipulations are merely optional, and do not provide with safeguards against abuses of citizen's privacy rights [6].

— The issues of privacy and IP rights enforcement are tightly related to the function of social web. The amount of information that defines the activity and identity of an individual, and which is located online, has increased with the rise of social networks. This makes the individual more vulnerable to abuses of his privacy rights. Moreover, the individual finds it natural to share on the web content which he has bought, in a similar way in which he does it in real-life. For the purpose of protecting the profits of private businesses, ACTA regulates the free flow of information that goes on in online medium with stricter rules that would apply in offline social connections, in an age in which an important part of the social interactions takes place online.

* the government would have access to any kind of data, with no warrant and no way of knowing after the fact * 603 government agencies would have access to the data (only NSA atm) * even local law enforcement will have access to the data and they could use it in an investigation * privacy policies become less relevant

The supporters claim the following as advantages: * shorter delays in finding cyber terrorists * real terrorists * easy way of detecting (and stopping?) online piracy

Net neutrality states that all data on the Internet should be treated equally, regardless of equipment and users. A bill like CISPA endangers net neutrality, since the data thats stored on US servers becomes easily accessible to the government. This means that there would be different terms on who can access what data, depending on where that data is store

3. WHAT WOULD BE DIFFERENT IF IN PLACE

Some of the facebook users share content that they have paid for with other reasons. SOPA/PIPA/ACTA require the online service providers to take down the content that infringes copyright. If a user continues the infringement, his account may be suspended, and that friend may not appear anymore in the friends' graph.

Through the privacy settings, the user has control over what information is available to which users. However, with the proposed regulations in place, third parties would have access to the individuals' information, regardless of his privacy settings - either for identifying an infringer of IP rights (SOPA/PIPA, ACTA), or for the use of the intelligence community (CISPA). In the optional task of exercise 4 of the assignment we were asked to use the label the individuals in the mutual friends graph with their location. If a user chooses not to share their location, we would not be able to see that information on our graph. However, organizations favored by CISPA would have complete access to all the information, and would have a more complete version of the graph.

4. REFERENCES

[1] E. Ayoob. Anti-counterfeiting trade agreement, the. *Cardozo Arts & Ent. LJ*, 28:175, 2010.

[2] D. L. Hoffman, T. P. Novak, and M. A. Peralta. Information privacy in the marketspace: implications for the commercial uses of anonymity on the web. *The Information Society*, 15(2):129–139, 1999.

[3] A. Kobsa. Privacy-enhanced web personalization. In *The adaptive web*, pages 628–670. Springer, 2007.

[4] G. R. Milne and M. J. Culnan. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3):15–29, 2004.

[5] A. Sharma and K. Shrivastava. Privacy implications of applications based on cloud computing for individual and business users: A magazine article. 2009.

[6] A. J. C. Silva. Enforcing intellectual property rights by diminishing privacy: How the anti-counterfeiting trade agreement jeopardizes the right to privacy. *Am. U. Int'l L. Rev.*, 26:601, 2010.

[7] Wikipedia. Anti-counterfeiting trade agreement, 2014. [Online; accessed 19-February-2014].

APPENDIX

A. FIGURES

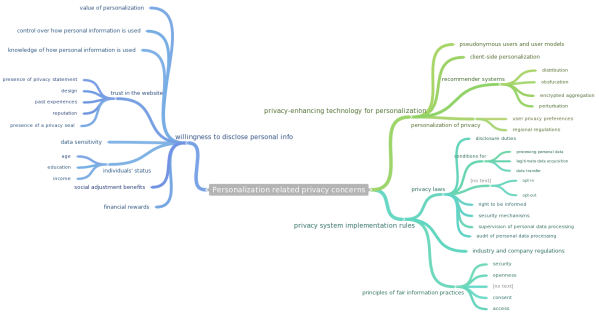

Figure 1: Concept map 1