Investigations on Privacy in Popular Online Systems

Sabine Weiss and Christof Hoell

Johannes Kepler University, 4020 Linz, Austria

Abstract. This article deals with the topic of privacy in popular online systems. First the problem is adduced that many people using online systems are unaware of which information about their personalities is collected. Then the definition of online privacy follows. Therefore some important criterias to compare popular online systems in a proper way are given. After the determinations of these dimensions some online systems, like Google, Facebook, Amazon.com and eBay.com are investigated by using these criterias. At last it is shown how people can prevent submitting too much information over the World Wide Web.

1 Introduction

Today online systems are very popular because more and more people use the services of these systems. But the problem is that most of these people don't know how much information is saved about themselves. In 1999 the Federal Trade Commission (FTC) discovered that "92.8% of websites were gathering at least one type of identifying (name, e-mail)" [3]. Collecting information without the awareness of the user is not the only problem with violating privacy. Additional to this, many online services share user data without the consent of the users. Turow writes in his article that in 2003 "57% of U.S. adults who use the internet at home believe incorrectly that when a website has a privacy policy, it will not share their personal information." [16]

Because of the World Wide Web it is easier than ever to gather and disclosure personal information about each user. Information isn't only collected when a user submits his personal data. Indeed, whenever a user's computer sends its IP address or other information, "the potential for a violation of privacy exists" [18].

2 Online Privacy

Before the investigation of the most popular online systems follows it is important to find out what privacy exactly is. There are many definition of privacy. For instance, Schoeman [17] writes that it is the "right to determine what (personal) information is communicated to others". On the contrary Chung [3] says in his article that it is the "right to be let alone". Therefore privacy can be seen as a kind of information privacy, "which is an individual's right to control his or her own personal information" [18].

2.1 Types of personal information

There are three types of personal information, which users leave in the World Wide Web when using online services [14].

The first type is personal data. This includes the user's name, marital status, email address, phone number and financial information. Second, the user leaves information about his digital behavior. This includes the user's Web activities, like visited sites, frequency and duration of these visits and his online shopping habits. The third type is information about his communication, which includes the user's electronic messages, postings to electronic boards, etc.

Since humans have reached the digital age, one of the major questions is that "who owns and who controls personal information" [15] of people using online services. These and other questions will be answered by investigating online systems with the following dimensions.

2.2 Dimensions of Online Privacy

In [14] eight dimensions of Web privacy are described in detail. These dimensions contain information collection, information usage, information storage, information disclosure, information security, access control, monitoring and policy changes. In this paper only five of these dimensions are focused.

The first focus lies on the information collection. This includes the way how the system gets the information about the user. The second dimension in this paper is the information usage. It defines what is done with the information the user submits. Third, the information disclosure is adduced, which describes if and to whom the company can give the collected user information. The fourth focus lies on the information security. It describes the security policies and mechanisms to secure the user data. The last dimension deals with policy changes. This includes the description of what happens if the privacy policy is changed.

Additional to these five dimensions of online privacy it is also mentioned in this paper how users agree with privacy policies and terms of service of each online system.

3 Privacy in Online Systems

For the investigation due to the topic of this paper Google, Facebook, Amazon.com and eBay.com, which are four very popular online services, have been chosen. The Terms of Service, the User Agreements and the Privacy Policies of these online systems are written in english and are posted on the websites of these systems. According to this topic only the parts of terms that are related to these investigation dimensions are regarded.

3.1 Google

Google is the name of the most popular search engine in the world. Because of the profit of the search engine, Google has started many services which are used

by millions of people around the world. Google is today the most valuable brand in the world.

Google has only one Term of Service [9] and one Privacy Policy [8] for all services it provides. If there are special terms needed for a service, a separate sheet is published by the service. [9] A user gives his consent to the terms by clicking to accept them or just uses the services. The only way of not accepting the terms is not using the services.

To use certain services the user has to fill out a registration form with his personal data. With the terms he also agrees, that his data is accurate, correct and always up-to-date. Google saves personal information on their servers and tries to get more information about the user: "We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services." [8]

The most important sentence in the terms of content items the user provides is in point 11: "By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive licence to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any content which you submit, post or display on or through the Services." [9]. This means that everything the user hands out to Google, belongs to Google. Therefore the user also argees with the terms that he has the right to give the rights of the content to Google.

If Google wants to give away the user's personal data it needs the consent of the user. But there are two exceptions [8]. First, Google is allowed to give personal information to subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on their behalf. The second exception can be interpreted in many ways: "We have a good faith belief that access, use ... is reasonably". [8]

According to Google the security measures of user data are "appropriate". These include internal reviews of the data collection and physical security measures. The only persons that have access to user data are "Google employees, contractors and agents who need to know that information in order to operate, develop or improve the services" [8].

Google changes its privacy policies frequently. According to [8] they can't reduce the users rights without notifing them. If Google makes significant changes it provides a more prominent notice on its sites. For some services Google will also provide an email notification.

Even if the terms don't exist any longer, the contract between the users and Google in form of the terms, will hold indefinitely. So even if Google doesn't exist any more, all services are indefinitely protected by these terms.

3.2 Facebook

Facebook is a social network that was invented by Mark Zuckerberg at the Harvard University. First, it was only used at Harvard, but then it became more

and more popular. Today `facebook.com` is the most visited website in the world with 120 million active users. Each user can have "hundreds of direct friends and hundreds of thousands of additional friends within just three degrees of separation from a subject" [10]. The financial background of Facebook comes from companies which are owned by the CIA. The CIA has also founded a Facebook group called "National Clandestine Service" to recruit new personnel.

By accessing or using the Facebook website the user accepts the terms of facebook [7]. It doesn't matter whether the user is a member of Facebook or not. It is important that people under 13 are not allowed to use Facebook. If the user is younger than 18 years, he has to be at college or high-school.

Facebook provides a My Privacy feature. With this users can control what information they make public. [12] shows that women are more likely to use such features and they self-censor their data more than men do. But "both genders are equally unfamiliar with Facebook's Terms of Service and Privacy Policy" [12].

Facebook gets two types of personal information about its users. First, during the registration the user has to give Facebook "your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information" [6]. Second, Facebook gets data from every visitor of the site. Browser type, IP address and more are stored for further use.

To improve services Facebook provides user information to third party companies. Facebook also says in their Privacy Principals [6] that its "service providers may have access to your personal information for use for a limited time", so that they can send emails, provide advertisements or do other jobs Facebook asked them to do. At the website of Facebook it is possible, that third party advertisers send ads to the users. If they do so, they will know the IP adresses of the users. They can also use cookies or javascript-code. Facebook claims to be not responsible for actions of third party advertisers.

One of the most dicussed Facebook features is Beacon. It receives data from other websites (e.g. shopping-sites) to show the user's friends in Facebook what he has bought. Many people think that this is violating their privacy (e.g. if a user bought a book about aids, all his friends would know this) [13].

Facebook protects personal information with secure servers behind firewalls. It also limits the access to its databases for search engines to protect personal data. When sensible information (like credit-card information) is needed Facebook uses the Secure Socket Layer technology (SSL). Facebook advices the customers not to use instant massaging or email to send private, sensible information.

Facebook reserves "the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice". If the changes are significant the user has 30 days to discover the new version on the site before the terms will take effect. The new effective date is published on the top of the terms.

3.3 Amazon.com

Amazon.com is America's largest e-commerce company. Not only in America, but also in Europe and Asia this online retailer sells products like books, VHS, DVDs, MP3's, computer software, etc. Due to Amazon.com's large popularity huge amounts of data must be managed and saved.

If a user visits the website of Amazon.com, he automatically accepts Amazon.com's Conditions of Use [2]. These Conditions of Use include collecting and analyzing information about the user and his shopping habits.

There are two ways Amazon.com gathers information about its users. On the one hand, the user offers his data voluntarily when he creates a new account at Amazon.com. With his account and profile the user at least hands out his name, email-address and password. At the registration of such a new account the user explicitly agrees to Amazon.com's Privacy Notice [1]. On the other hand, in comparison with the information Amazon.com saves without the aware of the user these information are the smallest part. The user's IP-address of his computer connected to the web, the browser type and version he uses and the time zone settings are saved. But as in Amazon.com's Privacy Notice described browser data like cookies and user's information collected by third parties are also used by Amazon.com. The user can block the cookies, but then he can't derive the advantages from Amazon.com. For instance, if the user leaves the cookies turned on and he browses through the products of Amazon.com, a big amount of information is stored. The next time he visits Amazon.com, services and products similar to the last visit are automatically offered.

But Amazon.com uses the customer's information not only for itself. Whenever personal data is given to others, the user will be informed and can reject the transactions [1]. For instance, affiliated companies, like Marketplace sellers, can sell their products with the services of Amazon.com. If the user is interested in such a product of a third party, he can tell Amazon.com that it provides his data to the affiliated company. Another way Amazon.com exchanges personal information is that it commissions other companies to perform special functions like sending mails, analyzing data and providing search results and links. Only for these performances the third parties can use the customer's data. The next example for sharing personal information is that Amazon.com often promotes special offers to certain user groups in cooperation with other businesses. In this case Amazon.com doesn't share the user data. Amazon.com only relays the offers to the customer who is then responsible for himself to give his data to these businesses. In the Customer Communication Preferences [1] each user can allow or forbid Amazon.com to relay these offers. Due to the expansion of Amazon.com, businesses, stores, subsidiaries or business units can be bought or sold. In this case the user information is a big part of the transactions and will be shared. However, conditions and promises defined in the pre-existing Privacy Notice will be remained. Amazon.com also shares the customer's data with other companies and organizations, if there is risk of violation of the law, for example fraud or obtaining credit by false pretenses. If the rights and safety of Amazon.com and

other customers aren't protected any more, Amazon.com also exchanges user data.

To guarantee the security of the user data during transmissions, Amazon.com uses Secure Socket Layer (SSL) software, which encrypts information [1]. By paying with credit card, Amazon.com only shows the last five digits of the credit card number. Just during the real transmission with the appropriate credit card company the entire number will be sent. Amazon.com also participates in the Safe Harbor Program to guarantee the security of user data. To protect the user's account against unauthorized access, the user has to keep his password a secret and to sign off each time he has browsed Amazon.com's website.

Summing up, Amazon.com manages all its practices in the Conditions of Use and the Privacy Notice. These include the promise that "we stand behind the promises we make" [1]. Every user can read these conditions any time on Amazon.com's website. If the Conditions of Use or other notices change, the user will always be informed by email, except he has denied this service.

3.4 eBay.com

eBay.com is an online auction and shopping website, managed by the American Internet company eBay Inc. Individuals and companies worldwide can buy and sell their goods and products with the services of eBay.com. Like Amazon.com and Google, there are also big amounts of information to be saved and managed.

Whenever a customer uses the services of eBay.com or other subsidiaries and international affiliates of eBay Inc., he agrees to the conditions and terms of the User Agreement [5] and to all other linked information. So, the user can visit the website without providing any personal data. But once he has an account at eBay.com, he agrees that his information is stored and shared by eBay.com [4].

Like other online systems, eBay.com collects not only personal data the user submits, but also information about his Internet connection and his browsing habits. At the user's registration eBay.com stores the email address, physical contact information and if needed the financial data, like credit card number. When a user offers, buys or sells a product, information about this item is also collected. Due to the shipping or billing of goods eBay.com stores information about these transactions. Communication between customers through the websites of eBay.com counts to the information eBay.com stores. eBay.com also collects hidden data, like information about the user's computer and his connection to the web (IP address, cookies, web log data), statistics on questionnaires, page views and traffic from and to eBay.com. If eBay.com verifies the user's identity, the user has to submit special personal data, like his ID. Another way eBay.com collects personal data is, when the user is in dept by eBay.com. In this case eBay.com is allowed by law to gather credit information about the user from a credit bureau.

With the use of cookies eBay.com offers special features, identifies customers and keeps them signed-in. Personal information is used by eBay.com to provide and improve services users request, to resolve problems between customers, to

prevent illegal activities, to compare information for accuracy and to promote its newest services [4]. Additional to these features, eBay.com combines the customer's data with information of other companies to expand its own services. Each user can allow or prevent this information sharing by setting his My eBay Preferences.

In the Privacy Policy [4] eBay.com guarantees the user, that it doesn't "sell or rent personal information to third parties for their marketing purposes without explicit consent" [4]. But there are some exceptions. For instance, members of the eBay Inc. corporate family can use personal information, if the customer allows this. They need this data to prevent illegals activities, to provide their content and services and to send marketing communications. eBay.com also sends user information to other companies under contract of eBay.com helping with fraud investigation, etc. Another way of information sharing is, when the user explicitly wants to hand out his data to a third party. To governmental officials the user information is disclosed as well, if they investigate a crime or unlawful acts. In this case each information relevant to the investigations is shared. For investigations of fraud, piracy or other illegal activities eBay.com gives user data confidentially to VeRO Program participants who help to prevent these acts. eBay.com's Privacy Policy also describes the sharing of user data, if eBay.com is sold or merges with another company. Then the new company gets the user information with the condition that the privacy policy is equal or similar to the old one.

For the security of the user data eBay.com participates in the TRUSTe program. One of the goals of this program is that it "covers only information that is collected through the web sites covered by this policy" [4] and not through software downloaded from eBay.com. To protect the stored user data against unauthorized access eBay.com uses many tools like encryption, passwords and physical security. But there is one thing eBay.com can't guarantee in its Privacy Policy: "we do not promise, and you should not expect, that your personal information or private communications will always remain private" [4]. There is also another lack in eBay.com's security, if the customer uses a shared computer. In this case certain user information is saved, so that the subsequent users can see this data.

eBay.com has the right to change its Privacy Policy at any time [4]. If there are any modifications eBay.com posts them in the Privacy Policy and notifies its customers through the Message Center. Changes automatically become effective 30 days after they are released. Each user can read the Privacy Policy and User Agreement on eBay.com's website at any time he wants.

4 Conclusion

This investigation on privacy policies shows that those are more or less equal. Every company has their own loop holes to aquire as many user data as possible.

Today online privacy is very important to everyone. Even if somebody has no internet, personal information about him can be found there (e.g. phone

numbers). One of the biggest problems in this century will be privacy. "Violation of privacy occurs when an organization collects, stores, manipulates, or transmits personal information unbeknownst to the individual." [11] But there are many companies and organisations who try to make money with everybody's privacy.

References

1. Amazon.com, Inc. (2008). Conditions of Use. `http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=508088`, (December 2008).
2. Amazon.com, Inc. (2008). Privacy Notice. `http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496`, (December 2008).
3. Chung, W., Paynter, J. (2002). Privacy Issues on the Internet. *35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, Volume 7, 193b.
4. eBay Inc. (2008). Privacy Policy. `http://pages.ebay.com/help/policies/privacy-policy.html`, (December 2008).
5. eBay Inc. (2008). User Agreement. `http://pages.ebay.com/help/policies/user-agreement.html`, (December 2008).
6. Facebook Inc. (2008). Privacy Policy. `http://www.facebook.com/terms.php?ref=pf`, (December 2008).
7. Facebook Inc. (2008). Terms of Use. `http://www.facebook.com/terms.php?ref=pf`, (December 2008).
8. Google Inc. (2008). Privacy Policy. `http://www.google.com/intl/en/privacypolicy.html`, (December 2008).
9. Google Inc. (2008). Terms of Service. `http://www.google.com/accounts/TOS`, (December 2008).
10. Gross, R., Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case). *Pre-proceedings version. ACM Workshop on Privacy in the Electronic Society (WPES)*.
11. Hann, I., Hui, K., Lee, S., Png, I. (2007). Analyzing Online Information Privacy Concerns: An Information Processing Theory Approach. *40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 210b.
12. Jones, H., Soltren, J. H. (2005). *Facebook: Threats to Privacy* Project MAC, MIT Project on Mathematics and Computing.
13. Knoke, F. (2007). *Spaehwerbung empoert Facebook-Nutzer*. Spiegel Online. `http://www.spiegel.de/netzwelt/web/0,1518,druck-519295,00.html`, (November 2007).
14. Rezgui, A., Bouguettaya, A., Eltoweissy, M. Y. (2003): Privacy on the Web: Facts, Challenges, and Solutions. *IEEE Security and Privacy*, 40-49.
15. Rose, E. (2005). Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*, Track 7, 180c.
16. Turow, J. (2003). *Americans and Online Privacy. The System is Broken.* Annenberg Public Policy Center, University of Pennsylvania, USA.
17. Schoeman, F. (1984). Philosophical Dimensions of Privacy. Cambridge Univ. Press.
18. Shaw, T. (2001). The Role of Identification in the Privacy Decisions of Information System Students. *34th Annual Hawaii International Conference on System Sciences (HICSS-34)*, Volume 8, 8040.