

Information Privacy

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions?
Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

When you visit a website, that website can automatically collect some information from your visit, such as the name of your provider, the location, the site you came from and the software you are using. In order to view the contents of the site or to become a member, the website may then ask for further personal information during your visit such as your name, email address and phone number. The website then has valuable information about you which can be used in different ways, or sold. This is one way that names get onto Spam mailing lists. Other sites such as your employer or bank may hold electronic personal information about you, which raises concerns about the security and privacy of electronic information. Some examples of the threats to online user privacy are the National Security Agency in America accessing Internet communications globally, and Amazon sharing customer information. Some people are asking if websites should be allowed to gather information about users, or if you give a site personal information, should that site be able to use your information and in what ways.

On the UAE government website it says that the site will not collect information about the user, and any information will be used for the purpose it was entered on the site. In the UAE there is no specific electronic data protection law, although the privacy and security of information is mentioned in some laws within the UAE. Employers must follow laws about how they store and share the information they have about employees, but the security of information stored electronically is difficult to guarantee.

Some companies collect personal data without user's knowledge or consent and then either share it or don't keep it safe. Websites can plant a cookie on your system, which can be encrypted and can remain for a long time, collecting information about you. Software called spyware can be planted on your system to collect information about you, and your surfing behavior online, tracking the websites you look at which is useful for advertisers. One sign that you may have spyware is an unusual amount of pop-up ads.

In a process called data mining, companies get trends and more information from the data they have collected. For example, Google admitted to taking information from student emails to learn how to better target advertisements at students. An investigation by a newspaper in 2010 found that Facebook was sharing personal information about tens of millions of users with advertisers. Even if the user had their privacy settings at the maximum, using an application like Farmville collected user information which Facebook then used. In another example, Apple was collecting and storing information on iPhones and iPads about the location of users, but as this was criticized the CEO Steve Jobs in 2011 made an apology. In 2007 Google added the Street View to Google Maps whereby users can see views of streets from webcams. This resulted in many privacy complaints and Google has paid fines and faced audits because users are worried about their privacy. In order to lessen the problem, Google introduced new features so users can choose to flag images for removal, and can blur faces and licence plates. However many countries are not happy, and Google had to pay France \$142,000 in March 2011 in a fine. Another major issue with privacy is social networking, where people may be tagged in photos or information about them might be revealed.

If private information about a person becomes public, it can have considerable consequences, such as medical information effecting insurance coverage or employment, financial information leading to fraud or identity theft. The right to privacy of information varies around the world, and the security of information held by databases and websites is difficult to guarantee. Just recently, an SSL bug called Heartbleed was discovered, which allows attackers to listen to communication, steal data and impersonate services and users. The attack leaves no traces and the user is unaware that data has been stolen.

References

Google Admits to Data-Mining Student Emails. (2014, March 19). Retrieved from EPIC.org:
<http://epic.org/2014/03/google-admits-to-data-mining-s.html>

Government.ae. (2014, April 10). Retrieved from The Privacy Policy :
<http://www.government.ae/en/web/guest/privacy-policy>

Alalwan, N., Alzahrani, A., & Sarrab, M. (2013). Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey. Retrieved from
<http://www.icofcs.org/2013/ICoFCS-2013-005.pdf>

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, A. (2010). Dealing with the problem of cybercrime. *Conference Proceedings of 2nd International ICST Conference on Digital Forensics and Cyber Crime.* Abu Dhabi .

Marsan, C. (2012, January 29). *The Worst Internet Privacy Scandals of all time.* Retrieved from TechWorld: <http://features.techworld.com/personal-tech/3333293/the-worst-internet-privacy-scandals-of-all-time/>

Miller, J. (2013, August 27). *Facebook to compensate users for sharing details on ads*. Retrieved from BBC News : http://www.bbc.com/news/technology-23848323?utm_medium=referral&utm_source=pulsenews

Steel, E., & Fowler, G. (2010, October 18). *Facebook in Privacy Breach*. Retrieved from The Wall Street Journal :
<http://online.wsj.com/news/articles/SB10001424052702304772804575558484075236968?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304772804575558484075236968.html>