Big Data

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?

Have you ever noticed that after you visit a website you see related advertisements popping up on other sites you use? Nothing in life comes free. When you visit a website, you often pay with personal information. A recent study by IBM states that 2.5 quintillion bytes of data is created every day. Data is powerful and valuable. For example, in 2018 Facebook made an average of $5.45 on each user through targeted advertising to take their annual sales to nearly $ 12 billion.

Websites can automatically collect some information from users, such as the name of the provider, location, the site you came from and the software you are using. The user may enter personal information during the visit such as name, email address and phone number. The website then has valuable information which can be used in different ways, or sold.

Some companies like Google and Facebook own a wealth of user information as they reach like octopuses over the Internet to collect data. Google owns many sites, for example DoubleClick which is one of the biggest trackers. With a population of 2.2 billion, Facebook would be the largest country in the world, and it has a lot of information about its members. Facebook collects information in various ways, such as through Facebook Connect, plugs ins and the 'like' button, and it owns WhatsApp. A very complete picture of a user can be created, from personal details, to location and behaviour including political and religious affiliations, relationships, education, work, interactions with friends and communities, surfing behaviour, down to which parts of webpages that user copies.

Some companies collect personal data without user's knowledge or consent and then share it. 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.

What do the companies do with all of this information? In a process called data mining, the data is explored for trends and user profiles can be created. Facebook and Google use computer algorithms to find trends. Google even freely publishes some of the trends. This is a profitable business; there are many companies such as TowerData and Cambridge Analytica, which build detailed user profiles and sell them.

The question is how ethical is this? Do users consent to their information being collected and analysed? It is not always apparent. For example, Google admitted to taking information from student emails to learn how to better target advertisements at students. A story first reported by two leading newspapers in 2018 found that 87 million Facebook profiles were harvested and used by Cambridge Analytica in order to profile users to send them supportive Donald Trump material. It is widely believed that this information influenced the outcome of the 2016 US presidential election. Even if the user had their privacy settings at the maximum, using applications allowed application developers to access to access user data from Facebook. The information can be used in various ways, to make market decisions, shape opinions, research, and refine products. There has also been media controversy that major US technology companies are involved in the work of the US intelligence agencies as they collect large amounts of communications data from foreigners, and at times, American citizens.

When this happens, the consequences could be considerable for users. If private information about a person becomes public, it can have considerable consequences, such as medical information effecting insurance coverage or employment. In 2012 Target sent coupons to a teenager for baby products after collecting information about her shopping habits. Her father complained, and so found out his daughter was pregnant. The right to privacy of information varies around the world, and the security of information held by databases and websites is difficult to guarantee.

Some people are asking if websites and companies 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. There are even companies which provide a service to trace your information and try to delete it such as UK Reputation.

Perhaps greater transparency is needed. 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.

Data collection is not going to stop. It is clear companies like Facebook and Google are powerful due to the amount of information they have. They have an ethical responsibility with that information.

Bibliography

BBC. (2018). *Facebook data: How it was used by Cambridge Analytica*. Retrieved April 30, 2018, from the BBC: http://www.bbc.com/news/av/technology-43674480/facebook-data-how-it-was-used-by-cambridge-analytica

Government.ae. (n.d.). *Privacy Policy*. Retrieved April 30, 2018, from the UAE Government: https://government.ae/en/footer/privacy-policy

Electronic Privacy Information Center. (2014). *Google Admits to Data-Mining Student Emails*. Retrieved June 1, 2015, from EPIC: http://epic.org/2014/03/google-admits-to-data-mining-s.html

Martin, E. (2014, March 27). *The Ethics of Big Data* . Retrieved June 6, 2015, from Forbes: http://www.forbes.com/sites/emc/2014/03/27/the-ethics-of-big-data/

Meredith, S. (2018). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. Retrieved April 30, 2018, from CNBC: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Mirani, L. (2015, January 12). *Why an obscure British data mining company is worth 3 billion* . Retrieved June 6, 2015, from Quartz Media: http://qz.com/323944/why-an-obscure-british-data-mining-company-is-worth-3-billion/

Nieva, R. (2018). *Facebook still cashing in on your data as sales surge*. Retrieved April 30, 2018 from CNET: https://www.cnet.com/news/facebook-first-quarter-earnings-2018/

Statistica. (2018). *Number of monthly active Facebook users worldwide as of 4th quarter 2017*. Retrieved April 30, 2018 from Statistica: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Tower Data. (2018). *Email intelligence, a TowerData service*. Retrieved April 30, 2018, from TowerData: http://intelligence.towerdata.com/

Volz, D. (2017). *Major U.S. tech firms press Congress for internet surveillance reforms*. Retrieved May 1, 2018, from Reuters: https://www.reuters.com/article/us-usa-cyber-surveillance-idUSKBN18M204