To what extent can private information online be accessed for negative purposes b...

Science, Computer Science

In this essay I will be investigating how severe the problem of online personal data being used for malicious purposes is. Private information can be defined as information of a person that they wish to keep to themselves so that the public does not know about it. This could be important information such as credit card numbers, personal ID numbers and passwords, or personal data like private pictures, conversations and browsing data.

This is an important discussion since once others get their hands on this information they can potentially use this to gain money by blackmailing the victim, steal from their accounts or sell their data to others interested in it. This obviously does a lot of harm to the victims and can lead to severe mental health issues. Nowadays the internet is used for basically everything from working to home management, so it would be a big problem if this information got leaked since that could potentially ruin your life. This is why I want to analyze the question “ to what extent can private information online be accessed for negative purposes by others”. I will do this by considering the problem in the context of Hong Kong as well as in other countries around the world such as America and Canada and also the viewpoints of various stakeholders such as large firms (Park’n Shop), underground businesses, government officials and consumers. Causes and consequences The internet is a relatively new piece of technology that was first developed in 1969. The dream to send a message from one computer to another was made into reality in 1980 when a British computer scientist linked hypertext documents into an information system, making it accessible from any node on the network. It was soon introduced to people all around the world and quickly

became widespread and popular in the mid 90s (History of the internet wiki article, 2018). The Internet’s functions back then included communicating through email, SMS, video calls, forums, blogs and social networks. These are still communication methods we use up until this day except they are much more technologically advanced.

Nowadays we have smart devices that varies from mobile phones and laptops to smart cars and smart lightbulb. We can turn on or adjust the lights, share pictures with friends or access our bank accounts with the flick of a finger. Our lives have never been so convenient ever before thanks to all these technological advancements, but the downside is that our private information is at risk of being easily seen by others we might not even know. Others are able to access more and more of our lives as people put more and more of their information online. The internet is playing an increasingly larger role in our daily lives. There are over 4. 2 billion internet users at the moment, which is over half of the entire population. An approximation of 23 billion messages are sent over the internet everyday. We are already so dependent on the internet that we averagely spend over 4 hours using it, which is ⅙ of our time everyday (2017). Even some basic daily actions like buying groceries and doing work are done through it. It is extremely hard to keep any data we put online secure, since hackers will always be able to find a way to surpass security systems. In the short term this causes people’s private information to be stolen by hackers for personal benefits like selling it to earn money or just to know information of a person. If this keeps up though not only would people stop putting all their data online, lots of

convenient function would be wasted as people become gradually more afraid of texting or paying online.

Hard work previous creator put in will be lost and we will be backtracking instead of making new technological breakthroughs. Computers would lose some of it’s very fundamental purposes like storing information and making communication easier. Therefore, data security is fundamental to the world’s leading economies and for the effectiveness in their functioning. From a global perspective, the Facebook and Cambridge Analytica data scandal is a good example of how dangerous putting information online can be. It involved Facebook violating privacy laws and harvesting user information without consent. In a court case, it was shown that Facebook was found to have been collecting information since 2014. According to (Harry Davies, 2015) The data was allegedly used to influence voter opinion in favour of the politicians who hired them. After being found guilty, Mark Zuckerberg apologized on behalf of Facebook in the midst of public outrage and risen stock prices. They were fined on the charges that the method in which the data was collected was inappropriate and had been done without consent. Almost 87 million user’s information were harvested, as Facebook had acquired millions of profiles from US citizens and used the data to build a software program to influence and predict the voters for the 2018 United States of America election.

The users were specifically paid a fee to take a personality test and “ consented” to have their data collected. This shows how easily our data can be exploited by someone who is looking for profit. Even when people are

cautious about their information being stolen and do things like avoiding entering personal data to untrusted websites or setting up firewalls, it is still highly likely that others are able access their data. (2008 cyber attack on United States wiki article, 2008) reported that in the 2008 Cyber attack on the United States, a simple USB drive containing a malicious malware designed to break systems and extract information was inserted into a highly secured Government computer. The virus spreaded without being detected throughout the central system. It took the Pentagon, one of the most technologically advanced organisation, nearly 14 months to get rid of the malware. Over thousands of important confidential files were stolen including weapon blueprints, industrial partners, operation plans and surveillance data (CNN wire staff, 2010). The attack raised alerts that led to the creation of a whole new branch of military, the U. S. Cyber Command. We can see how dangerous it is on the internet when the U. S. government had to use the military, a group that was meant to fight in wars and sustain security of the whole country, to fight against cyber attacks.

Hong Kong also has its own privacy issues. One example is that in mid 2010, a former worker of an insurance company reveal that Octopus, the Octopus Card Company, has been selling over 2. 4 million of their users' data. This was later confirmed by Octopus themselves (Peter Bullock, 2018). During May 1st to 7th 2011, Hong Kong held a privacy week to educate the public on the ongrowing problem of security on media associated apps or websites. They also reinforced laws about selling personal data or using it for marketing. This was to raise awareness about the risk of citizens' personal

information being stolen and to discourage firms from abusing user data for their own benefits. This didn’t stop the firms from using their collected data as we can see in the following case. Hong Kong’s Park’ N Shop was convicted for violating a law which prohibits use of personal data in direct marketing without obtaining the data subject’s consent. The impose and maximum fine for an offense against this law is 500, 000 HKD, which shows how serious the crime is. A customer of Park’N Shop had provided his personal data including his email address to the large company. After he received marketing email from the company he complained to the Commissioner. The case ended with Park’N Shop pleading guilty to the offense.

COURSES OF ACTIONS

For this issue there are several courses of action that can be taken into account, such as government intervention or subsidising technological advances to further improve personal data protection and softwares designed to easily overcome malwares and viruses designed to extract data. This is actually a very long term solution since its benefits will not just be seen locally, but could spread to become a global solution to privacy encryption. On March 6th 2018, The National Association of Local Councils urged the government to provide funding to help councils comply with the EU General Data Protection Regulation (GDPR). The aim of this program is to make Europe fit for the digital age. More than 90% of Europeans say that they want the same protection rights across the EU and regardless of where their data is processed. Data privacy is a right and everyone has the right to protect their data. The National Association of Local Councils uses roughly

300, 000 euros per month to comply with the charges needed to complete the program. If the government were to provide extra funding, the EU could use this money to provide analytical activities that include comprehensive research studies, training activities, surveys and the preparation of guides to widespread the acknowledgement of data breach. Furthermore, they would be able to pass laws that would restrict malware users for good and be able to protect data harvesting such as the case as seen in Facebook and Cambridge Analytica.

Another course of action would be for more firms to pay for professionals to find errors in their safety system that keeps their users safe. Larger firms like google and facebook have been practicing this for a long time to ensure no data would be leaked from their users. Conclusion After researching this issue for several weeks and writing this essay, I think that I do not have a major role to play to minimize this issue as it doesn’t affect me in a major way and i can’t do much about it. On the other hand, I think that my perspective on this issue has changed quite a bit after this investigation since our informations are much less secure than i’d thought they’d be. Hackers have much more power than i expected and more firms than i realised are using our information for their benefit. I used to think that data and privacy was really quite a small issue and that problems like hunger and poverty were affecting the world more. Now i think they are affecting the world on an equal level, if not more. I think I answered the question relatively well but I had a hard time finding solutions for my question or my issue because it is relatively new subject and it is quite difficult to find information

on it especially reliable information. While I have found that personal information can easily be harvested and used for harmful purposes, the ease with which data can be collected due to the Internet can actually be a good thing. For one, it has made gathering data for sociological research a lot easier. A recent study was done by tracking web traffic on Wikipedia and contributed a lot of insight on collective memory, a topic which had previously been difficult to investigate due to lack of data. In conclusion, private information online can be quite easily accessed by hackers and firms for their own beneficial good. Hackers can easily bypass safety defenses and firms can easily trick users in order to take their data. However people now start seeing the problem and have done measurements in order to combat with the issue. In time things will get better as we learn more about this piece of new technology.