An Inquiry into the Leakage of Internet Information and Solutions

Jingjing Wang[1a]

[1]University of California, Irvine, USA

[a] sixsunsss@gmail.com

Keywords: Information leakage, privacy, ethics

Abstract: We are living in the Information Age, while we are benefiting from the Internet, some security problems like information leakage has become increasingly prominent. After introducing the concept of the externalities, I give two examples of information leakage – Baidu Netdisk and Facebook. Facebook – Cambridge Analytica data scandal is the key case in my paper, as this case covers a wide range and is known by many people. The second half of my paper is the reflection of information leakage, which contains the externalities and relevant ethical theories. The private rights of customers may be harmed by companies contracts, because customers may not able to notice that their personal information are being leaked and used. The problem of information leakage could be viewed from various theoretical perspectives in regards to ethics, such as deontology and ethical egoism. It becomes more and more difficult to regulate network security because of the popularity of the Internet. There are some solutions to information leakage such as government regulations, privacy laws, and business rules, but what's more important is the self-protection awareness of the Internet users.

1. Introduction

In this era of rapid development of information technology, Internet brings us endless convenience and novelty. But while we are benefiting from the Internet, many troubles come after another, which bring some negative effects to our life. With the popularization of Internet application and people's dependence on the Internet, the security problem of the Internet has become increasingly prominent. Malicious programs, all kinds of phishing and technology theft continue to maintain a high rate of growth. Information leakage has gradually become the most serious Internet security problem and it happens very often in our daily life. With a large number of network attacks, a large number of Internet users personal information leakage and property losses continue to increase. In this paper, I'm going to talk about information leakage and the ethical issues of this serious network security problem.

Market failure is the economic situation defined by an inefficient distribution of goods and services in the free markets. There are four types of market failure including externalities, monopoly, information asymmetries, and free riding. Information leakage is related to one of the four causes of market failure - externalities. An externality refers to a cost or benefit to a third party who has no control over how that cost or benefit was created. Specific analysis about externalities and information leakage will be demonstrated later with two cases. With specific cases that I mentioned below, you will also have better understanding about the harm and ethical problems of information leakage.

2. Examples of Information Leakage

2.1. Baidu Netdisk

According to BBC News, Personal data is being collected and transmitted insecurely by thousands of apps using code from the Chinese net giant Baidu, say security researchers [1]. Baidu Netdisk is a cloud storage service launched by Baidu company, users will be able to easily upload their files to the network disk, and can view and share across terminals anytime and anywhere, but

millions of Chinese people are believed to have been affected by the data leaks. In 2016, the total number of users of Baidu Netdisk exceeded 400 million. and the APP focus more on personal storage and backup. On July 18, 2017, there was a WeChat official account issued a statement - in Baidu Netdisk, there are lot of private information can been seen by other users, even including enterprises and institutions' internal address book. After users choose to share photos, contacts and other content in a public way, everyone can see the shared content on their home page. The data reveals where people are, search terms, sites visited and the ID numbers of devices they own. In addition, the content containing personal information is easily searchable on some third-party disk search sites. A reporter of Beijing Youth Daily found a network disk file which contains more than 4,000 enterprise leaders' contact information of Jiangsu Xuzhou through a third-party network disk search website, and the file can be freely downloaded and shared. As for publicly shared files being captured by third-party online disk search, Baidu said it will step up efforts to crack down on third-party online disk search sites and constantly innovate to enhance users' privacy protection from technology.

Coincidentally, the information leakage problem is not only in China, but very serious all over the world. The Facebook-Cambridge Analytica data scandal was a major political scandal in early 2018 when it was revealed that Cambridge-Analytica had harvested the personal data of millions of people's Facebook profiles without their consent and used it for political advertising purpose [2]. On March 17th, it was reported that Cambridge Analytica, a British firm, had illegally obtained the personal data of 50 million Facebook users without their permission. The information was then used to accurately deliver advertising content to these users and help Trump's 2016 presidential campaign. As a result, Facebook's shares fell 6.8 percent on March 19th - the biggest one-day decline in five years, and 2.56 percent on March 20th - wiping out all of the company's gains in 2018 and Facebook lost $50 billion in its market value in two days. Meanwhile, shares of social media companies such as Twitter and Snapchat were hit hard as well. According to the source, the most frightening aspect of the whole affair is not just the risk of data leakage, but the fact that Facebook was aware of the existence of third-party applications that used its users' data for research purposes many years ago.

2.2. Facebook and Cambridge Analytica (CA)

The disclosure of Facebook customer information has become a major political event, economic event, technological event, big data event, and other major deep-seated problems [3]. The severity may not be due to the huge amount of data that has been leaked about 50 million customer information in North America, but rather to the accumulation of data on super platforms such as Facebook, especially how customer information is used and how to plug loopholes that have been abused. Especially when it is applied to political elections, big data turns out to be a tool of political elections, even an evil tool. The corporation agreements between those big companies violate users' privacy information, as the third party, Internet users have certain types of cost because of negative externalities. For a long time, Facebook's open API allows external third-party companies to provide psychological tests or small games on the Facebook platform, which enriches the content diversity of such social platforms, and further strengthens the stickiness of social relations between users through user participation and sharing. The main character in this scandal become 'famous' - Cambridge Analytica(CA). Cambridge Analytica analyzes users' behavior patterns, personality traits, value orientation and growth experience, and then delivers targeted information and campaign ads to influence American voters' votes in elections. A simple online application test allows a user to identify five personality traits: openness, conscientiousness, extroversion, agreeableness and neuroticism. They can infer a user's gender, sexual orientation, education and even childhood trauma based on the user's Facebook profile on thumb up. After accurate grasp of the customer, the precise release of guiding information can help them basically determine the customer's behaviour. Cambridge Analytica invited Facebook users to take a personality test between 2014 and 2015 to manipulate public opinion through massive data analysis and research. On March 30, Facebook announced that they will end cooperation with big data companies in the

next six months to better protect users' privacy. Not-too-surprising, CA closed operations in the course of this huge scandal, but the related firms still exist.

2.3. The Reflection of Information Leakage

2.3.1. Negative Externalities

There are negative externalities occurs to internet users when the information leakage problem exits. When an agreement was reached between the companies, their goals of making benefits may be approached, but the private rights of customers may be harmed by companies contracts. Consumers don't know their personal information or some comments they post will be used as tools for those big companies, their rights to be informed are invaded. Even though the negative externalities of this issue are obviously noticed by public, positive externalities also exists according to what Mark Zuckerberg and Sheryl Sandberg said. Some psychological tests and small games provided by third-party companies can somehow enrich the content diversity of such social platforms like Facebook. In addition, those small programs can also strengthen the stickiness of relations between users through plentiful interesting interactions.

2.3.2. Relevant Ethical theories

Facebook-Cambridge Analytica data scandal could be viewed from various theoretical perspectives in regards to ethics. CA used collected data to analyze the political preferences of voters, and targeted advertising. There are some states stay neutral, citizens in the states are not too democratic nor republican. Those people are the target population for CA cause the company can use advertise to wave people's idea and let them support Trump. For example, to populists, they push articles or videos that Trump defends America, drives away foreigners, builds walls, etc.; to business elites, they push advertisements that Trump's policy about cutting taxes, developing business, etc. Also, they put some negative advertisements to smear Hillary. Facebook should take responsibility to user agreement and App review, in the early days, in order to quickly establish an ecosystem and a development platform, Facebook agreed to launch a large number of inferior apps, which were of varying quality. On the one hand, we can analyze the behavior of Facebook and CA from the perspective of Deontology, which is a way that people judge the morality of other based on a set of rules. Deontology, can be explained as "Ethics as Duty" [4]. Immanuel Kant's understanding about deontology exactly matches the ethical issues that occurred here. Immanuel Kant focused on motives and the willingness of individuals to act for the good of others, even though that action might result in personal loss. It's extremely difficult to implement ethical principle in business where all that is important is time and money, but the customers will also eventually price the morality of the business. Facebook have the rights to access users' information, it also have the obligation to protect those informations. Even though we can not put all the blame on Facebook, but the company and the executive officers should clearly know their obligations to put customers and society on the first place. Doing something for the right reason was much more important to Kant than any particular outcome. From a Kantian perspective, it is clear that adherence to duty is what builds the framework for ethical acts. Duty, obligation, and good will are of the highest importance. According to Kantian, the company's decision of using customers' data to make profits violates the people's privacy rights. Facebook focused on the end with the motive of doing the ethically responsible thing - end the corporation with inferior third-parties. In conclusion, everyone had a duty to obey a categorical imperative to do the just and moral thing, regardless of the consequences. On the other hand, ethical egoism can also be used to explain those cases, which is a subcategory of Utilitarianism or Consequentialism. Ethical egoism is the view that each of us ought to pursue our own self-interest, and no-one has any obligation to promote anyone else's interests [5]. It is thus a normative or prescriptive theory: it is concerned with how we ought to behave. There are some arguments in support of ethical egoism. Bernard Mandeville (1670-1733), an Anglo-Dutch philosopher and political economist, believed that everyone pursuing their own self-interest is the best way to promote the general good. Scottish political economist and

philosopher Adam Smith wrote that when individuals single-mindedly pursue "the gratification of their own vain and insatiable desires" they unintentionally, as if "led by an invisible hand," benefit society as a whole. The decisions and actions done by CA and Facebook are rational according to these pro statement, because people are the best judges of what is in their own interest, and they are much more motivated to work hard to benefit themselves than to achieve any other goal. The goal of Facebook and CA may be the wealth and power, their corporation and the use of collected data can help them achieve their own goals. Not surprisingly, there are objections to ethical egoism because it goes against certain basic assumptions that most people have regarding what ethics involves. Firstly, ethical egoism has no solutions to offer when a problem arises involving conflicts of interest. In this case, ethical egoism will not provide any sort of resolution or common-sense compromise to both companies and customers. Secondly, ethical egoism goes against the principle of impartiality, because this seems to contradict the very essence of morality - the "golden rule", says we should treat others as we would like be treated. The executive officers in companies may not willing to let themselves in the circumstances of deception, and be used by others.

2.4. Solutions to the Information Leakage

2.4.1. Big Data Companies

The Facebook breach has proven that big data is far more powerful than people thought, and that big data analytics companies are far more capable than our expectations. Protecting personal network information is very urgent, it's illegal and unethical to disclose customers' private information. Advance legislation is extremely important - from a global perspective, the G20 should play its role as an international organization, seeking global multilateral cooperation and issue guidance on global digital protection as soon as possible. All countries, especially those big data countries, should soon adopt legislation to protect the use of online data, especially personal privacy information. The world should focus on and regulate big data giants. Those major companies such as Apple, Facebook, Amazon, Microsoft, Alibaba, Tencent and Baidu, should assist and cooperate with the government to protect the privacy of personal data, consciously comply with supervision, self-discipline, self-examination and self-restraint, and protect the privacy of personal data of the platform.

2.4.2. Privacy Law - GDPR

General Data Protection Regulation (GDPR) is the privacy law enacted by the European Union in 2016 - - protective umbrella of Netizens [6]. This regulation has been implemented in all local privacy laws across the entire EU and EEA region. It will apply to all companies selling to and storing personal information about citizens in Europe, including companies on other continents. This law helps citizens have greater control over their personal data and assurances that their information is being securely protected. Under the GDPR, individuals have 8 basic rights: information about how your personal data is processed, obtain access to the personal data held about you, ask for incorrect personal data to be corrected, request personal data to be erased, object to your personal data being used for marketing purposes, request the restriction of the processing of your personal data in specific cases, right to data portability, request that decisions based on automated processing involving you or your data are made by natural persons, not only by computers. This law was legislated in 2016, but came into force on May 25, 2018, which give companies two years to prepare. But as soon as May 25th arrives, if any company is found to have broken the law, it will be fined heavily. Either pay 20 million euros, or pay 4% of the turnover, which penalty to pay more. But what disappointing is that this law is not much enforcement in 2018, although some progress is being made, it not yet that impact. According to Raegan MacDonald, the Head of EU Public Policy at Mozilla, the impact of GDPR is not that big. She mentioned that many companies have updated their privacy policies and created tools to give users more control, many companies appear to be interpreting GDPR as narrowly as possible. McDonald concerned that privacy is still by default put at risk without users understanding or having meaningful control, but MacDonald is optimistic about the future: "We haven't seen the big fines levied just yet. But I

suspect that if 2018 is the year of implementation, 2019 will be the year of enforcement."

3. Conclusion

Government regulations is very useful, but what more important is that we as individuals should be more defensive and pay more attention to protect our own privacy information when using internet or APPs. For example, we must go to regular website when viewing message or browsing video, installed antivirus software also cannot assure computer won't catch a virus. Especially when we shopping, we must use regular and secure website because online shopping involves online payment. When using public networking tools, we should remember to remove traces before logging off. Using print materials as an example, we must ensure that we exit our mailbox after printing, change the login area if the computer is on "remember the password" setting.

It must be stressed that protecting the privacy of personal data does not mean denying the use of data. Accurate service through data is universal and can improve the efficiency of information distribution and user experience. It is the misuse of data, not the sharing of it, that is to blame. Data is a gold mine, if only emphasize protection and do not use mining, it will cause great waste. Decision makers in big companies should put business ethics in mind, their business conducts will be examined by ethical principles and moral standards. Customers and society norms should be put in the central place in this prosperity and development business environment.

References

[1]"Baidu Apps Found to Be 'Leaking' Personal Data." BBC News, BBC, 26 Feb. 2016, https://www.bbc.com/news/technology-35669817.

[2]"Cambridge Analytica." Wikipedia, Wikimedia Foundation, 10 Aug. 2019, https://en.m.wikipedia.org/wiki/Cambridge_Analytica.

[3] "Facebook–Cambridge Analytica Data Scandal." Wikipedia, Wikimedia Foundation, 9 Aug. 2019, https://en.m.wikipedia.org/wiki/Facebook–Cambridge_Analytica_data_scandal.

[4] Maack, Már Másson. "GDPR's Impact Was Too Soft in 2018, but next Year Will Be Different." The Next Web, 7 Jan. 2019, https://thenextweb.com/eu/2018/12/27/gdprs-impact-was-too-soft-in-2018-but-next-year-will-be-different/.

[5] OpenStax. Business Ethics, OpenStax Business Ethics, 20 Sept. 2018, https://opentextbc.ca/businessethicsopenstax/chapter/deontology-ethics-as-duty/.

[6] Westacott, Emrys. "What Is Ethical Egoism?" ThoughtCo, ThoughtCo, 27 Jan. 2019, www.thoughtco.com/what-is-ethical-egoism-3573630.ethical