# An Analysis of Data Ethics in the Internet Environment

Jin Yan

2022-10-05

## Abstract

This paper first discusses the value of the large amount of data available in the Internet environment, mainly related to medical health, advertising and credit building. It then demonstrates the problems of data misuse in the current Internet context. The importance of establishing data ethics is illustrated by comparison. At the end of the paper, the current state of personal data protection in Chinese society is presented, along with a specific analysis of the current situation.

## Introduction

The development of machine learning and artificial intelligence has made the footprints people leave on the Internet particularly valuable. Currently, the records of people's activities on the Internet, whether in the medical, advertising or financial sectors, can be used by the holders of these data to create enormous wealth. At the same time, ordinary Internet users are increasingly aware of the importance of their personal data. In the process of using these data, there are also things that can harm people's interests. There are heated debates on how to protect their data. The main purpose of this paper is to raise awareness of data ethics by showing the current problems of data misuse in the context of the Internet and the responses of various countries.

## Literature review

Personal data has contributed to the development of the following industries.

### Medical Industry

Machine learning and large-scale data sets have allowed the full potential of personal information to be exploited[1]. Specifically, there are now many fitness apps and diet intake apps that allow users to extract health information from recorded data, and the value of this data rises as the analytical and predictive capabilities of these apps improve. In addition, large-scale medical information can be used to treat diseases that could not be dealt with before[1]. Even some recent analyses suggest that the value of data needs to be reevaluated because the current ability to analyze and compile data has changed dramatically from what it was

before[2]. In fact, the market for medical data in the United States is in the billions. And there are already startups in the U.S. that are profiting from providing individuals with secure access to selling their personal information.

### Advertising Industry

In the "Big Data Era", data has become an effective input to the wide range of services offered by the Internet. With this data, Internet platform companies can provide customized advertising recommendations. The data shows that the conversion rate of advertisements has become twice as high as before compared to ordinary media.

### Financial sector

The most far-reaching change that technological advances have brought about for China is the creation of a social credit system. This system will evaluate and grade the creditworthiness of 1.4 billion people, by analyzing their social behavior and collecting economic and government data. For example, Tencent Credit, a subsidiary of Tencent Technology, has been collecting large amounts of data through QQ and other security applications and in the process has found that data generated by social media can effectively help in credit risk analysis.

### Problems in data use and some solutions.

Although the great value of medical data is valued by companies and research institutions, there is a large number of people who are not well aware of the value of their data[3]. In response to this situation those medical researchers who collect and use medical data, government agencies and companies should make vulnerable groups aware of the potential value of their own data[1]. Governments have also taken some measures to protect personal data. For example, in Europe the latest General Data Protection Regulation has recognized personal data as the property of individuals.

## Personal data specifics and analysis in China

### specifics

The development of big data and artificial intelligence technologies in China has led to a significant rise in the digital economy. It was able to reach 26 trillion RMB in 2017. The contribution to China's GDP reached 32%. At the same time, the growth rate of the digital economy was 18%, while the overall economic growth rate was 6.9%[4]. It is also important to note that the use of data in China has created some problems. Approximately 70% of the population's personal information is compromised on the Internet. This information includes names, addresses, phone numbets preparing for exams also receive phone calls and messages from people selling them preparation materials that they may use for the exam. There are

technology companies that help government public safety agencies develop surveillance systems through the use of big data, voice recognition, and image recognition. Data breaches can even lead to serious cases, and the Xu Yu Yu case is very typical. A high school graduate girl lost her college tuition because she was cheated with 8000 RMB, and then became depressed and had an acute heart attack. The reason was that the fraudster got her information by attacking the school database and thus won the girl's trust by using the real information in the database[5].

In fact, China has enacted numerous laws and regulations to address these issues: in November 2016, the "National People's Congress" enacted the Internet Security Law[6]. China's criminal law has also had two amendments in the last decade to address personal information security[6].

### Analysis

Although there is already a considerable amount of legislation in place to safeguard personal data, the current enforcement of the law is somewhat unsatisfactory. Despite the high number of cases related to personal information from 2010-2015, the number of actual convictions is relatively low. In addition, although the amendment to the criminal code increased the length of imprisonment to three to seven years, the most serious convictions between 2015 and 2016 were for two years, with two years of probation. In fact, the main reason for these problems is that the public is not well aware of the potential risks associated with personal data breaches. The public is also not very sensitive to the security of personal data. In such a situation, personal data can be easily obtained. This also affects the enforcement of legislation and laws. In addition, a questionnaire was used to investigate the perception of data protection among the 20-30 year old Chinese adult population. 100% of the respondents experienced problems due to information leakage. What is worth exploring is that when asked how much money they would be willing to spend to protect their data, 80% chose not to spend in this area. This result shows that the problem of personal data leakage is indeed common, but for most people the impact of online information leakage on their lives is relatively limited. Limited by the sample size, the samples involved in this survey study are all bachelor's degree holders with certain risk-averse ability. When asked whether they care about Internet companies recording their own behavioral data on the Internet for targeted advertising, 100% of people feel uncomfortable, and 40% of them feel very much so. Combined with the previous information, it can also be concluded that this group has a relatively strong sense of personal data protection. However, the awareness of the risks caused by data leakage is not quite sufficient.

## Conclusion

The above analysis shows that both officials and individuals are aware of the importance of data protection, but not enough attention has been paid to it. The measures currently in place do not fully address the risks of data leakage or misuse.

Therefore, the government should join hands with the data security industry to launch some educational lectures or regularly recommend some cases of data leakage to the public, so as to raise the importance of data security and reduce the occurrence of related cases.

## References


[1] Dulhanty A 2021 Present value of future health data: Ethics of data collection and use *Bull World Health Organ* **99** 162–163

[2] Foster J and Clough P 2018 Embedded, added, cocreated: Revisiting the value of information in an age of data *Journal of the Association for Information Science and Technology* **69** 744–748

[3] Cheah P Y, Jatupornpimol N, Hanboonkunupakarn B, Khirikoekkong N, Jittamala P, Pukrittayakamee S, Day N P J, Parker M and Bull S 2018 Challenges arising when seeking broad consent for health research data sharing: A qualitative study of perspectives in Thailand *BMC Medical Ethics* **19** 86

[4] Weber P A, Zhang N and Wu H 2020 A comparative analysis of personal data protection regulations between the EU and China *Electron Commer Res* **20** 565–587

[5] Feng Y 2019 The future of China's personal data protection law: Challenges and prospects *Asia Pacific Law Review* **27** 62–82

[6] Han D 2017 The market value of who we are: The flow of personal data and its regulation in China *Media and Communication* **5** 21–30