Advances in Social Science, Education and Humanities Research, volume 291

International Conference on Management, Economics, Education, Arts and Humanities (MEEAH 2018)

On private data of legal & technological protection in machine intelligence era

Ningxian Zhu

Shandong University of political science and law

Shandong, Jinan, 250014, china

zhuningixan@163.com

Keywords: machine intelligence. private data. Legal & technical protection

Abstract. In machine intelligence era, data value is derived from its free and shared. All behaviors of people can be automatically collected, quantified and coded by machines. Data is not only a kind of resource, but also a tool. People can translate them into insight and implementation. But if not used properly, it will bring about some serious problems. How to deal with it? Faced data oligopolistic firms, traditional legal & technological protection on private data has encountered severe attacks. This paper references on legislative reform and technical protection in Europe and America, explores some strategies and methods on legal and technical, meet the new challenges of social development.

Introduction

With the application of intelligent technology, private data is entered into various network systems, which were automatically collected, kept and analysis by the ubiquitous sensors. These data provide a lot of trouble when it comes to facilitating people. For instance: New community owners received advertisements from decoration company, students' parents received massive piles of SNS from training institutions, Some of the chain hotels encountered hacker attacks and results in the leak of sensitive information. Even more serious is loopholes of Netease mailbox (it has the highest level security certificate EAL3+), results in hundreds of millions of user private data leaked [1]. These private data are stored in various database server, which contains a huge amount of information, can dig out different use value, it is easy for an ulterior motives person to resell and profit. Personal data once is leaked, it will be very serious. How to avoid bad business happened? Private data protection has faced unprecedented challenges.

In 2010，the President Obama launched a "My Big data" plan; hope to make it easier for Americans to access to their private data. May 2014, the United States government released "Big data: Grasp the opportunity, Guardian value", which focused on the United States large data conditions, current situation, and policy framework and improvement proposals.

Now, whether the legal or technical, private data protection is still lacking in China, how to establish a sound private data protection laws and social supervision mechanism is a long way.

Private Data Faced with Problem

Private data's concept

Private data refers to the individual's reluctance to disclose or be known by others, such as the individual's behavior patterns, hobbies, health status, which is related to everyone's vital interests.

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

Because those data is related to individuals, or can indirectly identify individual identities. In EU services law, " Recognition " is the most important criterion to judge it, and it is also an important attribute of private data.

In an era of big data, the data becomes the "third eye", which dominates all the people private data. A large number of data oligarchs and data intermediaries have sprung, and become the key link of the personal private ecological chain. The big data is not only a resource, but also a profit-making tool, such as some search engine companies can import through traffic, sell customer resources. The potential value of data can be dig and delved. Even the most useless data, if those be gathered together, through algorithm analysis and cross alignment testing, can extract out some value from the data group, can also discover new use value. La Tanya Sweene, Harvard University Professor, study that as long as you know a person's age, sex and zip code, and Cross contrast the open database cross, you can identify 87% of the people.

Private data’s safe use and leakage

Without any supervision and restraint, the application of technology has made the private completely unmasked: High-definition camera can be clearly photographed private behavior in a car; 24.9 billion-pixel photos can clearly display a naked man in hotels in the Bund of Shanghai; smart family meters collect a real-time data in 6 seconds, and each kind of electronic equipment has the unique " the characteristics of typical load ", which can be analyzed the family member daily Behavior habit, even in the future, the gene sequencing which is core personal private data is related to everyone's life safety.

The biggest problem on personal private data is the availability of data and the limits of its use. And these problems are expressed in a specific made up of:

①Collecting data becomes ubiquitous. The doer is difficult to perceive, the duty of the subjects of electronic collecting is difficult to monitor effectively;

② the processing of data becomes the specialization and diversification, the doer is difficult to control his own information;

③ The original storage of data becomes cloud form, the leakage risk increases;

④ There is contradictions on open and sharing demands private data resources and so on.

In machine intelligence era, the relationship between the free use of private data and the security needs to be re-examined.

Individual behavior is guided by technology; the diversity of choices is losing

Individual behavior should be the rich diverse and selectivity. The application of data integration and recommendation algorithm in network enables people to enjoy the simplification and improve the quality of life, and also face the problem that individual behavior is predicted and guided by technology, thus result in losing the rich diverse and selectivity.

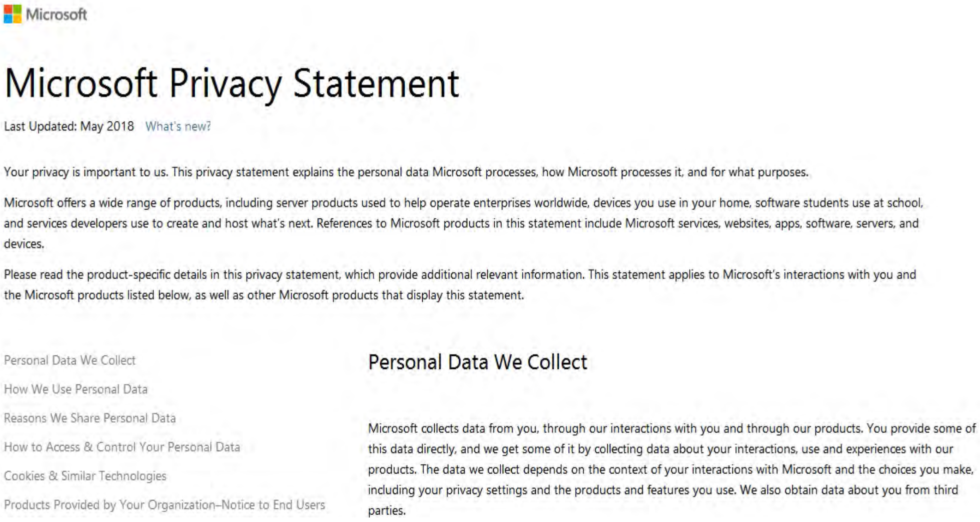
For example, in the process of online shopping, the individual purchasing behavior will be automatically recorded and analyzed by some machine. According to the personal shopping experience, shopping habits and preferences, and referring to similar people's shopping behavior, the merchant can actively recommend goods and services to them. Thus consumers seem to have greater rights and convenience of choice, and in fact, they are prey of machine. Because individual behavior reliance on the machine to help make decisions， which would be extremely damaging! Large data prediction will imprison human's rich diverse and selectivity, become the machine of selectivity, form a class of things with common features or attribute and but has no individuation, the latent possibility is dispelled on the altar of probability. This kind of machine "intelligence" facilitates the user, at the same time, also deprives the user rich diverse and selectivity.

The solution of Personal Private Data Protection

The inviolability of private and freedom is the core of civilized society. How to protect our individual behavior from machine recommendation systems? We should be carried out from the following aspects.

Legal protection

There is the framework of "Notification and Consent" in the law, Microsoft's private statement mentions the contents of "Our Collected personal Data" (Bing queries, Microsoft Cortana's instructions, documents on the cloud), and the purpose and implementation (cookies), and explains " How we use technology "-- mainly for personalized improvement, and show you some related ads, fig 1.



Microsoft

Microsoft Privacy Statement

Last Updated: May 2018 What's new?

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to Microsoft's interactions with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Personal Data We Collect
How We Use Personal Data
Reasons We Share Personal Data
How to Access & Control Your Personal Data
Cookies & Similar Technologies
Products Provided by Your Organization–Notice to End Users

Personal Data We Collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices you make, including your privacy settings and the products and features you use. We also obtain data about you from third parties.

Fig.1 Microsoft's notification and consent statement

The development of technology has brought new problems to t the framework of " Notification and Consent ", which has been defeated by the positive benefits of data. The user's control over the data is declining. Users and large data companies is asymmetry in the control of information, the user never know their personal private data at when, where, by whom, how to use. "Notification-consent" rule execution is difficult, because the data monopoly companies to take mandatory consent, users must agree to use their services, and once agreed that the scope of use of data is often magnified in the company's other business. And the difficulty of data supervision and accountability is increased, the responsibility of the diversification is difficult to identify.

To this，the United States, on the basis of the original private policy and law, revises laws and put forward policy propositions. It contributes to play the role of industry self-discipline, built a relatively perfect and unique network environment for private protection system.

Industry self-discipline and personal protection are not enough to protect our privacy data. We should rely on strong national laws to do it.. In the light of "Privacy Protection of consumer data in a networked environment – a policy framework for protecting privacy and promoting innovation in the context of the global digital economy" which signed by U.S. President Barack Obama at February 23, 2012, our " People's Republic of Network Security" was implemented at June 1, 2017, but it is lacking the protection of privacy data. The General Data Protection Regulation in European is known as the strictest privacy law in history. Although it carry out just two weeks, but already have produced a strong deterrent in the Internet companies.

Technical protection

The traditional private data protection technology is a differentiation private strategy, that is, for different private data, such as the online activities and related search records, pictures, geographical location and other fragmented data, with the processing of fuzzy and anonymous technology, so that all the data revealed personal situation is not reveal in the dataset. Although widely recorded, but it does not violate the user's private and data security.

With the increase of data sources and the application of data analysis technology, the data can be collected through social network and APPs, which has shown identity. Moreover, the boundaries of personal private data are increasingly blurred, because the traditional private data may also identify personal information by correlation matching.

① The "anonymity" strategy of traditional data protection is invalid. With the development of machine intelligence and the improvement of algorithm, the collection of personal private data is becoming more and more intensive and hidden,, which can be obtained from different data of fragmentation. Through multiple sources of personal information, merchant can form a complete personal portrait and real-time tracking.

②The " transparency " strategy of is under attack. Individual behavior can no longer be collected in a dominant manner, and it is difficult for users to know whether data is collected, analyzed and utilized, to discern which data can reveal private.

③The subject of data collection is complex and various, the sharing degree of data promotes. The sharing degree of data unceasingly deepens, the data association is close in them, and the boundary among them is blurred. For example, a shopping habit data may also derive the user's financial behavior.

④The data storage in third party causes the data and the user separated, the information storage and the responsibility undertakes becomes the latent problem[2]. In the interest-driven, individual information forms an interest chain. Responsibility and supervision is complex, which constitute a serious challenge.

Conclusion

In a word, faced with under the positive benefit of l private data, the traditional protection program loses its effect. What it is collected and used is getting out of control, which results in the legal and technology defect to protect private data. We can draw some conclusions.

1. Before embarking on a security mechanism to protect them, humans have always created the tools that might harm them. Just as the invention of printer has led to a change in social, the era of machine intelligence, we should deal with the long-standing challenges of the protection of privacy data, It is the infrastructure of the society, and is necessary to prevent the monopoly and abuse of information and to improve the legal & technological protection.

2. Social normative protection. The legal & technological protection doesn't work. We should build new social normative norms. What kind of technology will bring to the corresponding behaviors and reactions. People known firstly how to prevent loss of profit and know how to benefit from data assets.

Reference:

[1] Liming. American private protection system in large data era. Peking’s Financial & Law Studies Center. http://www.360doc.com/content/14/1211/13/20625606_432125588.shtml [OL]. (2014).

[2] Fanwei. New ideas of personal information protection in large data era. China Institute of Safety and Communication. xinhuanet. http://www.cbdio.com/BigData/2016-02/01/content_4576387.html [OL]. (2016).