Proceedings of the 2nd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/86/20241019

Consumer Privacy Breach Hazards and Governance

Wendi Qi[1,a,*]

[1]*Beijing Normal University - Hong Kong Baptist University United International College, Department of Business Administration, Zhu Hai, 519000, China*
a. r130026120@mail.uic.edu.cn
**corresponding author*

Abstract: Tens of thousands of transactions of all sorts take place around the world every day, and they are inevitable because different people have different needs every day. Often, many providers require consumers to provide a range of relevant information in order to unlock access to their services. E-payments are a typical example. The mandatory requirement used by e-money platforms requires consumers to enter personal information relating to themselves in order to complete real-name authentication, and most consumers are forced to accept real-name authentication in the face of the trend towards e-payments.[1] However, not all organizations can guarantee the encryption and non-disclosure of customer privacy, especially in China, where incidents of consumer privacy being compromised are commonplace. A large number of unscrupulous organizations are profiting from the exchange of customer information through underhanded collusion. There are also a number of research gaps in the area of data leakage. With the increasing exchange of information, there is an urgent need to address how to efficiently utilize data and how to monitor data breaches worldwide.

Keywords: Privacy Encryption, Data Breach, Data Monitoring

1. Introduction

Consumer privacy is basically composed of all personal information related to consumers, including but not limited to basic information such as name, gender, and contact information; document information such as ID cards and practice licenses; occupational information such as the industry to which one belongs and work experience; financial information such as personal finances and debt records and even health information such as medical cases and past medical history.2024 On March 6, at the China Development High-Level Forum, Ant Group's Chairman and CEO, Wells said that it is important to make privacy computing technology dedicated to the availability of data while protecting data privacy, aiming to make the value of data flow as securely and portably as tap water.

The research progress in this field is to avoid the occurrence and proliferation of consumer privacy leakage by strengthening network regulation and legislation.[1] However, there is a blind spot in the regulation, and the feedback and rectification of the information needs a relatively long period of time to be examined, so there are a series of gaps waiting to be solved in the field of data privacy, which are mainly embodied in the following aspects: quantitative assessment of privacy data, how to quantify the degree of infringement of individual privacy is extremely difficult to count, and it is necessary to establish a set of data privacy standards to be applied. The quantitative assessment of

DOI: 10.54254/2754-1169/86/20241019

privacy data, how to quantify the degree of infringement of personal privacy is extremely difficult to statistics, need to establish a set of scientific assessment system; the realization mechanism of the rights of the data subject, how to ensure that the data subject of the use and disposal of their personal information has the right to control, the right to know, and the right to choose, etc.; the cross-border data transmission of the protection of privacy, with further development of globalization, how to ensure that in the cross-border transmission of data has become more and more frequent premise of ensuring that personal privacy is not infringed upon by the legal differences between cross-border legal differences. In this paper, we will summarize the harms of privacy leakage and propose a series of possible solutions through the analysis of three typical consumer privacy leakage cases. Research in the field of data privacy has a series of practical significance, such as promoting technological innovation, safeguarding national security, protecting consumers' rights and interests, enhancing the efficiency of data utilization, and promoting social trust.

2. Cases of Privacy Leakage in Private Hospitals

With the continuous development of the GDP of the society, private hospitals in the society have also become prevalent in recent years and showed a rapid development trend. Due to the good privacy, elegant environment and one-on-one specialized services, a large number of affluent families of the middle class and above have been captured in the society, however, due to the attribute of "private", these hospitals tend to focus on the profit-making purpose. However, due to their "private" nature, these hospitals tend to be profit-oriented, so in the course of their development, some of them sell their customers' private diagnostic information in packages to medical aesthetic organizations with which they have cooperative relationships in exchange for high exchange fees.[2] The medical beauty industry is highly profitable in today's society, and the cost of a simple minimally invasive cosmetic surgery is extremely high. With the rapid development of society and the changing definition of beauty, the demand for cosmetic surgery, especially among the female population, is increasing day by day. Due to the high price of most aesthetic medical programs, it is difficult to sign an order if the customer is not targeted and induced to spend money. Therefore, a part of private aesthetic medical institutions have sprouted the idea of purchasing the privacy of potential customers' medical records in an attempt to hit the nail on the head and persuade patients in need of cosmetic surgery.[3] According to statistics, facial surgery and body contouring surgery ranked the top two in China's cosmetic surgery statistics for the whole year of 2023, with double eyelid surgery, eye bag surgery, facial liposuction, breast augmentation, abdominal contouring, and fat grafting ranking in the top three of the two categories of cosmetic surgery respectively.

From the patient's point of view, once his or her information about his or her visit to the private hospital is disclosed to the cosmetic surgery organization, a series of questions that the patient asked the physician at that time will be uploaded to the medical institution's database, so a part of the patients with allergic inflammation can't extricate themselves from the acne elimination program of the cosmetic surgery organization, and similarly, a part of the patients who need body contouring have a hard time maintaining their sanity in various types of body contouring surgical programs of the cosmetic surgery organization. The same is true for a portion of patients with a need for body contouring. Although under certain circumstances, such targeted surgeries do help some patients to solve their current physical problems and needs, this kind of sales approach based on illegal access to private data and induced marketing has caused a series of bad consequences such as a crisis of trust, loss of legal liability, and misuse of medical information. These persuaded patients have been developed into long-term potential customers by the beauty organizations without their knowledge, and countless traps and schemes are still waiting for them in a series of follow-up maintenance and upgrading surgeries. In response to this phenomenon, private hospitals need to regularly audit and evaluate the security of their customer databases, and raise the awareness of their staff in all

DOI: 10.54254/2754-1169/86/20241019

departments, as the last link in the chain of data leakage is the inability of some unscrupulous doctors to hold on to their ethical boundaries [4].

3. Cases of Privacy Breaches in Bank-Type Depository Institutions

China is known as a country with a high savings value, and the Chinese people generally have a strong sense of saving money. According to Wind website, in 2023 alone, the Chinese people saved close to 17 trillion yuan, and the balance of residents' RMB deposits has also realized a long-term, year-on-year increase since 2004, so banks have always played an important role as financial intermediaries in this regard. In the West, banks and financial institutions also play an important role, such as the United States, where the national debt is extremely high, and the federal government relies on strong daily tax revenues for its high expenditures. As of April 1, 2024, the U.S. federal government earns a staggering $1.86 trillion [5].

Residents rely heavily on banks to complete transactions for their income tax payments and daily consumption, and the prevalence of credit cards has also laid the foundation for the prosperous development of banks. The prevalence of credit cards also laid the foundation for the growth of banks. The personal information in personal deposit and loan statements directly reflects the purchasing power of the consumer and his or her main needs at the moment. At this time, some local banks have signed consumer information-sharing agreements with insurance companies, credit companies, and even trust companies in an attempt to fulfil their respective business targets and to absorb as many high-quality customer resources as possible. For example, when consumers' deposits are more than 1 million, simply keeping cash in the bank in exchange for regular income is not the optimal way to profit, so securities companies that get this part of consumers' information will take the initiative to contact the consumers by SMS, e-mail, etc., and further sell a series of financial products, programs, etc.; when consumers' credit card has a large negative value and there is a certain credit crisis, credit companies that get this part of the information will take the initiative to contact the consumers, to fulfill their business targets and absorb as much quality customer resources as possible. When a consumer has a large negative balance on their credit card and is in some kind of credit crisis, the credit company that has gotten this information will take the initiative to contact you and offer you a loan with a high interest rate for you to choose from. Because these organizations have access to accurate information, it is relatively easy for them to control the psychology of consumer demand and, through a series of means, ultimately achieve the profitability of the organization.

While this may help consumers with these needs in some cases, it is unethical and not legally permissible to do so against their will. In today's increasingly e-consumer world, all banking institutions are accelerating the pace of updating and expanding mobile applications that push out user information, thus putting the maintenance and protection of databases at greater risk. Once the customer information is leaked, it will bring great troubles to the daily life of the consumers who have their data leaked, and in the worst case, it will leak the inside information of the financial and legal industries, which will lead to vicious competition among industries and social pressure. [6] The rapid development of the information age has led to an increasing demand for confidentiality of private information, so it is incumbent upon banking and financial institutions to ensure a high degree of confidentiality of customer account information.

4. Data Privacy Leakage Case in the Automobile Industry

In 2023, Toyota, a famous Japanese automobile brand, was exposed to a case of user privacy leakage, according to China's CCTV financial news report, Toyota leaked vehicle data information about 2.15 million Japanese users, including but not limited to a series of user information such as vehicle usage data, vehicle geographic location, interior and exterior environmental data, and remote on-board

DOI: 10.54254/2754-1169/86/20241019

information and communication [7]. The reason for the leak is that Toyota's cloud system was incorrectly set up so that the data was "open" for nearly a decade, and the relevant monitoring department did not find any abnormality for a long time. The serious data breach, which also included some owners of Lexus, Toyota's premium automobile brand, quickly caused an uproar on the Internet. Toyota has a famous advertising slogan "Wherever there's a road in the world, there's a Toyota", according to which Toyota's position in the world's automobile industry is very important, because of this, such a company with a global brand effect has a series of problems such as data privacy leakage, we can learn that data leakage and we can see that data leakage is closely related to all of us. Not only Toyota and other old capitalist car manufacturers, in recent years, with the rise of electric vehicles and the impact of the global energy crisis, but a number of new electric car manufacturers have also emerged, gradually occupying the position of sales in the market and have an advantage over traditional fuel vehicles, however, new energy vehicles have not yet escaped the clutches of data privacy leaks. 2022 December 20, according to Azalea, the company's data is still not available. On December 20, 2022, according to a statement by the Chief Security Scientist of NIO Automotive Future Holding Co. on the official website of NIO Automotive, on December 11, 2022, NIO Automotive received an anonymous email claiming to have NIO's internal private data and using it to extort the company for the equivalent of US$2.25 million in Bitcoin. The privacy breach partially covered nearly 100,000 reports of NIO Motors-related user transactions since July 2021 [8].

According to the above two typical case studies, there is a high degree of likelihood that customer privacy breaches will occur, because during the transaction process, customers have to sign related information agreements to inform the automobile company of their private data, and often these data breaches originate from external hackers or internal executives' malicious leakage, which is extremely difficult for automobile companies to detect promptly. Either way, it is extremely difficult for automotive companies to detect and deal with the leaks promptly, and we are only aware of a few privacy leaks, and a large number of data leaks are still shrouded in the "dark room" of the information age. To further optimize the data security network platform, on the one hand, the government should strengthen the relevant legislation and the monitoring department of the government's functions from the legal supervision and policy implementation of the two dimensions of the occurrence of data leakage and further dissemination; on the other hand, the major companies should strengthen the data protection and anti-data leakage system on the investment, to ensure that the technology is constantly updated to cater to the new challenges of data theft, to fundamentally protect consumers' legitimate privacy leakage. On the other hand, companies should invest more in data protection and anti-data leakage systems to ensure that technology is constantly updated to meet the new challenges of data theft and to protect consumers' legitimate information rights. Although the automobile sales industry does not have a dominant influence on consumer information leakage, the process often reflects a consumer's level of consumption as well as information about their daily work, consumption, and place of residence. In this era of information explosion, any piece of sensitive information will make hard-working merchants profitable, so it is incumbent upon us to combat this illegal and unethical behavior.

5. Conclusion

This paper analyzes three typical cases of data privacy leakage, covering the medical beauty industry, banks and other savings institutions, as well as the automobile manufacturing industry. Summarizing the disclosure of privacy leakage behaviors in the above major industries, it can be found that privacy leakage is still difficult to monitor and pervasive social problem. Society and businesses need to give every consumer a minimum level of respect for their privacy, and so-called performance indicators and profitability criteria are not a reason to compromise consumer privacy. Therefore, a better solution is to strengthen the legislative effect and timely implementation of monitoring at the policy

DOI: 10.54254/2754-1169/86/20241019

level to reduce the frequency of data leakage horizontally, and to strengthen the awareness of data protection among citizens and the responsibility of enterprises to reduce the possibility of data leakage vertically. However, this paper does not provide recommendations to address some of the current research gaps in data privacy, such as how to effectively monitor the extent of residents' privacy infringement and the further inspection of cross-border information transmission and anti-data leakage, and so on. The issue of data privacy protection will continue to dominate social challenges for some time to come, and only when a strong data monitoring system is in place, under the umbrella of a fully transparent inspection system, will it be possible for consumer rights to be fully protected and respected.

References

[1] *Lu Jun. (2023). Research on e-commerce secure payment system based on mobile communication network. Changjiang Information and Communication (09), 89-91. doi: CNKI: SUN: HBYD.0.2023-09-028.*

[2] *Ding, Hongfa. (2019). Rational privacy preserving model and application (Doctoral dissertation, Guizhou University). https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CDFDLAST2021&filename=1020723945.nh*

[3] *Li, Li-Qing & Ding, H. F.. (2023). Risks of Patient Privacy Leakage and Strategies for Prevention and Control in China under the Background of "Internet+Medicine". Medicine and Society (01), 57-63. doi:10.13723/j.yxysh.2023.01.011.*

[4] *Mu Bochao. (2019). Risk analysis of patient privacy leakage during case management. Techwind (31), 219. doi:10.19392/j.cnki.1671-7341.201931194. https://fiscaldata.treasury.gov/americas-finance-guide/government-revenue/*

[5] *Ma, Wenbo (2024-03-15). Improving Financial Supervisory System to Enhance Financial Risk Prevention and Control Capability. China Business News, 002. https://new.qq.com/rain/a/20230516A01YYTOO*

[6] *Qiwen Wang & Yuli Wu, NIO: some user data stolen before last August, extorted for $2.25 million equivalent in Bitcoin, Dec.12,2022, https://www.thepaper.cn/newDetail_toward_21241139*

[7] *Yang Bo, Zhong Yongchao, Yang Haonan, Xu Zifeng, Li Xiaoqi & Zhang Yuqing. (2023). Study on the Risk of Wi-Fi Privacy Leakage in Smart Connected Vehicles. Journal of Xi'an University of Electronic Science and Technology (04), 215-228. doi:10.19665/j.issn1001-2400.2023.04.021.*

[8] *Mao, Yunlong. (2018). "Research on User Privacy Leakage and Protection in the Context of Internet Plus" (Doctoral dissertation, Nanjing University). https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CDFDLAST2019& filename=1019030120.nh*