ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Data information leakage and the threat to network information security

Yuk Cho Randy, Wang
University of California San Diego, San Diego, California, 92093, USA

Abstract: This article analyzes the social harm of data breaches from three dimensions: firstly, the technological models and social impacts of information breaches; Secondly, there are differences in the risks faced by different social groups, especially vulnerable targets such as children and the elderly; Thirdly, there are regulatory deficiencies at the institutional level and a lack of corporate responsibility.
Keywords: information leakage; internet security; information supervision

1. The expanding crisis of private data leaks and its public security impacts

The leakage of private user data has evolved into one of the most significant cybersecurity challenges of the digital era. Recent research shows an increase in both the frequency and intensity of data breaches across social media platforms and hospitality systems. Data breaches have become much worse than before. In the past, hackers only stole simple information like names or emails. But now, they steal very private details—Fingerprints, personal messages, bank records, and even government IDs. This change happened for two main reasons. First, big companies store too much user data in one place, making it an easy and valuable target. Second, hackers are now smarter, especially those working for governments. They use advanced techniques to break through security systems. The record of data breaches provided by the Privacy Rights Clearinghouse (PRC) shows: between January 2005 and December 2018, PRC archived over 9000 breach events impacting roughly 12 billion individual records. Each breach is classified by root cause—Insider misuse (INSD), payment-card fraud (CARD), physical loss (PHYS), stolen portable device (PORT), hacking or malware (HACK), stationary equipment loss (STAT), unknown methods (UNKN), or accidental disclosure (DISC) \cite{Alotaibi2019}.

These growing threats create dangers that extend far beyond privacy exposures. Private data leaks cause much bigger problems than just privacy violations—They create significant public security risks. Exposed personal information can devastate individual lives, while financial institutions and businesses suffer major losses, with hackers routinely targeting hotels to steal credit-card details and sell them on the dark web, which may cause incidents like credit card fraud. In early 2025, a cybersecurity failure at Cardiff Council resulted in the exposure of sensitive personal details of vulnerable children under its care—An incident officially described as posing "a potential safeguarding risk to children" and prompting escalated response from national cyber teams

2. Disproportionate impacts on vulnerable groups

The consequences of data breaches are not distributed equally across society. Vulnerable populations including children, elderly citizens, and low-income groups face amplified risks due to technological, economic, and social factors.

2.1. Children's data vulnerability

In the last few years, there has been increasing awareness about the unethical and often illegal data collection procedures of social media platforms and ed-tech companies, and their collection of data from minors. While a few platforms do their best to "protect" a minor's personal data, the reality is that most of these platforms will collect significant information about the minor, ranging from sexual orientation, browsing history, location information, behavioral details, etc. Not only do most social media platforms collect information from minors without obtaining proper parental agreements in compliance with COPPA and/or California laws, but they usually do not provide the minors with any level of protection. One of the most typical examples was TikTok: A

ISSN: 2424-8460(O)
2251-2608(P)

short-form video app that has popularize over the global: In 2023, TikTok was put against with a massive lawsuit for continuing to violate COPPA, incurring liability of up to 150 million dollar as a result of the lawsuit. The FTC alleged that TikTok collected sensitive data from users under the age of 13, including collecting identifiers to enable the company to deliver targeted advertisements. Before TikTok could begin to collect this kind of data, they were conditionally required to notify parents and obtain their permission before collecting any data from the minor. This is just one example of a greater trend suggesting tech companies that operate on a global scale are continually neglecting their ethical responsibility to "protect" their young audience while exploiting young users that may or may not even know what personal information they are offering.

In a similar pattern, Edmodo, which has been utilized as broadly in educational contexts as a way to provide virtual learning (and education technology) to schools, has also been accused of questionable data practices. Investigations discovered that Edmodo had collected information illegally from teenagers, including academic progress, login history, and personal messages and then shared or sold that information to third-party advertisers. This especially a concern since Edmodo has been marketed as a secure, approved tool from the school which led many parents and educators to trust the platform with kids' personal information. In place of advancing kids' privacy, the platform use the data to make profits without appropriate parental agreements and violated ordinary norms of data protection.

The problem isn't only with TikTok or with Edmodo. Other platforms have drawn similar criticism. For example, in 2019, YouTube was checked for apparently tracking children's viewing habits to better target advertisements, while Meta, has shown to be criticized for collecting data on underage users on Instagram. There is a systemic issue here within tech: their actions are not being rigorously enforced nor punished when it comes to protecting minors online. There are laws such as COPPA and GDPR in Europe, yet these companies will continue operating in grey areas or simply disregard laws all together since they have little to lose and would be soon overlooked by big profits.

In addition, there are troubling long term implications of this type of data usage. Consider that children and adolescents are much more susceptible to deceptive advertising, identity theft, and social profiling, and their online habits are tracked and then analyzed to form their habits and pReferencess. Studies reveal that increasingly excessive data collection, results in massive targeting or market, minors may therefore receive a large number of highly targeted advertisements, which are often persuasive and can have an impact on the physical and mental health of adolescents. Further, the sale of students' data on educational platforms brings its own ethical issues---should a child's achievement or activity in school be monetized for corporations?

2.2. Elderly targeting mechanisms

Older adult populations data breaches have gained immense popularity among cybercriminals due to the unparalleled completeness and richness of senior medical records. Senior medical records consist of well-documented, detailed healthcare profiles developed over decades, while populations younger than seniors consist of incomplete or less detailed medical histories. Cyberthieves exploit these information through a variety of methods, such as sophisticated access attempts targeting healthcare workers, exploiting poor or outdated authentication systems in independent and assisted care facilities, and hacking into insecure medical devices within long-term care settings such as nursing homes. These types of attacks tend to be well-planned, with the attackers going to great lengths to hit institutions holding or managing senior healthcare data, knowing that the payoff is worth much more than obtaining younger individuals' records.

With criminals now able to crack senior medical records, they're not only obtaining minimal contact info—they're obtaining full patient profiles that include Medicare numbers, full medical histories, full names, addresses, and even contact details for family members. . These kits are then packaged into valuable assets and sold on underground markets where they. Criminal buyers utilize these packages to facilitate a range of scams targeting elders, including making fake medical claims to Medicare for reimbursement, faking phony emergency alerts to scam relatives into paying, and utilizing identity theft in order to obtain controlled substances.

The allure of stealing senior health care data is in the high return on investment and the relative ease of exploitation. Medicare and other health programs targeted to seniors reimburse at higher rates, making phony claims much more worth it. In addition, seniors and seniors' families are also considered softer targets for social

ISSN: 2424-8460(O)
2251-2608(P)

engineering based on less familiarity with technology, trusting authority more easily, and having a greater fear for health-related crises. Social engineers exploit these vulnerabilities with complete confidence that their senior victim or its contacts are likely to fall into line with urgent or emotionally manipulative requests. Furthermore, as older medical records are not usually updated or audited as rigorously as younger counterparts, fewer opportunities exist for early discovery of fraud and therefore more time to gain additional profit.

Even worse, the delayed adoption of technology by the healthcare industry, particularly within elder care centers, only contributes to the issue. A majority of nursing homes and assisted living centers use outdated IT systems with minimal encryption, poor password habits, and limited employee training against phishing attacks. Connected medical devices such as insulin pumps or heart monitors often only have basic security parameters applied, which provide a simple entry point for hackers. With advanced hacking methods, the assault on older healthcare data grows, requiring promotion of cybersecurity systems, restricted regulatory controls, and more alertness from healthcare providers and families to delay these devastating incursions.

3. Broader societal harms of data breaches

The impact of data breaches extends far beyond the personal privacy invasions of individuals, it creates weaknesses that harm social stability and economic security. When sensitive data enters the public domain, it breaks down people's trust on online platforms that they prefer not leave any personal data online due to the worriness of data breachs. Many consumers may alter their online behavior after major data breaches have been reported, with many going as far as to discontinue services altogether. This impact majory affect on important areas like digital healthcare, where patients' unwilling to record accurate medical histories in the terms of privacy can lead to misdiagnosis and ineffective treatment.

In the financial sector, large-scale data breaches may lead to a contraction of the credit market, especially limiting financing channels for small and medium-sized enterprises. Financial institutions may raise credit thresholds and even misjudge the economic situation due to risk model adjustments, thereby exacerbating market volatility. This unexpected credit tightening may suppress business activity and delay economic recovery.

In the labor market, leaked sensitive information such as personal health records, financial history, or identity data may be used for recruitment discrimination, putting job seekers at a disadvantage. Although anti discrimination laws provide basic guarantees, data-driven implicit biases are often difficult to trace and prove, resulting in limited legal remedies. In the long run, this unfair competition may weaken labor market efficiency and exacerbate social inequality.

At the political level, data breaches have become a potential tool that affects social stability. The leaked citizen information may be used to manipulate public opinion, interfere with elections, or undermine social trust. For example, by accurately disseminating false information or creating targeted public opinion pressure, attackers may weaken democratic participation and even fuel the legitimacy narrative of authoritarianism. Such strategies not only threaten election fairness, but may also erode public trust in the system, leading to long-term political apathy or social division.

Overall, the impact of data breaches has surpassed the scope of individual privacy and penetrated into the core operational mechanisms of economic, social, and political systems. Its indirect effects may trigger market failures, exacerbate social inequality, and undermine the stability of the governance system. Therefore, building a more comprehensive data security and governance framework is not only a technical issue, but also a key factor in maintaining macroeconomic and social resilience.

4. Pathways to mitigation: Corporate and policy solutions

The problem of data breaches is becoming increasingly serious, and it is needed to establish a more effective data security protection system. This system cannot simply comply with regulations, but should proactively prevent problems. For enterprises, protecting data security should be an important part of their overall development plan. Specifically, different protection measures can be taken based on the importance and risk level of the data; Using new technologies to protect privacy while still being able to use data normally; Strictly control who can see which data and monitor abnormal operations; The entire process from data generation to deletion

ISSN: 2424-8460(O)
2251-2608(P)

must have protective measures in place; Regularly check system security and test protection capabilities through simulated attacks and other methods.

In terms of management, global cooperation is needed to establish unified rules, rather than each region acting independently. These rules should clarify basic issues such as data ownership and cross-border transmission, while also flexibly adapting to technological development. Regulatory authorities should focus on actual results allowing companies to choose protection plans that are suitable for their own situations. Important industries and critical facilities require stricter management, and departments and regions should also strengthen cooperation.

Due to the frequent involvement of multiple countries in cybercrime, there are still many difficulties for countries to cooperate in handling cases. It is necessary to establish specialized agencies under international organizations such as the United Nations to unify evidence standards and case handling procedures. Cybersecurity departments of various countries should share information, conduct regular drills, and be able to quickly and jointly respond to major incidents.

5. Conclusion

Technological innovation is very important, and it should focus on developing basic technologies for data security while applying new technologies such as artificial intelligence to enhance protection capabilities. It also need to strengthen talent cultivation and establish unified technical standards. Building this protection system requires the joint efforts of the government, enterprises, technical experts, and the public. The government should do a good job in coordination and supervision, enterprises should take responsibility and increase investment, technical personnel should constantly innovate, and the public should also raise safety awareness. Only with everyone's joint participation can a safe and reliable digital environment be established.

It is difficult for victims of data breaches to protect their rights now. A rescue system should be established, including legal assistance, psychological counseling, credit recovery, etc. Different levels of rescue measures can be initiated based on the severity of the incident, especially to help vulnerable groups such as the elderly and children. In the long run, data security insurance can be established to share risks.

References

[1] Wang, W. N., Zhang, J., Wu, J. (2025). A Method for Detecting Leakage Risks in Network Information Transmission Based on Artificial Neural Networks. Computer Programming Skills & Maintenance, (07), 170-172. https://doi.org/10.16184/j.cnki.comprg.2025.07.003.

[2] Cheng, H. Z. (2025). Application of Big Data Analysis Technology in Prevention of Information Network Data Leakage. Network Security and Informatization, (07), 134-136.

[3] Cheng, F. Y. (2025). Discussion on Influencing Factors and Preventive Measures of Computer Network Information Security. In Proceedings of the 2025 Smart Design and Construction Experience Exchange Conference (pp. 251-253). China Wisdom Engineering Research Association; Shanghai Yapu Network Technology Co., Ltd. https://doi.org/10.26914/c.cnkihy.2025.035588.

[4] Zhang, J. Q. (2025). Legal Regulation of Algorithmic Recommendation on Network Platforms and Protection of User Rights and Interests. Legality Vision, (17), 27-29.