Digital Government Information Disclosure and Privacy Protection

Wenjian Chen

College of Liberal and Professional Studie, University of Pennsylvania, Pennsylvania PA 19104-3335, USA

Cwj2233254746@163.com

Abstract. Digital government information disclosure is a global trend. Governments of all countries expand the scope of information disclosure through legislation, policies, and technical means to enhance government transparency and credibility. The Chinese government has also gradually promoted information disclosure, making its decisions public through digital government construction and online press conferences. In recent years, with the popularity of social media, the government has also acted with the public through Weibo, Douyin, and other means to protect citizens' right to know better. However, while promoting information disclosure, the issue of privacy protection has become increasingly important. With the wide application of digital technology, the digital government collects, stores, and processes a large amount of citizen data in the process of information disclosure, which poses a potential threat to citizens' right to privacy. Therefore, balancing information disclosure and privacy protection has become a key challenge in constructing a digital government. To ensure public interests, the government needs to take effective legal and technical measures to protect individual privacy and ensure that information disclosure does not damage citizens' legitimate rights and interests.

Keywords: Digital Government; Data disclosure; Privacy Protection.

1 Introduction

The newly revised "Regulations on Government Information Disclosure" was promulgated and implemented in 2019, emphasizing that "disclosure is the norm and non-disclosure is the exception"[1]. As an essential part of government work, information disclosure has received unprecedented attention in today's society. Transparent and open government information has far-reaching significance for building a sunshine government and a government ruled by law. In addition, the "China's Cybersecurity Law" passed in 2016 proposed that disclosing personal sensitive information should respect the true wishes of the subject of personal information [2]. It can be seen that the country attaches great importance to privacy protection and actively curbs the chaos of illegal abuse of personal information.

L. Zhu et al. (eds.), *Proceedings of the 2024 4th International Conference on Public Relations and Social Sciences (ICPRSS 2024)*, Advances in Social Science, Education and Humanities Research 874,
https://doi.org/10.2991/978-2-38476-305-4_30

2 Definition of Digital Government Information Disclosure and Privacy Protection

2.1 A Subsection Sample

Digital government information disclosure is the process by which the government provides government information to the public using digital and information technology[3]. Through information disclosure, government transparency can be enhanced, the public's understanding and supervision of government behavior can be promoted, and the government's credibility and service level can be improved. The scope of information disclosure is broad, covering government policy orientation, legal and regulatory provisions, administrative decision-making processes, and results [4].

Digital government privacy protection protects citizens' personal information and privacy data security while the government discloses information[5]. With the widespread application of digital technology, the government may involve much personal information in data collection, processing, storage, and sharing. Once this data is leaked, the consequences will be unimaginable. Privacy protection is a multi-faceted concept that prevents personal data from being abused, leaked, or unauthorized access while ensuring that this information is used in a legal, transparent, and controlled environment. To achieve this goal, various measures must be taken, including formulating and improving relevant laws and regulations, implementing strict technical security measures, clarifying the boundaries of data use, and giving citizens access to and control over their data. This comprehensive protection mechanism not only safeguards individuals' privacy rights and interests but also creates conditions for the rational flow and use of data in society, thus achieving a balance between protecting individual rights and interests and promoting the development of informatization.

3 Necessity and Challenges of Digital Government Information Disclosure

In the digital age, the pattern of information disclosure is undergoing profound changes. With the advancement of digital transformation, government information disclosure is transforming traditional paper documents and face-to-face communication to electronic platforms and online services[6]. This transformation has dramatically improved the efficiency of information release and acquisition and reshaped the interaction model between the government and the public. Using Internet technology and digital tools, the government can disseminate information quickly and widely, and the public can access and supervise government information more conveniently and directly[7]. This digital way of information disclosure promotes the improvement of government transparency, opens up new channels for citizens to participate in public affairs, and promotes the government governance model to develop in a more open, interactive, and efficient direction[8] .

Digital government information disclosure first increases the speed of dissemination. Publishing information through digital platforms can achieve real-time updates, and the

public can obtain the latest policy trends and government information in the first place, significantly shortening the time for information dissemination[9]. Secondly, the cost of obtaining information has also been reduced to a certain extent. The public does not need to go to government departments or consult paper documents; they can obtain the required information through the Internet, reducing the time and economic cost of information acquisition. Finally, digital means allow information to cover a broader range of public groups, especially those in remote areas and those who need more timeline paper information, which increases the communication and transparency of government information.

Digital government information disclosure undoubtedly brings many conveniences to the public but also faces some challenges. The most prominent problem is the digital divide phenomenon[10]. The electronic release of government information requires the public to have specific digital skills and Internet access capabilities, and everyone does not still need this prerequisite. This situation may cause some citizens, especially the elderly, rural residents, or groups with poor economic conditions, to be disadvantaged in obtaining government information. In addition, digital government information disclosure also has the problem of information redundancy and overload [11]. Online information disclosure may lead to a large influx of information, making it difficult for the public to distinguish and understand the authenticity and importance of information. Finally, digital government information disclosure will simultaneously lead to the rapid spread of false and erroneous information. Due to the accelerated speed of information dissemination and the diversification of channels, erroneous, false, or unverified information will coexist, decreasing the public's trust in government information[12].

Digital government information disclosure is essential in improving government transparency and public participation. However, to ensure the effectiveness, fairness, and security of information disclosure, it is necessary to continue paying attention to and responding to various challenges and problems that arise in this process.

4 Necessity and Challenges of Privacy Protection in Digital Government

Digital government faces the problem of information leakage, so it is necessary to do an excellent job of privacy protection[13]. Digital government integrates government services through information technology to improve government work efficiency and service quality. However, at the same time, it also brings privacy risks and potentially threatens citizens' privacy rights. The digital government needs to collect a large amount of data, and the leakage of this data will lead to severe consequences such as identity fraud[14]. In the process of digital transformation, in order to improve the quality of public services and optimize social governance, the government inevitably needs to collect and process a large amount of citizens' personal information. Such an extensive database also brings potential risks. If this sensitive information is improperly used or leaked, it will seriously infringe on citizens' privacy rights and may even endanger per-

sonal safety[15]. Therefore, while promoting the construction of digital government, balancing data application and privacy protection has become a critical issue that needs to be solved urgently.

In addition, digital government also faces the challenges brought by cross-departmental data sharing. Cross-departmental data sharing is a double-edged sword in the construction of digital government[16]. On the one hand, it helps to break down traditional information barriers and promote collaboration among government departments, thereby improving administrative efficiency and public service quality. On the other hand, this data integration also brings new challenges. Cross-departmental data sharing may become a hotbed for data abuse without a sound management system and strict supervision mechanism. Departments may excessively call or improperly use citizens' sensitive information for convenience or other reasons, infringing on personal privacy rights[17]. For example, some non-essential departments may obtain citizens' medical records or financial status, which not only exceeds their authority but may also cause the information to be used for purposes other than what should not have been used.

5 The Contradiction between Digital Government Information Disclosure and Privacy Protection

In digital government construction, there are inevitable conflicts and contradictions between privacy protection and information disclosure[18]. Information disclosure aims to enhance government transparency and improve public trust and participation in the government, while privacy protection is to ensure the security of personal information and prevent it from being abused. This contradiction is mainly reflected in the following aspects.

First, the boundary between information disclosure and personal privacy is blurred. The balance between information disclosure and personal privacy protection is like a tightrope. On the one hand, the public expects the government to operate more transparently and requires sufficient information to monitor government behavior. On the other hand, the government is responsible for protecting citizens' privacy rights and ensuring that sensitive personal information is not improperly disclosed. This contradiction is particularly prominent in practice. For example, when publicizing government subsidy information, to what extent should it be disclosed? Only publishing the number of beneficiaries and the total amount may not meet the public's requirements for transparency; however, if each beneficiary's identity information and specific subsidy amount are listed in detail, it may excessively infringe on personal privacy.

Second, there is a conflict between public interest and personal privacy. Another thorny issue facing digital government is how to strike a balance between maintaining public interests and protecting personal privacy. This contradiction is particularly prominent regarding major social issues such as public safety and health. Taking the COVID-19 epidemic prevention and control as an example, the government's disclosure of the activity trajectories of confirmed cases can help the public take protective

measures promptly and effectively curb the spread of the virus[19]. However, this practice will inevitably expose the patient's personal information, which may cause them to suffer unnecessary social discrimination and psychological pressure.

Third, the public's perception of privacy and information disclosure is different. In the process of digital government construction, a challenge that must be addressed is that the public's perception of privacy protection and information disclosure is significantly different. This difference is not only reflected between different groups, but even at the individual level, it may vary depending on the situation. On the one hand, some public members strongly call for the government to increase transparency. They believe that only by fully disclosing government information can we effectively supervise government behavior, prevent abuse of power, and promote democratic governance. Such groups tend to support a broader range of information disclosure policies and are willing to sacrifice a certain degree of personal privacy in exchange for higher government transparency[20]. On the other hand, the public is susceptible to personal privacy protection. In the context of frequent data leaks, they are worried that excessive information disclosure may lead to violations of personal privacy. Such groups tend to support stricter privacy protection measures, even if this may limit the degree of disclosure of government information to some extent. What is more complicated is that the same person may hold contradictory positions in different situations. For example, a person may advocate transparency when asking the government to disclose details of its fiscal spending but attach great importance to privacy protection regarding their medical records.

6 Solutions for Digital Government Information Disclosure and Privacy Protection

The balance between information disclosure and privacy protection is crucial in the construction of digital government. Effectively protecting citizens' privacy while improving government transparency is a complex challenge. This requires the joint participation and cooperation of stakeholders such as the government, enterprises, and the public. To resolve the contradiction between privacy protection and information disclosure, the government can take a series of comprehensive measures.

First, improving the application level at the technical level can greatly promote the balance between information disclosure and privacy protection. Artificial intelligence technology for intelligent information screening and desensitization, blockchain technology to ensure the authenticity and immutability of information disclosure, and big data analysis technology to optimize information disclosure decisions are all feasible technical means[21]. At the same time, it is also indispensable to establish a safe and reliable information disclosure platform to ensure the security of information transmission and storage[22].

Second, improving the legal system at the legal level is an important cornerstone for ensuring information disclosure and privacy protection. The government needs to revise and improve relevant laws and regulations, clarify the boundaries of information disclosure and privacy protection, and formulate special regulations on data security

and personal information protection. Establishing and improving the regulatory mechanism for information disclosure and privacy protection, strengthening cross-departmental and cross-regional legal coordination, and eliminating conflicts in the application of laws are all important tasks at the legal level [23].

Finally, talent is the key to balancing information disclosure and privacy protection. Strengthening talent training and capacity building, cultivating professional information disclosure and privacy protection talents, carrying out data literacy training for civil servants, and raising awareness of information security is necessary. Establishing a cross-departmental information disclosure and privacy protection expert team and encouraging colleges and research institutions to conduct research and innovation in related fields will also provide intellectual support for long-term development.

Through the comprehensive application of technology, law, and talent, the government can achieve a better balance between information disclosure and privacy protection, both meeting the needs of the public interest and effectively protecting citizens' privacy rights. This requires long-term efforts and continuous cooperation from all parties to build a transparent, efficient, and secure digital government ecosystem. In this process, the government, enterprises, and the public need to work together, explore, and innovate continuously to truly realize the beautiful vision of digital government.

7 International Comparison and Reference

The balance between information disclosure and privacy protection is crucial in the construction of digital government. Effectively protecting citizens' privacy while improving government transparency is a complex challenge. This requires the joint participation and cooperation of stakeholders such as the government, enterprises, and the public. In order to resolve the contradiction between privacy protection and information disclosure, the government can take a series of comprehensive measures, among which it is essential to learn from international experience and pay attention to global trends. By comparing the experiences of different countries in digital government information disclosure and privacy protection, we can analyze their successful experiences and challenges and draw valuable lessons and experiences from them.

The UK's "Transparent Government" program is a successful case worth learning from[24]. Through this program, the British government vigorously promoted information disclosure and established a government data portal (data.gov.uk) to disclose many non-sensitive public data for the public and enterprises[25]. At the same time, the UK has strictly protected citizens' privacy through laws such as the Data Protection Act and the General Data Protection Regulation[26]. The British government also emphasizes data anonymization and strict access control and successfully achieved a balance between information disclosure and privacy protection[27]. This practice provides a valuable reference for other countries, showing how to promote information disclosure within the legal framework while protecting citizens' privacy rights.

However, there are also lessons from failure in developing digital government in various countries. The "health data leakage" incident in the United States is typical. In

promoting the electronicization of medical data, large-scale health data leakage incidents have occurred many times in the United States due to insufficient data protection measures. In 2015, the health insurance company Anthem suffered a data leakage, and the personal information of about 80 million customers was stolen by hackers[28]. The incident exposed the severe consequences of inadequate data protection measures in the context of large-scale information disclosure. Through this incident, the US government realized that in the process of informatization construction, it is necessary to strengthen data security measures, improve technical protection capabilities, and ensure privacy protection[29]. This lesson reminds us that we must attach great importance to data security and privacy protection while promoting information disclosure.

The controversy over India's "digital identity system" (Aadhaar) is also worthy of attention. As the world's largest biometric database, Aadhaar aims to improve the efficiency of government services through a unified identity authentication system [30]. However, the system faces serious privacy protection issues, including data leakage and unauthorized access. Due to ineffective data protection measures, the public and the international community have widely criticized the privacy protection of the Aadhaar system[31]. As a result, the Indian government passed the Personal Data Protection Bill in 2023 to strengthen personal data protection[32]. This case shows that when promoting large-scale digital projects, privacy protection must be taken as a core consideration, and a sound legal and technical guarantee system must be established.

By learning from international experience and paying attention to global trends, China can better balance information disclosure and privacy protection in constructing a digital government. This requires the joint efforts of the government, enterprises, and the public to continuously innovate and improve relevant policies, laws, and technical measures. Only in this way can we truly build a transparent, efficient, safe, and reliable digital government ecosystem that provides citizens with high-quality services while effectively protecting their privacy rights.

8 Conclusion

Digital government information disclosure and privacy protection are important issues in the digital age. Information disclosure aims to improve government transparency and credibility but also faces challenges such as the digital divide and information security. Privacy protection is to prevent the leakage of personal information, but it faces risks in large-scale data collection and sharing. There are contradictions between the two, such as the blurred boundaries between information disclosure and personal privacy and the conflict between public interests and personal privacy. Solving these problems requires a multi-pronged approach: establishing transparent information classification standards, promoting refined management, improving the level of technology application, improving laws and regulations, strengthening talent training, promoting international cooperation, and strengthening public participation. Learn from international experiences, such as the UK's "Transparent Government" plan, and learn from the lessons of the US health data leak. China can better balance information disclosure and privacy

protection in the construction of digital government and build a transparent, efficient, safe, and reliable digital government ecosystem.

References

1. Wang, Y., & Zheng, Q. (2020). Regulation of citizens' abuse of the right to apply for government information disclosure: Focusing on the deletion of the “three needs” clause. Open Journal of Legal Science, 8, 250.
2. Wang, L. M,, & Ding, X. D. (2021). On the highlights, features and applicability of the Personal Information Protection Law. Legal Scholar, 6, 1-16.
3. Karimullah, S. S., Sugitanata, A., & Elmurtadho, F. (2023). Juridical Analysis of Public Information Disclosure in Government Systems in the Digital Era. *Constitution Journal*, *2*(2), 1-18.
4. Zafarullah, H., & Siddiquee, N. A. (2021). Open government and the right to information: Implications for transparency and accountability in Asia. *Public Administration and Development*, *41*(4), 157-168.
5. Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.
6. Sandhu, K. (Ed.). (2021). *Disruptive technology and digital transformation for business and government*. IGI Global.
7. Milakovich, M. E. (2021). *Digital governance: Applying advanced technologies to improve public service*. Routledge.
8. Arshad, S., & Khurram, S. (2020). Can government’s presence on social media stimulate citizens’ online political participation? Investigating the influence of transparency, trust, and responsiveness. *Government Information Quarterly*, *37*(3), 101486.
9. Yao, F., & Wang, Y. (2020). Towards resilient and smart cities: A real-time urban analytical and geo-visual system for social media streaming data. *Sustainable Cities and Society*, *63*, 102448.
10. Sadigova, L. (2023). *E-Government and the Digital Divide: A Case Study of Azerbaijan's ICT Landscape* (Doctoral dissertation, K).
11. Saxena, D., & Yasobant, S. (2022). Information Overload. In *Encyclopedia of Big Data* (pp. 566-568). Cham: Springer International Publishing.
12. Lin, Y., & Zhang, S. (2021). The proliferation of fake news in network communication and the reconstruction of media credibility. *Academic journal of humanities & social sciences*, *4*(11.0).
13. Susanto, H., Yie, L. F., Setiana, D., Asih, Y., Yoganingrum, A., Riyanto, S., & Saputra, F. A. (2021). Digital ecosystem security issues for organizations and governments: Digital ethics and privacy. In *Web 2.0 and cloud technologies for implementing connected government* (pp. 204-228). IGI Global.
14. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.
15. Susanto, H., Yie, L. F., Setiana, D., Asih, Y., Yoganingrum, A., Riyanto, S., & Saputra, F. A. (2021). Digital ecosystem security issues for organizations and governments: Digital ethics and privacy. In *Web 2.0 and cloud technologies for implementing connected government* (pp. 204-228). IGI Global.

16. Zelin, X., Yang, Z., & Jieren, H. (2022). Cross-departmental Collaboration within the Government in China: The Case of Shanghai. *China: An International Journal*, *20*(1), 73-92.
17. Citron, D. K., & Solove, D. J. (2022). Privacy harms. *BUL Rev.*, *102*, 793.
18. Eom, S. J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly*, *39*(2), 101690.
19. Cheng, Z. J., Zhan, Z., Xue, M., Zheng, P., Lyu, J., Ma, J., ... & Sun, B. (2021). Public health measures and the control of COVID-19 in China. *Clinical reviews in allergy & immunology*, 1-16.
20. Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2021). Research on influencing factors of personal information disclosure intention of social media in China. *Data and Information Management*, *5*(1), 195-207.
21. Zhou, Z., Liu, X., Zhong, F., & Shi, J. (2022). Improving the reliability of the information disclosure in supply chain based on blockchain technology. *Electronic Commerce Research and Applications*, *52*, 101121.
22. Gupta, I., Singh, A. K., Lee, C. N., & Buyya, R. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. *IEEE Access*, *10*, 71247-71277.
23. Raul, A. C. (Ed.). (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.
24. O'Hara, K. (2011). Transparent government, not transparent citizens: a report on privacy and transparency for the Cabinet Office.
25. Gray, J., & Darbishire, H. (2011). Beyond access: Open government data & the right to (re) use public information. *Access Info Europe and Open Knowledge*.
26. Bell, J., Aidinlis, S., Smith, H., Mourby, M., Gowans, H., Wallace, S. E., & Kaye, J. (2019). Balancing data subjects' rights and public interest research: Examining the interplay between UK law, EU human rights law and the GDPR. *Eur. Data Prot. L. Rev.*, *5*, 43.
27. Stalla-Bourdillon, S., & Knight, A. (2016). Anonymous data v. personal data-false debate: an EU perspective on anonymization, pseudonymization and personal data. *Wis. Int'l LJ*, *34*, 284.
28. Moffit, R. E., & Steffen, B. (2017). Health care data breaches: A changing landscape. *Maryland Health Care Commission*, 1-19.
29. Gomez, J., Sensato, C. E. O., Konschak, C., & Divurgent, C. E. O. (2015). Cyber-security in healthcare.
30. Masiero, S. (2018). Explaining trust in large biometric infrastructures: A critical realist case study of India's Aadhaar project. *The Electronic Journal of Information Systems in Developing Countries*, *84*(6), e12053
31. Satpathy, T. (2017). The aadhaar: "Evil" embodied as law. *Health and Technology*, *7*(4), 469-487.
32. Collaco, A. M. (2024). Contours of data protection in India: the consent dilemma. *International Review of Law, Computers & Technology*, 1-19.