Comparative Study of Privacy Protection Policies on Open Government Data Websites (Postprint)

Authors: Zhang Jianbin, Huang Bingqing, Long Juanyong, Zhang Mingjiang, Zhou Zhifeng

Date: 2023-10-08T00:00:00+00:00

Abstract

[Purpose/Significance] Government open data portals serve as the platform for data openness, and their personal privacy policies directly determine whether individual privacy is adequately protected during the opening process. [Method/Process] To optimize personal privacy protection strategies for China's government open data portals and promote data openness, this study systematically compares domestic and international personal privacy protection policies for government open data portals across policy framework, personal privacy collection, sharing and use, and protection measures. [Results/Conclusion] The study proposes enacting comprehensive personal privacy protection legislation, strengthening professional training for government employees, enhancing supervision of personal privacy utilization in the government data openness process, standardizing external links, and implementing other measures to improve personal privacy protection strategies for China's government open data portals.

Full Text

Preamble

ChinaXiv Cooperative Journal *Academic Exploration*

Comparative Study on Personal Privacy Protection Policies of Open Government Data Websites

Zhang Jianbin[1], Huang Bingqing[1], Jun Yonglong[1], Zhang Mingjiang[1], Zhou Zhifeng[2]

Abstract

[**Purpose/Significance**] Open government data websites serve as the primary platform for data openness, and their personal privacy protection policies are directly related to whether individual privacy is adequately safeguarded throughout the data opening process. [**Method/Process**] To optimize personal privacy protection strategies for China's open government data websites and advance data openness, this study systematically compares domestic and international privacy protection policies across multiple dimensions, including policy frameworks, personal data collection, sharing and usage, and protective measures. [**Result/Conclusion**] The study proposes that China should enact comprehensive privacy protection legislation, strengthen professional training for government officials, enhance supervision over personal privacy utilization during the data opening process, and standardize external linking practices to improve privacy protection policies on open government data websites.

Keywords: open government data website; personal privacy protection; policy comparison

Classification Number: G202

Citation Format: Zhang Jianbin, Huang Bingqing, Jun Yonglong, et al. Comparative study on personal privacy protection policies of open government data websites [J/OL]. *Knowledge Management Forum*, 2017, 2(5): 390-397 [citation date]. http://www.kmf.ac.cn/p/1/658/.

The advent of the big data era has profoundly impacted government administration and catalyzed the movement toward open government data. As open data practices have expanded, both academia and practitioners have increasingly focused on theoretical and practical issues related to government data openness, making it a prominent field of study. Open government data first emerged in Western countries, where the United States, European Union, Canada, and Australia have achieved remarkable success. These nations have established dedicated open data portals as platforms for data release, promptly opening public service-related data to improve citizen services, enhance public awareness of policies, and promote democratic dialogue through public participation. China has closely followed the pace of Western nations in national data openness. Building on experiences from government information disclosure practices, China released the *Outline for Promoting Big Data Development* in 2015, mandating the establishment of a unified national government data open platform by the end of 2018. Several provincial governments (including Zhejiang, Guangdong, Guizhou) and sub-provincial cities (such as Wuhan, Guangzhou, Shenzhen, and Qingdao) have subsequently launched their own open data platforms to promote administrative transparency and deliver data-driven benefits to citizens, creating new models of governance.

However, as open government data initiatives have deepened, privacy protec-

tion concerns on these platforms have garnered increasing attention. Government data often involves citizens' personal privacy, and governments may collect privacy-related information to deliver quality services. Personal privacy refers to personally identifiable information. In the context of open government data, privacy breaches primarily occur in three stages: source leakage (information collection), process leakage (information sharing and use), and result leakage (information security). Therefore, this comparative study of Chinese and foreign open government data website privacy policies focuses on these three aspects, aiming to provide valuable insights for optimizing China's privacy protection policies and advancing data openness practices.

1. Challenges of Open Government Data to Privacy Protection

Open government data websites differ from other government portals in several key aspects: they emphasize government proactivity and service orientation, prioritize user-centered design, focus on personalized service experiences, and provide complete datasets to users. The establishment of these platforms and the advancement of data openness have introduced new challenges to personal privacy protection, primarily in four areas:

1.1 Increased Privacy Risks from Government Data Reuse

Data published on open government platforms is typically freely accessible, providing convenient conditions for public utilization, particularly by enterprises. For example, Zhejiang's government service portal features a "Credit Information" section that discloses citizens' professional qualifications, including information on cultural brokers, medical practitioners, and nurses. The open data includes names and certification dates, which companies can leverage to develop query systems. Moreover, under real-name registration requirements for phone services, some businesses may obtain detailed citizen information from telecom companies for commercial purposes once they have citizens' names, potentially triggering privacy breaches.

1.2 Privacy Leakage Risks from Government Departments and Officials

Open government data websites contain substantial amounts of citizen personal privacy, including: privacy inherent in government public databases; information captured through cookies about citizens' browsing activities; and personal details citizens provide when registering to access public services. Government departments and officials are the primary entities that access and manage this information. Inadequate government control, inconsistent understanding of privacy standards, insufficient information literacy among officials, or poor professional ethics can all create risks of citizen privacy leakage.

1.3 Enhanced Privacy Risks from Big Data Mining Technologies

With the widespread application of big data technologies, data mining can analyze seemingly unrelated fragmented information to establish correlations, potentially infringing on citizen privacy without their awareness. Big data has facilitated the formation of privacy information markets, which, while not initially intended to violate privacy, often produce that outcome [1]. Big data enables cross-validation of data content, making privacy protection increasingly difficult through technical means alone. Government open data platforms publish public service information that inherently contains personal privacy, creating opportunities for commercial enterprises to extract valuable personal information using big data mining techniques.

1.4 Information Security Issues Triggering Privacy Leaks

With the rapid development of information and communication technologies, intrusion techniques continue to evolve, enhancing the capability to attack specific websites. Citizens must provide some personal privacy to access public services or consult with government agencies, meaning open data platforms hold large volumes of personal information. Although current platforms claim to implement adequate technical safeguards, risks remain. Once a website is breached, irreparable damage to personal privacy may occur, with massive theft or infringement of private information. This concern has made some government departments hesitant and cautious about data openness. The tension between open government data and privacy protection requires governments to take robust measures to prevent information security crises.

2. Comparative Analysis of Privacy Protection Policies on Open Government Data Websites

Through investigation of national and local government websites with well-developed open data practices, this study examines their published privacy policies to systematically compare how different governments protect personal privacy during data openness, aiming to provide valuable recommendations for advancing China's open data initiatives. Foreign governments selected include early and successful practitioners: the United States, European Union, Canada, and Australia. Domestic cases include provincial governments (Beijing, Shanghai, Zhejiang, Guangdong, Guizhou) and sub-provincial cities (Wuhan, Guangzhou, Shenzhen, Qingdao) that have established operational open data platforms.

2.1 Overall Comparison of Privacy Protection Policies

Website investigations reveal that most open government data platforms, both domestic and foreign, have established privacy protection policies. Some Chinese local government platforms embed privacy policies within disclaimers, as

seen in Qingdao and Guangzhou. From a public policy perspective, policy quality directly affects implementation and enforcement. The completeness and specificity of privacy policy content directly influence the strength of privacy protection and policy execution.

According to EU standards, a comprehensive and detailed privacy policy should include: what information is collected, to whom it is disclosed, how citizens can access their information, how long information is retained, what security measures are implemented, and contact information for inquiries [2]. Detailed review of various government policies shows that the United States, EU, Canada, Australia, and Guizhou Province have explicitly stipulated procedures for collection, processing, disclosure, use, and protection of personal privacy. Shanghai specifies exceptions to collection and sharing, while Zhejiang and Guangdong regulate sharing and protection measures. Beijing, Wuhan, Shenzhen, Guangzhou, and Qingdao simply state respect for user privacy and pledge not to proactively disclose personal information to third parties without user consent or legal mandate.

A notable difference is that Western countries have enacted specialized privacy protection laws, providing clear legal foundations for their open data privacy policies. While China has issued sector-specific personal information protection regulations, such as the 2012 *Decision on Strengthening Network Information Protection*, it lacks comprehensive privacy protection legislation. Consequently, Chinese local government open data platforms lack explicit legal basis for privacy protection, merely referencing relevant internet management laws and regulations. Some governments have enhanced citizen privacy awareness by including reminders in privacy statements, such as advising citizens not to disclose sensitive information or to review privacy policies of externally linked sites. Another significant distinction is that Chinese government platforms explicitly disclaim responsibility for privacy breaches resulting from information security or reuse, a provision absent from foreign government websites.

2.2 Comparison of Personal Data Collection Policies

Information collection represents the source of privacy leakage. The amount of personal data collected directly correlates with potential harm from privacy breaches. The United States, EU, Canada, and Australia generally specify what personal information will be collected or what citizens must provide to access public services.

In the United States, when users visit open data websites, the platforms do not proactively collect personal information unless voluntarily provided, but do collect IP addresses, access times, searched filenames or keywords, clicked items, and operating systems and browsers used [3]. Websites use cookies for technical purposes, but users have the autonomy to refuse cookie collection without affecting service experience. When communicating with the government, users may optionally provide email addresses without supplying additional personal

information, particularly Social Security Numbers. A unique feature of U.S. practice is that when users represent federal, state, local, or judicial agencies, or NGOs seeking administrative privileges, the website collects names, organizational affiliations, titles, business addresses, office phone numbers, and email addresses. Unlike other governments, the U.S. specifically addresses minors' privacy protection in separate privacy statement sections.

In the EU, users can access most websites without providing any information. However, to access e-government services (information services, interactive communication, and transaction services), citizens must provide personal information. In Canada, IP addresses are protected as personal information because, while not personally identifiable alone, they can identify individuals when combined with other data such as access times. Canadian open data websites adhere to principles of consent and recognition, seeking information subjects' approval before collection and informing them of collection purposes and their rights to correct information, with personal information collection statements provided in certain circumstances [4]. Personal information is collected when users communicate via email or complete feedback forms.

In Australia, users need not provide personally identifiable information to access services, but when contacting the government or requiring feedback, the government collects identifiable information such as email addresses, names, and phone numbers. Websites use cookies to collect user preferences for site analysis and service improvement, and while users can refuse cookie collection, unlike in the U.S., this may affect service experience.

Chinese local government platforms exhibit varying collection policies, ranging from detailed, high-quality policies like Guizhou's to vague, general statements like those from Beijing, Guangdong, Zhejiang, Wuhan, Shenzhen, Guangzhou, and Qingdao. When users visit the platform, Guizhou collects the same scope of information as the U.S. government: IP addresses, access times, searched filenames or keywords, clicked items, and operating systems and browsers. Similar to Australia, Guizhou uses cookies to collect user preferences for site analysis and service improvement, allowing users to disable cookies though this may affect service access. When registering, customizing services, or participating in surveys, users must provide extensive personal information that must be authentic, including but not limited to name, gender, ID number, phone number, email address, occupation, and education level [5]. Shanghai allows browsing and downloading all content without registration, but requires personal information when users publish data applications or communicate with government departments.

This analysis reveals that when citizens access personalized public services or interact with government through open data platforms, governments collect personal privacy information such as names and email addresses to understand user preferences and needs, enabling more precise and satisfactory service delivery. However, extensive collection of citizen personal data by open data platforms may create privacy leakage risks.

2.3 Comparison of Personal Data Sharing and Use Policies

In current Chinese practice, most privacy leaks occur during the sharing and use stage, making policies in this area critical for privacy protection. In the United States, the government shares some personal information with third-party institutions for scientific research purposes, such as user access information, IP addresses, and access times. Additionally, when public services involve multiple government departments or legal requirements, personal information is shared with relevant agencies.

In Canada, the government generally does not disclose user personal information to anyone unless required for government employees to perform their duties. When users select services provided by other government departments or agencies, they must review those agencies' privacy notices. Personal information collected through interactive communication is used for government statistics, evaluation, and reporting. In the EU, when citizens provide personal information to access e-government services, departmental privacy controllers review processing methods and purposes to ensure compliance with privacy policy requirements. In Australia, the government does not share personal privacy with other departments except to prevent illegal activities or serious threats to health and safety. Unlike the U.S., EU, and Canada, when providing cross-departmental services, Australia does not share citizen information with relevant departments unless the citizen consents or the law requires it, instead informing citizens of relevant processing opinions and which departments to contact for services [6].

Shanghai regulates data reuse behavior on its open data platform, requiring users to accept the platform's user agreement and pledging not to provide, sell, lease, share, or trade collected personal privacy with any third party, except when necessary to provide effective responses to users [7]. Guizhou explicitly lists purposes for collected personal privacy: (1) verifying user identity and providing corresponding services; (2) informing users of relevant information via email or other means; (3) executing user instructions and responding to inquiries, suggestions, or reports; (4) using information for specific purposes provided by users, such as participating in online surveys. Similar to Australia, Guizhou provides principles for restricted use, limiting the use of collected personal privacy when user consent has been obtained or when serving public interests without harming users' major interests [5].

Beijing [8], Wuhan [9], Shenzhen [10], Guangzhou [11], and Qingdao [12] share identical personal privacy sharing policies, stating that without user permission or mandatory legal provisions, the platforms will not proactively disclose user personal information to any third party. Zhejiang [13] and Guangdong [14] have similar sharing policies, explicitly stipulating that collected personal privacy will not be provided to third parties except with user consent and confirmation, as required by national laws and regulations, or to protect the legitimate rights and interests of the open data platform, while also allowing joint use with relevant government departments as needed. This indicates that Zhejiang and

Guangdong's sharing policies are significantly weaker than those of other Chinese provinces.

This analysis reveals that although policies vary across countries, commonalities exist. Except for the U.S., which discloses information for research purposes, governments generally adopt proactive privacy sharing policies and do not actively disclose or share personal privacy with third-party institutions or individuals. Sharing and utilization of personal privacy are based on public needs, including meeting citizens' personalized service demands, protecting public interests or health and safety, and exercising public authority. While some scholars claim that notice-and-consent privacy protection strategies have become ineffective in the big data era [15], governments bearing public responsibility must differ from private enterprises in handling citizen personal privacy, respecting and protecting citizens' privacy rights. Consequently, most governments and organizations have established information subjects' consent and permission as a fundamental principle for personal privacy sharing and use.

2.4 Comparison of Personal Privacy Protection Measures

The strength of government privacy protection directly determines the risk and harm of privacy leakage. As government-hosted, certified facilities, open data platforms bear responsibility and obligation to ensure security. All platforms have established privacy protection measures, though with varying detail and strength. In the United States, data websites remind users not to provide personally identifiable information such as email addresses or phone numbers when posting online comments. The U.S. government emphasizes privacy impact assessments, evaluating systems that collect personally identifiable information and reviewing whether privacy is adequately protected. The U.S. strengthens cybersecurity through physical, electronic, and procedural safeguards, strictly restricting illegal attacks or unauthorized uploads or modifications, with penalties under computer crime, abuse, and national information infrastructure protection laws.

In Canada, the government uses software programs to monitor and identify harmful attacks involving uploads or modifications, sharing this information with law enforcement to optimize security strategies and enhance protection levels. In Australia, the government employs physical, technical, and administrative measures to protect collected personal privacy, continuously updating and testing security technologies. To ensure privacy security, Australia emphasizes confidentiality training for employees, strictly limiting government officials' use of citizen personal privacy even when necessary for public service delivery. Under the EU's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) and *Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (2012), each government department has designated data protection officers to ensure strict implementation of personal data protection laws and provide recommendations

to departmental data controllers. Additionally, the EU has established an independent Data Protection Supervisor as an oversight agency separate from all government departments, specializing in monitoring government privacy protection.

Chinese local governments employ varying privacy protection strategies. Shanghai utilizes existing technologies to protect the open data platform and all stored and transmitted user data, legally pursuing responsibility for leaks caused by computer viruses or other illegal software [7]. Guizhou, Zhejiang, and Guangdong adopt technical measures to properly safeguard personal privacy collected on open data platforms, taking necessary measures to reduce user losses from leaks caused by force majeure, computer virus infections, or hacker attacks. Beijing, Wuhan, Shenzhen, and Guangzhou simply mention respecting and protecting all users' privacy rights without providing specific protective measures. Qingdao's approach is distinctive: because linking multiple datasets may cause privacy leakage, the platform reserves the right to remove such data at any time, and the public may not continue to save or use the data for any reason; when using platform data and services, the public must comply with relevant laws and regulations and may not use the data for any purpose that may infringe on personal privacy [12]. Additionally, to provide quality public services, open government data platforms provide numerous external links. Since external websites have different privacy protection strategies, governments both domestically and internationally generally remind users in privacy statements to review the privacy policies of externally linked sites.

This analysis reveals that unlike foreign governments that employ multiple protection measures, Chinese local government open data platforms rely primarily on single technical protection methods. Moreover, regarding incidents of privacy leakage caused by illegal website intrusions, Chinese governments have not fully utilized legal means to pursue responsibility.

3. Recommendations and Implications

Foreign governments have implemented numerous privacy protection measures in advancing open data practices, many of which provide valuable lessons for China. To further improve personal privacy protection in open government data and advance data openness, China needs to adopt the following measures beyond existing technical protections:

3.1 Formulate Comprehensive Privacy Protection Legislation

The United States, Europe, and other countries and organizations have clear personal privacy protection laws governing privacy protection in open government data. Comprehensive privacy laws explicitly define the scope of protected privacy. For example, EU personal data protection law specifies that ID numbers, location data, online identifiers, and physical, psychological, genetic, mental, economic, cultural, and social identities are legally protected [16]. Privacy pro-

tection laws can clearly define protection scopes, regulate collection and sharing behaviors of organizations including governments, and require collectors and users to implement protective measures. During legislation, emphasis should be placed on quality, with detailed enumeration of protected information, including: (1) information related to citizens' addresses, ID numbers, photos, contact details, educational backgrounds, work histories, and marital status; (2) health information, medical histories, and fingerprints; (3) political views, transaction records, and criminal records; (4) correspondence, emails, and diaries; (5) driver's license numbers, traffic records, and communication records. Legislation should also stipulate principles of legitimate and reasonable purposes for collecting and using personal privacy, with exceptions for cases involving information subjects' health, public interests, or safety where personal privacy may be used without consent, and information related to criminal facts should be excluded from legal protection. Additionally, laws should detail and quantify harms from privacy leakage to facilitate judicial practice and penalize harassment using others' privacy that does not cause substantive damage. National comprehensive personal protection legislation would provide clear foundations for privacy protection policies on open government data websites, further enriching and improving policy content and quality.

3.2 Strengthen Professional Training for Government Officials

Government officials engage in a special profession and should be "professional citizens" and responsible administrators [17]. The public holds role expectations for government officials, expecting good professional ethics and administrative responsibility. Formation of good professional ethics relies not only on internal self-discipline but crucially on external cultivation through extensive training to enhance officials' internal qualities. For example: (1) organize study tours to developed countries like the United States to deeply learn specific privacy protection practices in open government data, strengthening understanding of confidentiality importance and privacy protection; (2) conduct relevant training for government officials, inviting domestic and international experts in privacy protection research to teach officials how to protect personal privacy and the penalties for privacy leakage. By improving officials' professional ethics, they will consciously protect personal privacy encountered during data openness, effectively avoiding privacy leaks caused by negligence or mistakes.

3.3 Enhance Supervision of Personal Privacy in Open Government Data

To eliminate current situations where some government departments and officials sell, leak, or improperly use personal privacy information, this study recommends incorporating whether departments and officials holding personal privacy legally and reasonably collect and use such information into performance evaluations for unit leaders and staff as an important assessment indicator, linking evaluation results to rewards and penalties. Government departments and offi-

cials who illegally collect, leak, sell, or use personal privacy should be publicly criticized, and those causing damage to information subjects—whether material, mental, or personal safety—should be held legally accountable for civil and criminal liability. Additionally, drawing from institutional arrangements in China's government information disclosure practices, this study recommends establishing information protection officers within government information disclosure offices to specialize in supervising whether personal privacy is strictly and legally protected throughout the data openness process and conduct full-process reviews of personal privacy collection and use by government departments.

3.4 Standardize External Links on Open Government Data Websites

Open government data websites are government-established platforms providing convenient electronic services to citizens. To provide complete, quality public services, governments allow some social websites to link to open data platforms, enabling the public to quickly access needed services. As organizations bearing public responsibility, governments are the primary entities for privacy protection in data openness and have responsibility and obligation to establish licensing standards for external links and conduct reviews, prohibiting links to websites with inadequate privacy protection strategies to effectively avoid privacy leakage caused by external links on open government data platforms.

References

[1] COHEN J E. Privacy, visibility, transparency, and exposure[J]. *The University of Chicago Law Review*, 2008, 75(1): 181-201.

[2] Information contained in a specific privacy statement[EB/OL]. [2017-03-09]. https://ec.europa.eu/info/legal-notice_{en}#disclaimer.

[3] Privacy policy[EB/OL]. [2017-04-10]. https://www.data.gov/privacy-policy.

[4] Privacy[EB/OL]. [2017-04-10]. https://www.canada.ca/en/transparency/privacy.html?_{ga}=1.254538688

[5] Guizhou Provincial Government Data Open Platform Privacy Statement [EB/OL]. [2017-05-10]. http://www.gzdata.gov.cn/privacy.html.

[6] Privacy policy[EB/OL]. [2017-05-10]. http://data.gov.au/about.

[7] Shanghai Municipal Government Data Service Network Terms of Use [EB/OL]. [2017-05-10]. http://www.datashanghai.gov.cn/home!toUseProvisions.action.

[8] Beijing Municipal Government Data Resources Network Privacy Protection Statement [EB/OL]. [2017-05-11]. http://www.bjdata.gov.cn/gywm/mzsm/index.htm.

[9] Wuhan Municipal Government Open Data Service Network Privacy Protection Statement [EB/OL]. [2017-05-20]. http://www.wuhandata.gov.cn/whdata/disclaimer.jsp.

[10] Shenzhen Municipal Government Data Open Platform Privacy Protection Statement [EB/OL]. [2017-05-20]. http://opendata.sz.gov.cn/common/toserviceTerms.

[11] Guangzhou Municipal Government Data Unified Open Platform Privacy Protection Statement [EB/OL]. [2017-05-22]. http://datagz.gov.cn/data/sitelaw.htm.

[12] Qingdao Municipal Government Data Open Website Disclaimer [EB/OL]. [2017-05-24]. http://data.qingdao.gov.cn/data/interact/law.htm.

[13] Zhejiang Government Service Network Privacy Protection [EB/OL]. [2017-05-25]. http://www.zjzwfw.gov.cn/col/col42277/index.html.

[14] Guangdong Province Open Data Management Platform Privacy Protection Statement [EB/OL]. [2017-05-28]. http://www.gddata.gov.cn/index.php/Index/ArticleDetails/id/5.html.

[15] Mayer-Schönberger V, Cukier K. Big Data Era: The Great Transformation of Life, Work, and Thinking[M]. Translated by Sheng Yangyan, Zhou Tao. Hangzhou: Zhejiang People's Publishing House, 2013: 200.

[16] European Commission. Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation) [EB/OL]. [2017-06-10]. http://ec.europa.eu/justice/data-protection/document/review2012/com_{{{2012}}*{{11}}}{en}.pdf.

[17] Ding Huang. Outline of Western Administrative Theory[M]. Beijing: China Renmin University Press, 2003: 308-327.

Author Contributions: Zhang Jianbin: Responsible for drafting and reviewing the article; Huang Bingqing: Participated in information collection and translation of foreign government open data websites; Jun Yonglong: Responsible for information collection and processing of provincial government open data websites; Zhang Mingjiang: Responsible for information collection and processing of sub-provincial city government open data websites; Zhou Zhifeng: Responsible for proofreading the article and providing revision suggestions.

Note: Figure translations are in progress. See original paper for figures.