Information Security Risks Posed by Cloud Service Agreements and Countermeasures for Libraries and Information Institutions: Postprint

Authors: Huang Guobin, Zheng Xia, Wang Ting

Date: 2023-04-01T16:15:55+00:00

Abstract

[Purpose/Significance] The application of cloud services in libraries can effectively enhance their data storage and computing capabilities; however, it also introduces numerous information resource security issues, and the non-standardization of cloud computing service agreements further exacerbates the information security risks faced by libraries.

[Method/Process] This study selects service agreements from eight representative cloud service operators as samples, focusing on information security-related clauses in cloud service agreements, and conducts an in-depth analysis of the information security risks present in current cloud service agreement clauses from five dimensions: data collection, data storage, data transmission, data access, and service security.

[Results/Conclusion] The information security risks that libraries may face when adopting cloud services include: absent content in cloud service agreements, making it difficult to ensure definite protection of user information security; ambiguous wording in cloud service agreements, with no well-established security safeguard mechanisms; and the formulation of cloud service agreements being more favorable to cloud providers, rendering user rights susceptible to infringement. In this context, libraries should further clarify the ownership of library user data and emphasize the security of library information resources.

Full Text

Information Security Risks Caused by Cloud Service Agreements and Countermeasures for Library and Information Institutions

Huang Guobin[1], **Zheng Xia**[1], **Wang Ting**[2]
[1]School of Government, Beijing Normal University, Beijing 100875
[2]Capital Medical University Library, Beijing 100069

Abstract:
[Purpose/significance] The application of cloud services in libraries can effectively improve data storage and computing capabilities, but also brings numerous information resource security problems. The non-standardization of cloud computing service agreements further exacerbates the information security risks faced by libraries. [Method/process] This study selected service agreements from eight representative cloud service operators as samples, focusing on information security clauses in cloud service agreements. It conducted an in-depth analysis of current information security risks in cloud service agreement terms from five aspects: data collection, data storage, data transmission, data access, and service security. [Result/conclusion] The information security risks that libraries may face when applying cloud services include: incomplete cloud service agreement content making it difficult to ensure user information security; vague descriptions in cloud service agreements without established security guarantee mechanisms; and cloud service agreements formulated to favor cloud providers, making user rights vulnerable to infringement. In this environment, libraries should further clarify ownership of library user data and emphasize the security of library information resources.

Keywords: cloud service; service agreement; information security

Classification Number: G250.7
DOI: 10.13266/j.issn.0252-3116.2020.12.005

Since cloud computing was introduced to China in 2007, the industrial landscape has undergone dramatic changes and business models have become increasingly integrated, becoming an important driving force for technological development in the cloud services industry. According to statistics from the "Cloud Computing Development White Paper (2018)" [1] recently released by the China Academy of Information and Communications Technology, China's overall cloud computing market reached 69.16 billion yuan in 2017, with a growth rate of 34.32%, indicating a stage of rapid growth. Especially in recent years, with the active promotion of artificial intelligence, big data, and "Internet Plus," cloud computing technology is accelerating its penetration into government affairs, finance, transportation, industry, education, healthcare, and other fields, pushing China's cloud computing technology applications in various industries toward a period of vigorous development. Against this backdrop, applying cloud services to library business operations has become an inevitable trend. With

deepening development and application, cloud computing has brought profound changes to libraries in terms of software environment, hardware storage, application platforms, and service models, while also introducing numerous security issues that threaten the secure storage of library data resources, intellectual property protection, data confidentiality, user rights management, and access control management.

Cloud service agreements are service contracts formed through negotiation between cloud service providers and libraries, representing normative documentation that specifies the types and methods of services that cloud service providers can offer. Analyzing these agreements from the perspective of their content composition and basic modules can comprehensively reflect the service products and basic models that existing cloud service providers can offer to libraries, revealing the information security risks libraries face when applying cloud services. In view of this, this paper conducts content analysis of existing representative cloud services applied to libraries, focusing on their service agreements, to identify the types and consequences of information security risks that may arise from library application of cloud service products, and to provide targeted countermeasures combined with library business operations, aiming to provide reference and basis for library managers and users when selecting and operating cloud services.

2 Literature Review

In September 2019, the author searched CNKI, Web of Science, and other databases using “cloud service” AND “information security” as title keywords and found limited research on this topic both domestically and internationally. Domestic scholars’ relevant research can be mainly divided into the following aspects:

(1) Construction of cloud service platform information security systems. For example, Dai Tianfeng [2] elaborated on three principles for data information security system architecture: system classification principle, innovation principle, and resource integration principle, and proposed main approaches for building computer cloud service data information security systems. Additionally, against the backdrop of government information disclosure, many domestic scholars have conducted research on government data information security system construction based on cloud services, with representative works by Bi Jianhuan [3], Chen Jie [4], and Liu Qin [5], all of whom argue that in building government data information security systems based on computer cloud services, data mining technology should be scientifically applied, complete cloud service technical modules should be designed, and reasonable information security infrastructure plans should be formulated.

(2) Research on legal issues of cloud service information security. Ji Feng [6] believes that in the process of building cloud service platforms, digital libraries mainly face issues such as data resource security, copyright,

agreement sharing, and data location storage. He recommends introducing targeted policies and laws to strengthen secure storage and management of library information resources, setting different login permissions and access registration to ensure the integrity and confidentiality of library information resource services. Similarly, Liu Ping and Liu Chun [7] point out that although cloud computing technology effectively integrates library information resources, there are many security hazards. Therefore, both libraries and cloud service providers should ensure the integrity and confidentiality of information resources and properly manage user permissions and access control. Huang Guobin and Zheng Lin [8] analyzed cloud service agreement information security responsibility issues from four perspectives: privacy policy, disclaimer, agreement termination, and legal application based on cloud service agreements.

Compared with domestic scholars, foreign research focuses more on using empirical research methods to explore risk factors and countermeasures for information security issues in cloud service environments. S. T. Park et al. [9] divided security risk factors into information leakage risk, failure recovery risk, compliance risk, and service interruption risk, and conducted empirical analysis on the impact of these four factors on continuous adoption intention. Similarly, S. K. Madria [10] believes that the key factor hindering cloud service development at present lies in the security of data provided by cloud service providers, which may involve issues such as data storage, data replication, integrity verification, access control, risk assessment, and secure query processing. In response, A. N. Kang [11] proposed that cloud services should be used to strengthen enterprise information security, and the smooth implementation of the plan requires dual support from policy and technology. T. Halabi [12] designed a quantitative evaluation method for cloud security service performance and verified its applicability and evaluation result validity by applying it to three cloud service providers.

Comprehensive analysis of existing domestic and international research reveals that information security risk issues caused by cloud services have not yet received widespread attention from the academic community. Many scholars focus on construction plans and implementation strategies for cloud service information security systems, or summarize types of information security risks caused by cloud services based on practical experience. However, research analyzing information security risks from normative documents that better represent cloud service providers' service standards—that is, from the perspective of cloud service agreements—remains relatively rare. Currently, due to the introduction of cloud computing technology, large amounts of library information resources are no longer in libraries' own hands but are hosted on the "cloud," posing a great threat to the security and confidentiality of digital information resources. Based on this, this paper conducts content analysis of service agreements involved in cloud services applied to libraries to identify the information security risks libraries face.

3 Research Methods and Data Sources

Examining various information services that libraries can provide in cloud computing environments and the information security issues involved requires systematic investigation of product types and business areas involved in applying cloud services to libraries. Currently, cloud services applicable to libraries include both general cloud services designed for various industries and specialized cloud services specifically designed for libraries based on their business characteristics. General cloud services refer to standardized cloud service products designed for industry-wide needs, while library-specific cloud services are designed for library business needs, with main functions including hosting library management systems, discovery services, online databases, and statistical analysis tools. The author comprehensively investigated currently widely used general and specialized cloud service products for library business operations and the libraries using them, with results shown in Table 1 .

Table 1 Current Status of Major Cloud Services Applied in Libraries

Cloud Service Type	Cloud Service Provider	Representative Libraries
General Cloud Services	Google	Google Cloud Platform: Western Colorado State College Library [13], Ghent University Library [14], Eastern Kentucky University Library [15], etc.
	Amazon	Amazon Web Service: New York Public Library [16], Ohio State Library [17], York University Library [18], etc.
	Microsoft	Windows Azure [19]: Library of Congress, University of Maryland Library, etc.
	DuraSpace	DuraCloud [20]: Library of Congress, MIT Library, Cleveland Public Library, Georgia Tech Library, University College Dublin Library, etc.

Cloud Service Type	Cloud Service Provider	Representative Libraries
Specialized Cloud Services [21]	WorldShare Management Services	University of Birmingham Library, University of Twente Library, Mannix Library McGill University Library, Utrecht University Library, United Arab Emirates University Library, etc.
	ExLibris	Cambridge University Library, California State University Fullerton Library, Orange Coast College, City College of San Francisco Library, University of Sierra Leone Library, etc.
	Biblionix	Biblionix Apollo: McBride Memorial Library, Philadelphia-Neshoba County Library, Salado Public Library, etc.
	Innovative Interfaces	Sierra: University of California East Coast Branch Library, Australian National University Library, Huazhong University of Science and Technology Library, etc.

4 Analysis of Cloud Provider Service Agreements Applied to Libraries

By interpreting the privacy policies and terms of service of representative cloud computing service operators applied to libraries, this paper designed the "Core Content Overview of Cloud Service Agreements" shown in Table 2 from five perspectives of the data management lifecycle in cloud service processes: data collection, data storage, data transmission, data access, and service security. This overview provides textual analysis of service agreements from eight representative cloud service providers selected for this study, revealing the information security risks libraries face.

Table 2 Core Content Overview of Cloud Service Agreements

Data Lifecycle	Google [22]	Amazon [23]	Microsoft [24]	DuraSpace [25]	OCLC [26]	ExLibris [27]	Biblionix [28]	Innovative Interfaces [29]
Service Agreement Content	√	√	√	√	√	√	√	√
Storage Location	√	√	√		√	√		√
Data Security	√	√	√		√	√		√
Data Retention and Deletion		√	√		√	√	√	√
Encrypted Transmission		√						
Transmission Failure	√	√	√		√	√	√	√
Access Subject	√	√	√		√	√	√	√
Access Restrictions	√	√	√	√	√	√	√	√
Service Interruption	√	√	√		√	√	√	√
Service Termination	√	√	√		√	√	√	√

Data Life-cycle	Google [22]	Amazon [23]	Microsoft [24]	DuraSpace [25]	OCLC [26]	ExLibris [27]	Biblionix [28]	Innovative Interfaces [29]
Agreement Modification	√	√	√	√	√	√	√	√
Disclaimer and Liability Limitation	√	√	√	√	√	√	√	√

Note: "√" indicates that the cloud service provider's service agreement involves this core content.

4.1 Data Collection

Cloud provider service agreements involved in the data collection stage aim to clarify the specific content of user data to be collected, the main purposes of data collection, and the means or methods used for collection. Overall, information security statements in existing cloud service agreements for the data collection stage mainly include three aspects: collection content, collection purpose, and collection methods.

(1) Collection Content. Analysis of existing cloud service provider agreements reveals that user data collected by cloud providers mainly includes two types: first, identity information containing user personal data, such as name, account number, password, identification information, and contact details; second, usage trace data generated after users employ cloud service provider products, such as location information, device information, or other log data. For example, Amazon states in its service agreement that collected user data includes: personal data information provided by users to Amazon, specific types of data information automatically generated when users use products, and information from other sources (such as service providers, third-party partners, or public sources). OCLC stipulates that it does not forcibly collect user information but rather allows users to voluntarily choose whether to submit their personal data to the service platform. If users choose not to share their personal data, OCLC cannot provide more personalized service applications. ExLibris and Innovative Interfaces also make the same provisions as OCLC in their service agreements. Additionally, OCLC specifies the details of user personal information it collects, including user account information, personal profile information, professional background information, communication information, user-generated content, device and browser information, usage information, and transaction records.

Biblionix states: "Except for data provided by library clients, we do not collect or maintain any other data, including any updates, additions, or modifications directly or indirectly generated by users."

(2) Collection Purpose. Collection purpose refers to the goals or results that cloud service providers aim to achieve through relevant software or third parties after collecting user data. Among existing cloud service providers, Amazon, OCLC, ExLibris, Biblionix, and Innovative Interfaces all specify collection purposes in their service agreements. Generally, data collection purposes mainly include four types: necessary for services or products; improving services or products; marketing or advertising; other purposes. For example, Amazon stipulates: "We use your personal information to operate, provide, and improve Amazon products, such as completing Amazon services, improving or evaluating Amazon products, identifying user preferences and providing personalized products, and fulfilling legal obligations." Similarly, Innovative Interfaces will use collected user personal information to provide required information to users, help users register for seminars or academic exchange activities, send users content, communication information, or product services on topics of interest, and statistically identify website visitors to analyze user behavior. Meanwhile, OCLC additionally proposes that after obtaining user data, it may share user data with other third-party service providers, including cloud provider partner organizations, social media platforms, other OCLC affiliates, and national libraries, following data reasonable use rules during the sharing process and employing reliable security technology to protect user personal information from leakage.

(3) Collection Methods. Among existing cloud service providers, only OCLC, ExLibris, and Innovative Interfaces specify methods for collecting user information. For example, OCLC states that its main methods for collecting user information include: collecting information when users interact with OCLC and its subsidiaries, collecting information through users' computers or web browsers, obtaining information through user-authorized third-party sharing, or acquiring information through active user sharing. ExLibris mainly collects user information through three methods: collecting information during user registration, automatically collecting user information through technical means by cloud providers, and collecting user information through third-party organizations.

4.2 Data Storage

Cloud provider service agreements involved in the data storage stage aim to provide users with information about data storage location, format, and security to ensure high reliability and transparency of stored data. Overall, information security statements in existing cloud service agreements for the data storage stage mainly include three aspects: storage location, data security, and data retention and deletion.

(1) Storage Location. In cloud computing environments, users are unclear about the physical address of data storage. User data may be transferred by service providers to other countries or regions, or simultaneously stored in multiple countries or regions, leading to disputes under different judicial jurisdictions. Therefore, it is necessary to analyze relevant clauses in cloud service agreements regarding data storage location to understand the data security risks involved. Among existing cloud service providers, Google, Amazon, and Microsoft specify data storage locations in their service agreements, proposing that users can independently select data types, locations, and geographic regions for storage. If users do not set a data storage location, cloud service providers will automatically store user data content according to actual conditions. Microsoft explicitly states in its agreement that personal information collected through Microsoft sites and services may be stored or transferred to any country or region where Microsoft headquarters, branch offices, or subsidiaries are located. This obviously exposes user data to issues of how to coordinate management across multiple jurisdictions, and differences in legal systems and levels of legal protection across countries or regions also exacerbate user information security risks. Relatively speaking, Amazon's provisions are more user-friendly, stating in Section 3.2 of its user service agreement: "You can set the region for personal data storage yourself. We will not transfer your data to other countries or regions without permission, unless required to comply with laws or government requests." This allows users to select storage regions with different levels of legal protection according to their needs. However, for cases where user data storage location must be transferred, details regarding the form and timing of notification are not explicitly mentioned in Amazon's agreement.

(2) Data Security. In cloud computing environments, data storage locations shift from local disks to networks. This means users are not the sole owners of data; service providers also own this data, creating significant insecurity for users. Especially for library users, once data is stored in the "cloud," neither the library nor its users are the de facto data owners and processors. Cloud service providers possess permissions that even exceed those of library users. Once these permissions are 失控, they will affect library users' data privacy.

Among the eight analysis samples selected in this study, except for DuraCloud, the other seven cloud service providers mention data security provisions in their service agreements. Generally, cloud service providers should provide physical security measures and technical security measures for data. Specifically: Physical security measures refer to security protection of equipment and facilities through physical isolation. For example, Google states in its service agreement: "Equipment and facilities used for storing and processing user data must follow security standards to improve the security and confidentiality of user data, prevent user information from unnecessary threats that reduce data integrity, and prohibit access to and storage of user data using unauthorized facilities or applications." Technical security measures refer to protection of user accounts or associated passwords through digital encryption technology, such as key services, permission management, and firewall technology. For example, Amazon

provides data encryption functions for stored data and flexible key management options, allowing users to choose to control storage content themselves or entrust Amazon to ensure data security. Additionally, OCLC and ExLibris have established user data security protection procedures to prevent unauthorized illegal access, disclosure, alteration, destruction, or processing of user data.

It should be noted that although most cloud service provider agreements involve data security provisions, they only provide general provisions without detailed protection plans. Specifically, Biblionix and Innovative Interfaces explicitly state in their service agreements that they cannot guarantee absolute security of user-stored data and do not mention handling plans for data loss or deletion caused by accidents, posing significant security risks to user-stored content.

(3) Data Retention and Deletion. In cloud computing models, various types of library data are randomly stored in virtual data centers at different physical locations, weakening users' control over their personal data. Even after users delete data, some service providers may still retain copies of this data, significantly increasing the risk of user privacy rights being violated. Therefore, it is necessary to further analyze relevant provisions in existing cloud service agreements regarding data retention and deletion.

Among the eight research samples selected in this study, except for Google and DuraCloud, the other six cloud service providers provide relevant explanations for data retention and deletion. From the perspective of data deletion, existing cloud service providers all state that users can retain or delete personal information at any time. For example, Microsoft states in its service agreement: "When your subscription service expires or is terminated, we will continue to retain your customer data for at least 90 days so you can extract it. In free trial service functions, we can delete customer data immediately without a retention period." However, some cloud providers do not specify time limits for data retention or deletion. For example, OCLC states: "We will retain your information according to service agreement provisions and fulfill storage content supervision obligations in accordance with legal rules. If storage content is no longer subject to legal effect, we will destroy or delete user information, or convert it into anonymous form for continued retention." Additionally, although Amazon mentions in its service agreement that it will delete information upon user account cancellation as requested by users, it does not provide definitive explanations regarding whether data can be completely deleted or whether company servers will still retain user data. This undoubtedly exposes users to the risk of privacy rights infringement. Similarly, Biblionix explicitly states in its service agreement: "To ensure the normal operation of library information systems, Biblionix will perform multiple backups of all data information (including user data). Even if user-stored data has been deleted from the repository, it cannot completely delete all data backed up in system backend storage media. However, all backup information stored in storage devices will be encrypted and protected."

4.3 Data Transmission

Cloud provider service agreements involved in the data transmission stage aim to clarify whether the data transmission process is protected by encryption to ensure reliable and secure transmission content; what force majeure threats may be encountered during information transmission that could cause transmission failures; the targets and objects of information transmission; and users' right to know and control during the information transmission process. Information security statements in existing cloud service agreements for the data transmission stage include two aspects: encrypted transmission and transmission failure.

(1) Encrypted Transmission. Regarding encrypted transmission, only Amazon explicitly states in its service agreement: "When you transfer data to Amazon websites, applications, and other service platforms, we use encryption protocols and software to ensure information transmission security." The other seven cloud service providers do not explain the technologies to be used for encrypted data transmission. However, even if cloud service operators adopt encryption technology, it can only ensure data remains encrypted during transmission. When storing and processing data, it is highly susceptible to access by other service providers or business partners, exacerbating the risk of user information leakage.

(2) Transmission Failure. Transmission failures mentioned in cloud service agreements can be divided into two types: first, failures caused by damage to computer systems, hardware, or software; second, data transmission failures caused by viruses or worm infections. It should be noted that cloud service providers do not explain solutions for transmission failures caused by the above reasons, defaulting to users bearing information security risks themselves. For example, Google states in its service agreement: "Neither service providers nor users need to bear responsibility for inability to perform or delayed performance of agreement content caused by force majeure." OCLC states: "When uncontrollable accidents such as fire, explosion, and communication failure occur, neither users nor cloud service suppliers need to bear responsibility for any inability to perform or delayed performance of agreement content." Amazon stipulates: "If we delay or fail to perform any obligations stipulated in the agreement due to various uncontrollable factors (such as natural disasters, labor disputes, public utility equipment failures, earthquakes, storms, etc.), neither we nor our service affiliates shall bear any responsibility for this."

Hackers and viruses are fatal factors threatening network information security in the cloud computing era. "Cloud" services highly integrate various types of digital resources from libraries across different regions, and the cloud environment is extremely complex, greatly increasing opportunities for hackers to steal or misuse library data by exploiting security vulnerabilities in cloud environments. These threats can even rapidly spread to computer systems of other users connected to the "cloud computing" system, causing greater losses. In addition to security risks brought by hackers and viruses, hardware systems can

also cause information leakage. For example, information in computers may leak through electromagnetic waves, and external network communication lines may be intercepted or monitored.

4.4 Data Access

When users upload data to the cloud, it directly weakens their control over the data. In cloud service models, users are no longer the sole accessors of data. Cloud service company employees and partners may all access user data, and if enterprises are involved in mergers, acquisitions, or other transactions, they may transfer user data as personal assets, giving companies involved in transactions with the enterprise the right to access user data, thereby increasing the risk of user data leakage. Cloud provider service agreements involved in the data access stage aim to clarify the subjects of data access, usage methods, possible service interruptions or terminations during use, and corresponding rescue measures. Current cloud service agreements' information security statements for the data access stage involve access subjects and access restrictions.

(1) Access Subjects. Provisions regarding access subjects in cloud service agreements aim to specify individuals or organizations authorized to access user data or service product content. Clarifying permissions of access subjects under different application scenarios is of great significance for the privacy security of user-stored information. According to existing cloud service provider agreements, data content access subjects can be divided into three types: users, cloud providers, and third-party organizations. For example, Amazon stipulates in its service agreement that users can access and use service products according to the service agreement and should comply with service agreement terms and all laws and regulations during access. It also states: "Except as necessary to provide services requested by users and as required by relevant laws and regulations, Amazon will not arbitrarily access or use user data, or disclose user data to any third party." Microsoft states: "We do not allow third-party organizations (including law enforcement agencies, government agencies, or civil litigants) to access user data. If disclosure of user data is required under special circumstances, we will immediately notify users to provide copies of their data."

However, cloud service provider agreements do not mention management and verification measures for accessor identities, causing libraries to face information security issues due to unclear identity management, access control, and user permissions by cloud service providers. In cloud computing models, libraries are no longer the sole owners of data, and cloud service providers often have the same data. Driven by certain economic interests or political purposes, some cloud service providers may access data stored by libraries in cloud service provider systems in unauthorized ways unknown to libraries, infringing on library users' privacy and causing irreparable consequences to libraries. Moreover, data in the "cloud" is in a highly shared environment. Without reasonable user access control and effective management of information operation permissions, library data is highly likely to be illegally accessed.

(2) Access Restrictions. Access restrictions refer to reasonable restrictions on data access processes, methods, and subsequent use during the data access stage. They form the basis and foundation for users to legally fulfill information restriction clauses and are of great significance for users to ensure information security and personal privacy during data access. Specifically, access restrictions include usage rights, license restrictions, and copyright policies: Regarding usage rights, Google proposes: "Except when necessary to provide services to users, we will not arbitrarily access or use user data." Regarding intellectual property rights, most existing cloud service providers have proposed relatively detailed copyright policy provisions. For example, Google states that it owns intellectual property rights to cloud services and all software, while handling user data copyright issues will follow the Digital Millennium Copyright Act and help copyright owners manage their intellectual property rights online in real time. Meanwhile, if users believe others have infringed their intellectual property rights, they can submit relevant complaints through Google's official website at any time to seek assistance from Google's backend. Amazon provides relatively detailed intellectual property provisions, requiring users to strictly comply with restriction conditions stipulated in the service agreement. If intellectual property disputes occur, users shall be responsible. DuraCloud states that it will grant users permanent, global, non-exclusive, free copyright licenses for reproducing, displaying, publicly performing, or redistributing copyrighted works. ExLibris, Biblionix, and Innovative Interfaces all propose that all content on their websites (including text, images, logos, etc.) is protected by copyright, and no entity may arbitrarily access, modify, or copy service content without website permission. Regarding service product licenses, Amazon grants users a limited, non-exclusive, revocable, non-transferable usage license. Users must follow agreement provisions when accessing and using cloud service provider services and may not obtain intellectual property rights to service products.

4.5 Service Security

In addition to the above modules, existing cloud service providers also make relevant provisions for service security in their service agreements. Service security mentioned in cloud service agreements aims to explain how service providers ensure user information security during service provision, how they handle data loss or deletion caused by accidents, and also includes operators' disclaimers or liability limitations for fulfilling their responsibilities.

(1) Service Interruption. Cloud computing is an Internet-based computing model with very strong network dependence. The vast majority of service agreements provided by existing cloud service providers stipulate that if content published by users or their operational behaviors violate reasonable use rules, cloud service providers will notify users within a specified time, requiring them to correct violations or suspending some or all functions of users' cloud service products. For example, Google stipulates: "If users fail to correct violations within 24 hours as required by Google, Google may suspend some or all func-

tions of this product." OCLC's provisions on service interruption are relatively vague, stating: "If users seriously violate these terms, OCLC will immediately take measures to suspend user access to the WorldShare platform." However, this agreement does not provide clear definitions of "violations," undoubtedly giving the service provider considerable discretionary power.

In addition to service interruptions caused by users' violation of service products, in business practice, sudden events such as power outages and earthquakes, or software failures, hardware aging, and human operation errors may all cause network failures. Once network failures occur, cloud computing services will be interrupted, and libraries will be unable to work with the aid of cloud services. At the same time, if cloud computing service providers go bankrupt or are acquired by others, service interruption or instability will also result. Service security also includes the legality of service agreements. Under cloud computing models, some service content provided by cloud service providers to libraries may not completely match service agreements. Once operators intend to stop certain services, users cannot transfer their data in advance because they have not received notification, which also brings security risks to libraries.

(2) Service Termination. Similar to relevant provisions on service interruption, most service agreements provided by existing cloud service providers also propose that if users' operational behaviors violate service agreements, service providers will terminate users' use of some or all services or projects. In addition, Google supplements other situations that may lead to service termination, specifically including: If users have not used the cloud service platform or had other network activities for 60 days, and have not responded after Google provides 30 days advance notice, Google will terminate users' rights to use Google service products; For management convenience, either users or Google can terminate the service agreement at any time, and Google does not need to bear any responsibility to users. OCLC's provisions on service termination emphasize its own situation more, stating: "OCLC can partially or completely terminate users' use of the WorldShare platform at any time and for any reason without bearing any responsibility." Similarly, Biblionix states: "Biblionix can send users written notice of service termination at any time and for any reason with 120 days advance notice."

Regarding the consequences of service termination, different cloud service providers have made different explanations. For example, Google proposes that if services are terminated, it will return or delete all data stored by users on cloud servers. Similarly, Biblionix also proposes: "Biblionix should promptly delete or otherwise destroy all user data it owns or controls." However, Amazon stipulates: "We will not remove any data stored by users in Amazon systems due to service termination."

(3) Agreement Modification. Existing cloud service provider service agreements usually stipulate that if service agreements are updated or modified, cloud service providers should promptly send agreement modification explanations to users through their personal accounts or email addresses and encourage users to

take necessary protective measures to prevent personal information loss or deletion. However, different cloud providers have different explanations regarding advance notice time. For example, both Amazon and Google stipulate that if service providers modify service agreements, they should provide at least 90 days advance notice to users. Microsoft stipulates: "We may change service agreements from time to time. Unless security, legal, or system performance considerations require immediate deletion of user data, we will notify you 12 months in advance before updating or deleting any service functions." Both OCLC and ExLibris state in their service agreements that cloud service providers can change service terms on their own at any time and inform users by sending emails or posting service change announcements on service platform websites.

(4) Disclaimer and Liability Limitation. Disclaimers aim to clarify situations where cloud service providers do not need to bear responsibility for failing to fulfill service agreement content, while liability limitations specify legal means to limit the scope of responsibility for cloud service providers and users under specific circumstances. Analysis reveals that existing cloud service provider service agreements all contain relatively detailed provisions on disclaimers and liability limitations. Common requirements for disclaimers are: except for items explicitly stipulated in service agreements, users shall be responsible for any losses resulting from violation of service agreements, and cloud service providers bear no responsibility for this. For example, DuraCloud stipulates: "Except as stated in this service agreement, we do not provide any express, implied, or other warranties, including warranties of merchantability or fitness for particular purposes."

Meanwhile, some cloud service providers provide detailed explanations of liability limitations in their service agreements. For example, Google elaborates on specific implementation plans for liability limitations from three parts: indirect liability limitation, liability cap, and liability limitation exceptions. Indirect liability limitation requires: "To the extent permitted by law, both Google suppliers and users will bear losses or indirect compensation according to this agreement." Liability cap requires: "To the extent permitted by law, users shall not pay Google amounts exceeding the rated liability payment within the 12 months preceding the event giving rise to liability." Liability limitation exceptions require: "The above liability limitations do not apply to situations such as one party infringing the other party's intellectual property rights, indemnification obligations, or customer payment obligations." Biblionix states: "Under any circumstances, Biblionix does not need to bear responsibility to users for subsequent compensation arising from this agreement."

5 Information Security Risks Caused by Cloud Service Agreements for Libraries

Based on the above analysis, information security risks that cloud service agreements may cause for libraries can be summarized into three categories:

5.1 Incomplete Cloud Service Agreement Content Makes User Information Security Difficult to Guarantee

Current cloud service agreements have vague descriptions, making it difficult to ensure library user information security. From the data collection perspective, although most cloud service providers explicitly propose provisions on data collection content, purposes, and methods in their service agreements, they do not clearly define relevant concepts, such as the conceptual scope of library user personal data. Additionally, some operators will collect user personal data through third-party service platforms but do not mention how to securely identify and authenticate their identities, giving different operators considerable freedom when actually collecting user personal data and posing significant potential threats to user personal information security. From the data storage perspective, most cloud service operators do not seem to consider it necessary to explain user data storage locations and transfer situations. Data storage or transfer is entirely determined by cloud service operators themselves. This will lead to continuous weakening of users' control over data during service processes and violates the user informed consent principle that should exist during transactions. More importantly, data storage and transfer relate to legal application issues when disputes occur. Arbitrarily storing user data in other countries or regions will significantly increase the legal liability of users using international cloud computing services.

From the data transmission perspective, currently most cloud service providers do not propose in their service agreements whether encryption technology or security standards are adopted during data transmission. Moreover, while emphasizing the use of multiple means to ensure data security during transmission, they include situations such as computer system, hardware, or software damage and other performance failures, virus and worm infections—which should be the responsibility of cloud service operators—in disclaimers, emphasizing that cloud service operators do not need to bear responsibility once these situations occur, and users bear the risks themselves. This is very unfair to users.

From the data access perspective, some cloud service agreements control access subjects and establish corresponding access control policies, but do not mention how to authenticate access subjects' identities or what laws should be followed to handle infringement acts if they occur during data access. This means that during data access, most access subjects can still freely access, utilize, and even abuse library data without being held responsible for their actions.

In summary, current cloud service agreement provisions are not comprehensive enough, have not provided solutions for information security issues, appear somewhat powerless when dealing with complex information security risk problems, and make it difficult to ensure user information security.

5.2 Vague Descriptions in Cloud Service Agreements, Without Established Security Guarantee Mechanisms

From the perspective of expression methods in cloud service agreements, existing cloud service provider agreements contain vague descriptions. From the data collection perspective, cloud service providers stipulate in their service agreements the methods and purposes for collecting user data, but some operators state in the collection purpose section of their service agreements that they will share user data with third-party organizations without clearly specifying whether this behavior aims to improve services or products or for other purposes.

From the data storage perspective, according to the above analysis, current cloud service provider service agreements ambiguously address the thoroughness and timeliness of data deletion. Additionally, some cloud service providers regularly back up data. This means that after a library user deletes personal data stored in the "cloud" through library-used cloud services, the data may still be recoverable through backups. Consequently, user privacy cannot be well guaranteed.

From the data access perspective, existing cloud service providers explain access subjects and restrictions in their service agreements, but there are still ambiguous expressions. For example, some operators stipulate: "If user data needs to be disclosed under special circumstances, we will notify users to provide copies of personal data," but they do not clearly define the scope and extent of personal data that users should provide in such cases.

Thus, current cloud service provider-drafted service agreements have vague descriptions, especially regarding the protection scope of user personal data security. They have not established sound user information security protection measures. Coupled with the fact that most users have insufficient information security awareness and do not realize the important role that cloud service agreements play in information security risk responsibility determination, few users actively check whether cloud service agreements have missing, ambiguous, or vague issues. This leads many users to directly use cloud services without understanding the relevant clause obligations in cloud service agreements, making them unable to seek compensation from cloud service operators when their information security suffers losses.

5.3 Cloud Service Agreements Favor Cloud Providers, Making User Rights Vulnerable to Infringement

In addition to the above analysis, existing cloud service agreements also have problems favoring cloud service providers, causing the balance of rights to tilt toward cloud service providers while users' legitimate rights are more vulnerable to threats. This problem is mainly reflected in provisions regarding service security in cloud service agreements. For example, from the service security perspective, the vast majority of cloud service agreements explicitly stipulate that cloud service operators do not need to be responsible if information security

is threatened due to service interruption or untimely service. Moreover, except for a few cloud service agreements, most do not explain service termination. This means that once cloud service operators unilaterally end cloud services without notifying users, causing user data damage, cloud service providers can also use the excuse that cloud service agreements do not contain relevant provisions to evade responsibility.

From the above analysis, it can be seen that current cloud service agreements are demanding toward users while including almost all situations that may lead to user data leakage and damage in disclaimers. The formulation of cloud service agreements is more favorable to service providers, causing users' legitimate rights to be vulnerable to threats and allowing them to protect themselves with cloud service agreements when disputes occur. Cloud service providers have already explained possible information security risk situations and corresponding responsibility allocation in service agreements, omitting the process of consultation with users. Users must unconditionally accept all provisions in cloud service agreements to use cloud services; otherwise, they cannot use the corresponding cloud services. This leads many users to 被迫放弃其他应有权利 in order to obtain cloud service usage rights, thereby increasing their own information security risks and responsibilities.

6 Library Countermeasures for Cloud Service Agreement Information Security Risks

Cloud service agreements are contracts for effective communication and problem resolution between libraries and cloud providers. Although different cloud service providers offer different cloud service agreement content, when signing such cloud service agreements, libraries should not only emphasize essential content modules but also have clear considerations regarding specific content positions. Based on the above analysis, the author believes that libraries should take the following measures to address information security risks caused by cloud service agreements when applying cloud service provider products:

6.1 Clarify Ownership of Library User Data

Libraries should ensure they retain ownership of all information resources. Library information resources include traditional information resources, personal data, and virtualized computing resources. In terms of manifestation, library information resources mainly include all text, numerical data, database records, media files, demographic information, search history, geographic location information, and metadata, or other data and information, including data directly provided by libraries as cloud computing service users to cloud service providers, or other library information resources that cloud service providers directly or indirectly access due to providing library cloud services. If data usage behaviors unfavorable to cloud services occur, cloud service providers must inform libraries in a timely and appropriate manner. Prerequisites for public data ac-

cess include: formal data authorization letters from data owners authorizing release, prior notification to data owners, or official court orders for data disclosure that have jurisdiction over the data. In all cases, owners of criminal justice information must be notified in real time of any attempted or completed illegal access to their data.

6.2 Emphasize Integrity of Information Resources

Libraries need to ensure the integrity of information resources, requiring cloud service providers to maintain both physical and logical integrity of library information resources, which can be achieved through physical or logical separation between cloud storage and services. Library information resources should not be stored, shared, processed, or modified in any way that damages data integrity. If cloud service systems are designed to store personal data served by libraries, cloud service providers need to ensure the integrity of user data access logs and allow libraries to establish a 监管链 for information resources with high privacy protection requirements and intellectual property protection demands. When libraries need to extract operation records of library information resources, cloud service providers should also assist libraries in establishing 监管链 or other cloud-related technical demonstrations. When libraries request to select data, cloud service providers should notify libraries whether and when the physical storage location of data has been changed.

6.3 Ensure Confidentiality of Library Information Resources

Cloud service providers should ensure the confidentiality of information resources they store on behalf of libraries. Libraries need to require cloud service providers to adopt all necessary physical, technical, managerial, and procedural measures to protect the confidentiality of library information resources. These measures may include physical security measures, access permission requirements, network security requirements, criminal history background checks for staff and contractors who can access systems or data, security awareness training, encryption, regular audits, and geographic location restrictions. Cloud service providers should provide corresponding credentials proving they have the technical and business capabilities to independently evaluate the network security of systems and services provided to libraries. Cloud service providers should provide timely and appropriate documentation to prove they currently possess network security risk early warning measures. Additionally, cloud service agreements should indicate that cloud service providers agree to continuously maintain the various risk prevention measures described above during cooperation with libraries.

6.4 Ensure Availability, Reliability, and High Performance of Library Information Resources

After obtaining cloud services through cloud service providers, libraries need to ensure the availability, reliability, and high performance of information re-

sources. Libraries should require cloud service providers to provide cloud services according to performance indicators agreed upon in cloud service agreements and to provide corresponding levels of cloud services based on the importance of involved businesses. For some services (such as retrieving archived data or email), lower levels of availability and performance may be acceptable. However, for more critical services such as Computer-Aided Dispatch, higher levels of availability and performance are required.

In addition, librarians responsible for signing cloud service agreements need to carefully read the agreements to promptly identify issues detrimental to maintaining library information security. Typically, when registering for cloud services, individual users do not carefully read cloud service agreements. Even if they read them, they do not do so very seriously, mostly just browsing roughly. This situation occurs partly because users themselves do not attach enough importance to cloud service agreements and do not recognize the potential information security risks. It is also related to the deliberate guidance of cloud service providers. Generally, cloud service agreements mainly have two types: click-wrap and browse-wrap. Click-wrap refers to the service agreement form where users must click "I agree" to complete registration; browse-wrap refers to the service agreement form where users need to actively read the service agreement and click to enter the corresponding interface for browsing. Click-wrap agreements have better noticeability, meaning they can remind users to read service agreements to a certain extent. Browse-wrap services have poorer noticeability, directly defaulting that users have read the service agreement and have no objections unless users actively search for it. Moreover, browse-wrap services usually place buttons linking to service agreement content pages in the least conspicuous positions on websites, more easily causing users to neglect service agreements. Of course, both types of agreements are standard agreements. For libraries applying small-scale cloud services, they can consider directly accepting such standard agreements. However, once the signed cloud service agreements involve larger business scopes, cover more library information resources, or involve more sensitive personal data, libraries should not directly accept such standard agreements. Instead, they should confirm each clause through negotiation before signing cloud service agreements. For such cloud service agreements, from drafting and modification to finalization, librarians responsible for signing agreements should strictly check agreement quality.

References

[1] China Academy of Information and Communications Technology. CAICT Releases 2018 Cloud Computing Development White Paper - Industry Cloud Era Fully Opens [EB/OL]. [2019-08-26]. http://www.caict.ac.cn/kxyj/qwfb/bps/201808/t20180813_{181718}.

[2] Dai Tianfeng. Construction of Data Information Security System Based on Computer Cloud Services [J]. Digital Technology and Application, 2017(11): 188-190.

[3] Bi Jianhuan. Research on Construction of Government Data Information Security System Based on Computer Cloud Services [J]. Digital Technology and Application, 2016(2): 203.

[4] Chen Jie. Research on Construction of Government Data Information Security System Based on Computer Cloud Services [J]. Shandong Industrial Technology, 2016(3): 116-117.

[5] Liu Qin. Research on Construction of Government Data Information Security System Based on Computer Cloud Services [J]. China Management Informationization, 2018, 21(12): 138-139.

[6] Ji Feng. Discussion on Architecture and Information Security of Digital Library Cloud Service Platform [J]. Inner Mongolia Science Technology & Economy, 2018(20): 49-51.

[7] Liu Ping, Liu Chun. Research on Library Construction and Information Security Strategy Based on Cloud Services [J]. Lantai World, 2015(8): 126-127.

[8] Huang Guobin, Zheng Lin. Analysis of Cloud Service Provider Information Security Responsibility Based on Service Agreements [J]. Library, 2015(7): 61-65.

[9] PARK S T, PARK E M, SEO J H, et al. Factors affecting the continuous use of cloud service: focused on security risks [J]. Cluster computing, 2016, 19(1): 485-495.

[10] MADRIA S K. Security and risk assessment in the cloud [J]. Computer, 2016, 49(9): 110-113.

[11] KANG A N, BAROLLI L, PARK J H, et al. A strengthening plan for enterprise information security based on cloud computing [J]. Cluster computing, 2014, 17(3): 703-710.

[12] HALABI T, BELLAICHE M. Towards quantification and evaluation of security of cloud service providers [J] Journal of information security and applications, 2017, 33: 55-65.

[13] VASANTHAR N. Cloud computing for college library automation [EB/OL]. [2019-12-14]. https://www.slideshare.net/Vasan-thrz/cloud-computing-for-college-library-automation.

[14] JUTA S. Digitizing and cataloging the Boekentoren [EB/OL]. [2019-12-15]. https://blog.ml16.eu/digitizing-and-cataloging-the-boekentoren-book-tower-ffc0070793ac.

[15] ZAINAB A, CHONG C, CHAW L. Moving a repository of scholarly content to a cloud [J] Library HiTech, 2013, 31(2): 201-.

[16] AMAZON. New York Public Library's cloud journey [EB/OL]. [2019-12-16]. https://amazonAmazon-china.com/cn/blogs/enterprise-strategy/new-york-public-librarys-cloud-journey/.

[17] OSU.EDU. Ohio State Amazon now includes enterprise support [EB/OL]. [2019-12-16]. https://it.osu.edu/news/2019/03/04/ohio-state-Amazon-now-includes-enterprise-support.

[18] Today in APIs: Amazon Announces EC2 Spotathon [EB/OL]. [2019-12-16]. https://www.programmableweb.com/news/today-apis-Amazon-announces-ec2-spotathon-nasdaq-music-to-your-ears-and-11-new-apis/2012/11/09.

[19] Microsoft Azure [EB/OL]. [2019-12-17]. http://www.microsoft.com/windowsazure/.

[20] DuraSpace. DuraCloud [EB/OL]. [2019-12-17]. https://duraspace.org/duracloud/.

[21] Library technology guides [EB/OL]. [2019-12-18]. http://librarytechnology.org/.

[22] Google cloud platform agreement [EB/OL]. [2019-12-18]. https://cloud.google.com/terms/#google-cloud-platform-agreement.

[23] Amazon customer agreement [EB/OL]. [2019-12-18]. https://www.amazon.com/gp/help/customer/display

[24] Microsoft Azure legal information [EB/OL]. [2019-12-18]. https://azure.microsoft.com/en-au/support/legal/.

[25] License. DuraCloud [EB/OL]. [2019-12-18]. https://duraspace.org/duracloud/license/.

[26] OCLC. WorldShare platform terms and conditions [EB/OL]. [2019-12-18]. https://www.oclc.org/content/dam/developernetwork/PDFs/platform_{{{general}}}_{{TCs}}}0%20(1).pdf.

[27] Terms of Use. ExLibris Knowledge Center [EB/OL]. [2019-12-18]. https://knowledge.exlibrisgroup.com/TERMS_{{{OF}}}_{{USE}}}.

[28] Apollo integrated library system subscription purchase agreement. Biblionix [EB/OL]. [2019-12-18]. https://seguin.biblionix.com/agreements/subscription/?agreed=2019-02-15%202015%3A45%3A27.

[29] Terms of Use. Innovative [EB/OL]. [2019-12-18]. https://www.iii.com/terms-of-use/.

Author Contributions:
Huang Guobin: Topic selection, paper writing, revision, and guidance;
Zheng Xia: Material collection and organization, paper writing and revision;
Wang Ting: Partial material collection, initial draft writing.

Information Security Risks Caused by Cloud Service Agreement and Suggestions for Library and Information Community

Huang Guobin[1], Zheng Xia[1], Wang Ting[2]
[1]School of Government, Beijing Normal University, Beijing 100875
[2]Capital Medical University Library, Beijing 100069

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