Research on Current Situation and Countermeasures of Data Privacy Protection Under Cloud Computing

Hong Guo
Hunan City University, Yiyang, China

Abstract: cloud computing brings frequent cross-border transmission of personal data, which poses unprecedented challenges to the jurisdiction of traditional privacy protection laws. The traditional privacy legal jurisdiction mainly follow the "human", "local" and "location of equipment" principle, and cloud computing to "human", "local" and "location of equipment" principle use has brought confusion, can not solve the "two transfer" problem well. The design should be based on the characteristics of cloud computing a new privacy protection legal jurisdiction theory, the "human" principle, to limit the storage location for the limit to third parties to take encrypted personal data protection in cloud computing.

Keywords: Cloud computing; Data privacy; Protection

1. Introduction

Cloud computing is a new business model in network economy era due to the application of new technology, its appearance has brought the unprecedented challenge to national privacy protection laws [1-6], because in the past there has never been such repeated across borders whenever and wherever possible business models. However, the adaptation of law is not the error of cloud computing, and the law as superstructure should change with the development of economy and technology. Therefore, neither the improvement of privacy protection law nor the reconstruction should be the obstacle to the development of cloud computing, and the balance between the development of business model and the protection of personal data must be balanced [7-15].

2. Perplexity and Countermeasures of Judgment of the Place Involved in

Cloud computing is born without geographical restrictions, service providers, users, data entities and servers may belong to different countries, and the jurisdiction of privacy protection laws is usually limited to national boundaries. Therefore, the application of legal jurisdiction has caused a lot of confusion. In one scenario, an Australian citizen uploads personal data to the cloud of a cloud service provider in the United states. Which country law should have jurisdiction over personal data stored in the cloud? There may be several options: (1) Australian law, because the data body is Australian citizens; (2) The laws of the United States, because the cloud service provider is an American enterprise; (3) upload or access to personal data locations, perhaps the Australian citizen was traveling in Europe to visit his mailbox; (4) the data center of the data storage location; (5) according to the nature of the data subject to the complaint, if tort the case, apply the law of tort.

If the law restricts the cross-border flow of personal data, it will greatly reduce the vitality and efficiency of cloud computing, which is no different from the traditional physical equipment processing and storage. Moreover, the principle of territorial jurisdiction is unable to solve the new problems mentioned above, such as the "two transfers", "equipment location", "overseas jurisdiction" and so on.

On the contrary, after the evolution of the principle of personal jurisdiction according to the data subject to determine the nationality of legal jurisdiction, but also seize the pulse of cloud computing. Like the proposal made by the chief legal officer of the Microsoft, the data of the laws governing the citizens and residents of each country, if it relates to the data of the residents of other countries, needs to consult with the government to establish a bilateral legal assistance mechanism. The principle of personal jurisdiction under the EU to EU residents of personal data has jurisdiction, if foreign cloud service providers or registered in the local business cloud service providers against the EU residents personal data (data leakage, data subject without consent to the disclosure to third parties and so on), the data can be exercised subject to territorial jurisdiction. National data protection authorities (DPA) sued the cloud service provider. DPA the jurisdiction in the cloud services business, taking surveys, fines, and other legal measures shall be ordered to compensate for the ban on it; if the cloud service providers to be executed, then DPA has the right to leave the euro area. Principle of personal jurisdiction can well solve the problem of "two transfer" and "location of equipment". According to this principle, the EU law has jurisdiction over the EU personal data for "two transmission", and does not have jurisdiction over the cloud services that use the EU equipment but do not involve the EU resident data. In addition, the United States government in dealing with similar to Microsoft for a citizen of the United States in the region's mailbox information case, can also follow this principle, if only for United States citizens information, cloud service providers can provide; if you need information related to the EU residents, in consultation with the EU government, legal assistance. In this case, the United States to Microsoft for storage in the EU area electronic mailbox a resident of the United States information is legitimate, but because the object relationship with the citizens of the United States mail is mostly EU residents, if the mail to the U.S. government will leak EU residents personal data. Therefore, the United States has only partial jurisdiction over this case and needs the assistance of the European union.

3. Perplexity and Countermeasure of 3. Contract Jurisdiction

Before the use of cloud services, the data provider generally contracts a service contract with a service provider (a unified contract written by a service provider), in fact, through an agreement to click agreement. The contract is written by the service provider, and usually requires the consumer to agree to the jurisdiction of the court as the law of the country where the service provider is located. Many cloud service users in the use of cloud services before not carefully read the terms of the contract agreed to choose, reason is: first, the terms of the contract is long, the average user has no patience and expertise make it completely clear; second, if you do not agree to the terms of the contract, the user can use cloud services, so many users are forced to accept service provider service contract. The Brussels convention, the Rome regulation I and the American court of justice have recognized the legitimacy of the court's choice clause. If there is no dispute jurisdiction court in the contract, the sixth clause of the Rome regulation I stipulates that the contract is governed by the user's conventional residence law, and the service provider shall abide by the mandatory law of the user's place of residence. According to the provisions of the "Regulations of Rome I", cloud computing privacy cases both may be affected by the service provider under the jurisdiction of the law, and may be affected by the user where the laws of the legal profession in the end make visible network location of a service provider or consumer is located under the jurisdiction of the court is not a clear direction.

4. Conclusion

Many countries out of cloud computing is not easy to control concerns, requiring cloud service providers to keep their residents data on the cloud server Microsoft, the data of the laws governing the citizens and residents of each country, if it relates to the data of the residents of other countries, needs to consult with the government to establish a bilateral legal assistance mechanism. The principle of personal jurisdiction under the EU to EU residents of personal data has jurisdiction, if foreign cloud service providers or registered in the local business cloud service providers against the EU residents personal data.

References

[1] Haiping Huang, Hao Chen, Ruchuan Wang, Qian Mao, Renyuan Cheng.(t, n) Secret Sharing Scheme Based on Cylinder Model in Wireless Sensor Networks. Journal of Networks, Vol 7, No 7 (2012) pp. 1009-1016

[2] Yuedong Xu, John C. S. Lui, Dah-Ming Chiu. On oligopoly spectrum allocation game in cognitive radio networks with capacity constraints. Computer Networks, Volume 54, Issue 6, 29 April 2010, Page(s): 925-943

[3] Antonatos, S., Anagnostakis, K., Markatos, E., 2004. Generating realis- tic workloads for network intrusion detection systems. ACM SIGSOFT Software Engineering Notes 29 (1), 207–215.

[4] Tavallaee,M. and Cybernetics, 2010, Toward credible evaluation of anomaly-based intrusion-detection methods, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,pp516-524

[5] Al-karaki J.N., and Kamal A.E.,"Routing techniques in wireless sensor networks: a survey", IEEE Wireless Communication, vol.11, pp. 6–28, November, 2004.
http://dx.doi.org/10.1109/MWC.2004.1368893

[6] Li C, Ye M, Chen G, and Wu J,"An energy-efficient unequal clustering mechanism for wireless sensor networks",IEEE International conference on Mobile Adhoc and Sensor Systems Conference, pp. 597-604, 2005

[7] Xin Huang, Xiao Ma, Bangdao Chen, Andrew Markham, Qinghua Wang, Andrew William Roscoe. Human Interactive Secure ID Management in Body Sensor Networks. Journal of Networks, Vol. 7, No. 9 (2012), 1400-1406 http://dx.doi.org/10.4304/jnw.7.9.1400-1406

[8] Zhao Liangduan, Zhiyong Yuan, Xiangyun Liao, Weixin Si, Jianhui Zhao.3D Tracking and Positioning of Surgical Instruments in Virtual Surgery Simulation. Journal of Multimedia, Vol. 6, No. 6 (2011), 502-509

[9] C. Bfhm, S. Berchtold, D.A. Keim, "Searching in High-Dimensional Spaces: Index Structures for Improving the Performance of Multimedia Databases", ACM Compute, 33(3), pp. 322-373, 2007

[10] Paxson, V., Sommer, R., Weaver, N., 2008. An architecture for exploiting multi-core processors to parallelize network intrusion prevention. In: Sarnoff Symposium, 2007 IEEE. IEEE, pp. 1–7.

[11] Kasman Suhairi, Ford Lumban Gaol, The Measurement of Optimization Performance of Managed Service Division with ITIL Framework using Statistical Process Control. Journal of Networks, Vol 8, No 3 (2013), 518-529

[12] Guang Yan, Zhu Yue-Fei, Gu Chun-Xiang, Fei Jin-long, He Xin-Zheng, A Framework for Automated Security Proof and its Application to OAEP. Journal of Networks, Vol 8, No 3 (2013), 552-558

[13] Muhammad J. Mirza, Nadeem Anjum.Association of Moving Objects Across Visual Sensor Networks.Journal of Multimedia, Vol 7, No 1 (2012), 2-8

[14] Muhammad J. Mirza, Nadeem Anjum.Association of Moving Objects across Visual Sensor Networks. Journal of Multimedia, Vol 7, No 1 (2012), 2-8

[15] Zhao Liangduan, Zhiyong Yuan, Xiangyun Liao, Weixin Si, Jianhui Zhao.3D Tracking and Positioning of Surgical Instruments in Virtual Surgery Simulation. Journal of Multimedia, Vol 6, No 6 (2011), 502-509