CLOUD COMPUTING IN E-COMMERCE IN PALESTINE: LEGAL ISSUES AND CHALLENGES

Yahya Y. F. Hasan
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
Email: d.yahya_y@hotmail.com

Sonny Zulhuda
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
Email: sonny@iium.edu.my

ABSTRACT

Today's infrastructure of e-commerce increasingly depends on cloud computing. Companies use cloud computing in e-commerce, because it prevents data loss and provides a complete network with hardware and software, which further enables the merchant to manage their e-transaction in the best possible manner. On the other hand, cloud computing provider is obliged to provide the merchant with the best solution based on their respective agreements. In addition, providing adequate levels of security while using the cloud computing service is equally important because any breach of security will affect the reputation of the merchant and provider, and affect the users via loss or leakage of their data. Although the benefits of cloud computing to the merchants and consumers in e-transaction are clear, there are undoubtedly some challenges and concerns. This paper will discuss these challenges of using cloud computing within e-commerce including the liability surrounding the data security and privacy in the cloud. In addition, this paper seeks to clarify the provider's liability for loss or destruction of the information during cloud computing. Furthermore, this study aims to examine the legality of unfair contract terms in the cloud computing contracts under the Palestinian laws. This study mainly used the analytical and library research to examine the main issues of cloud computing. The laws of Palestine and the Directive 95/46/EC are used in this study to clarify the legal positions on the relevant issues above. It is found from this study that the current laws in Palestine are inadequate to regulate the cloud computing issues. The outlying contract should include a high level of security to the customer to protect their data and information in cases of cloud computing. The cloud provider should provide the appropriate technical means and the procedures to protect personal data against any accident of loss, unauthorized disclosure, and access or transfer of the data via the Internet. The benefit of this paper is to propose some recommendations to develop the Palestinian laws in order to address the issues of cloud computing which will contribute in the development of e-commerce in Palestine.

Key words: Electronic Commerce, Cloud Computing, Liability, Security, Privacy

Introduction

Cloud computing (Cloud service providers) service refers to the development and implementation of models that allow users access to different resources of computing (e.g. networks, servers, storage, applications, and services). This includes the network access techniques that the service provider provides to cloud users.[1] Computing resources in cloud computing are used for different purposes through short periods of time. The process of requesting and receiving resources are completed automatically within a few minutes. Cloud computing contains hardware, software, networks, storage, services, and provides share resources, software, and information to the computers. People do not need to buy and build an IT infrastructure or understand the basics of technology, as all of the operations are done on cloud computers.[2]

A cloud service provider plays an essential role in e-transactions as they provide hardware and software services relating to computing resources. In general, there are many legal issues which may arise from using cloud computing in e-commerce such as the standards provided by cloud computing services, regulatory issues and unfair contract terms. In addition, security is the main concern that faces the users when they use cloud computing services. Therefore, the researcher will discuss all these important issues and the liability of a cloud service provider if he fails in fulfilling his obligations in e-transactions.

Cloud Computing In E-Commerc

[1] Mendhe, T., Kamble, P.A., Thakre, A. K. (2012). Survey on Security, Storage, and Networking of Cloud Computing. *International Journal on Computer Science and Engineering (IJCSE)*, ISSN: 0975-3397, Vol. 4 No. 11, 1780–1785.
[2] Gampala, V., Inuganti, S., Muppidi, S. (2012). Data Security in Cloud Computing with Elliptic Curve Cryptography. *International Journal on Computer Science and Engineering (IJCSE)*, ISSN: 2231-2307, Vol.2, Issue.3.

The businesses in e-commerce rely on hardware and software as their technical architecture, which enables them to determine the best techniques and strategies vis-à-vis e-marketing. Therefore, cloud computing service is an increasingly essential element in building, implementing, and maintaining the technical architecture of e-commerce today.[3]

Cloud computing is essential for e-commerce because it provides a high level of data reduction in an efficient, professional, and safe manner. Furthermore, cloud computing is an increasingly popular option in reducing the loss of data due to safety problems.[4] For the merchants, cloud computing enables them to manage and operate data processing in an effective and flexible manner.[5] Cloud computing is user friendly because the users do not necessarily need to install the software on their system; they just need an Internet connection and a web browser.[6] In short, the infrastructure of e-commerce understandably now depends on cloud computing both on services of the computing software and hardware.

The role of cloud computing in e-commerce indicates its liability, especially because e-commerce depends on software and hardware. Therefore, the cloud provider should be potentially liable if there is any failure in e-transaction due to software and hardware. Hence, cloud computing provider is obliged to provide the merchant with the best software and hardware based on their respective agreements. As a result of this, the provider of cloud computing would be potentially liable under the provision of contractual liability if they do not provide the merchant with the software and hardware that were previously agreed upon. Furthermore, the cloud provider would be liable according to the contractual liability if there were any failure in e-transaction due to failure in software and hardware. On the other hand, the cloud provider would be liable to the end user in e-commerce if there is any harm that befall them due to defects in software and hardware, or if there are any infringement in data security.

In 2011, the percentage of Palestinians aged ten years and above who used the Internet for e-commerce was 3.4% of the whole populations, compared to 11.2% of the firms which implemented e-transactions in the same year. In addition, the percentage of the firms which had a website was 4.8% of the whole firms in the Palestinian Territory in 2011.[7]

In fact, the Palestinian Information Technology Association (PITA)[8] provides many types of products and services such as software development (29%), sale of hardware (28%), internet provision and website design and hosting (11%), training and consulting (10%),services of telecommunications (7%), integration of system and outsourcing(5%), the services of marketing and declaration (5%), industrialization (3%), and electronic equipment design and manufacturing (2%).[9]

On the other hand, the output of communication and information services in Palestine was $588.9m in 2010.[10] In addition, the ICT revenue (percentage of GDP) of this sector was 0.8% in 2008, compared to 3.5% in Egypt and 1.4 in Lebanon.[11]

However, the percentage of spending on the public and private clouds was 15% of the worldwide IT spending in 2011; growing at four to five times the rate of the overall IT market. In 2014, this study expected that 80% of new software offerings will be available as cloud services with over one-third of software purchases will be via cloud. In addition, this study, expected that cloud and traditional service providers will account for 12% of IT infrastructure spending, growing to 20% in 2014.[12]

These statistics reflect the importance of cloud computing around the world, and that the individuals are interested in spending a sum of their money on IT sectors. In addition, the companies are competitive in offering new types of software to the customers. On the other hand, using the Internet in Palestine has increased in the last few years; this encourages the legislator to regulate

[3] Wang, D. (2013). Influences of Cloud Computing on E-Commerce Businesses and Industry. *Journal of Software Engineering and Applications*, Vol. 6 No. 6, pp. 313-318. Accessed on: 6/9/2014.
[4] Sun, Ch. (2012). *Research of E-Commerce Based on Cloud Computing*. Advances in CSIE, Vol. 2, AISC 169, pp. 15–20.
[5] Liu, T. (2011). E-commerce Application Model Based on Cloud Computing. *International Conference of Information Technology, Computer Engineering and Management Sciences (ICM)*. Papers presented at Nanjing, Jiangsu, 24-25 Sept (pp, 147 – 150).
[6] Hashemi, S.M., Bakhtiari, S. (February 2013). Cloud Computing and its Effects on Electronic Commerce: A Survey. *ARPN Journal of Systems and Software*. Vol. 3, NO. 2,. Pp. 25-30.
[7] Palestinian Central Bureau of Statistics. (2011). *Results on ICT Business Survey 2011: About Half of economic establishments Use Computers*. http://www.pcbs.gov.ps/portals/_pcbs/PressRelease/Press_En_ICTBS2011E.pdf. Accessed on: 23/11/2015.
[8] The Palestinian Information Technology Association (PITA) is a non-profit organization that is created by the business men in 1999, and it attends the interests of the Palestine's Information and Communication Technology (ICT) sector. PITA contains more than 160 Palestinian ICT companies. http://www.pita.ps. Accessed on: 23/11/2015.
[9] Wihaidi, Rami. (2009). The Palestinian ICT Sector: A Three-Year Outlook. Based on Economic Indicators. The Palestine Information and Communications of Companies (PITA). http://www.lacs.ps/documentsShow.aspx?ATT_ID=2181. Accessed on: 30/6/2015. At: 10
[10] Palestinian Central Bureau of Statistics. (2012). National Accounts at Current and Constant Prices (2009, 2010). http://www.pcbs.gov.ps/Portals/_PCBS/Downloads/book1838.pdf.Accessed on: 23/11/2015. At: 46.
[11] United Nations Economic and Social Commission for Western Asia. (2009). Regional Profile of the Information Society in Western Asia. http://isper.escwa.un.org/Portals/0/Regional%20Profiles/Regional%20Profile%202009-E.pdf. Accessed on: 23/11/2015. At:141
[12] Gens, F. IDC (International Data Corporation) Predictions 2011: Welcome to the New Mainstream. http://www.ris.org/uploadi/editor/1295368911IDCPredictions2011_WelcometotheNewMainstream.pdf. Accessed on: 23/11/2015. At: 3

new laws organizing this issue; including cloud computing to protect the individuals during the purchase of their goods and services through the Internet.

In general, Palestinian firms have not fully utilised the cloud computing technology with all its features because they face many hindrances in adopting the cloud computing technology such as inadequate financial resources, lack of experts in the issues of cloud computing, insufficiency in network bandwidth, legal and regulatory issues and data sensitivity.[13] Nevertheless, these issues need solution to encourage the adoption of cloud computing in Palestine. In view to support the use of Clouds in Palestine, the researcher recommends that Palestinian legislator creates new laws that motivates the use and addresses the issues of cloud computing as well as clarifies the liability of the Cloud Service Provider regarding any failure or problem in the system which may result in damage to the users or institutions that adopted the cloud computing system. In addition, the Cloud Computing Provider is obliged to take all the procedures to protect the security of the users and their data against unauthorized access and security threats. Finally, there is a need for cooperation between the Palestinian government and the cloud computing firms to organize training courses in the issues of cloud computing to attain professional experience in such issues.

Standards Provided By Cloud Computing Services

The cloud-based e-service model is still dissimilar in its implementation. In other words, the cloud computing services are specific to each cloud provider such as Amazon's S3 and IBM's Blue Cloud. In addition, the cloud providers try to keep their users by providing the services in a way that makes it hard to move to another cloud provider. Given this potential difficulties, it is arguably important to develop and implement a unified industrial standard if we want to develop our system and implement new models into it.[14] Creating such a standard would help principally in service quality, format of data, providing of resources, and the issues of privacy and security.[15]

Creating standard services of the cloud is important to protect the privacy and security of the users such as protecting the data against unauthorized access which potentially comes from ubiquitous sources globally. It is necessary to find the best method to introduce cloud computing services. Furthermore, there is a need to find a manner that obligates the cloud computing providers to fulfil these standard services. As an example, the ISO (the International Organization for Standardization) and IEC (the International Electro-technical Commission) form a specialized system for worldwide standardization; it introduced the ISO/IEC 27018:2014 – Information technology-Security techniques-Code of practice for the protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.[16]

The purpose of the above standard is to ensure that the Cloud Service Provider offers the appropriate controls of information security which maintain the privacy of their customers by securing Personally Identifiable Information (PII).[17] This standard contains various provisions that protect the customer in the case of concluding a contract with the Cloud Service Providers. For example, the Cloud Service Provider is obliged to take permission from the customer if he wants to use the Personally Identifiable Information (PII) for advertisements.[18] This requirement is important to protect the privacy of the users as the cloud provider is obliged to use their information for the specific purpose of the cloud only; he is forbidden from using this information for other purposes. It is an increasing trend that individuals do not like to publish their personal information in an advertisement. In addition, there are many advertisers which bother the customers when the commercial companies had obtained the customers' email addresses; they try to send several messages to them every time, causing a nuisance. In addition, the standards provide that the cloud provider should have the procedures to transfer, delete, or return the data in the case contract termination of the cloud services.[19]

Normally, the cloud services contract contains the provisions of contract termination such as the reason of termination and the period of the cloud computing contract. Therefore, the cloud computing provider is obliged to protect the privacy of the users after terminating the contract, and he is obliged to maintain the users' privacy and information from any unauthorized person, delete them or return them to the users after the cloud contract is terminated. Furthermore, the cloud provider is obliged to apply

[13] Almabhouh, AlaaEddin. (January 2015). Opportunities of Adopting Cloud Computing in Palestinian Industries. *International Journal of Computer and Information Technology* (ISSN: 2279 – 0764). Volume 04 – Issue 01.Pp, 103-109.
[14] Hashemi, S.M., Bakhtiari, S. At: 5
[15] Rashmi., Sahoo, G., Mehfuz, S. (August 2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, Vol. 3, No.4. Pp, 1-11.
[16] International Standard. ISO/IEC 27018. Information technology- Security techniques- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. First edition: 2014-08-01. https://webstore.iec.ch/preview/info_isoiec27018%7Bed1.0%7Den.pdf. Accessed on: 21/7/2015
[17] ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. http://www.iso27001security.com/html/27018.html. Accessed on: 25/11/2015.
[18] Information Integrity Solutions. ISO/IEC 27018 Prime. http://www.iispartners.com/downloads/IIS%20Primer%20on%20ISO%2027018.pdf. Acceded on: 24/7/2015. See also, Beckham, J.A., Hawa. K,. Ramson, A. F., and Sutin, A.N. (November 2014). ISO 27018 - Data Protection Standards for the Cloud. Greenberg Traurig, LLP. http://www.martindale.com/business-law/article_Greenberg-Traurig-LLP_2184114.htm. Accessed on: 24/7/2015.
[19] McCann FitzGerald. (October 2014). *ISO/IEC 27018* – the New Cloud Security Standard. Pp, 1-3. http://www.mccannfitzgerald.ie/McfgFiles/knowledge/5809-ISOIEC%2027018%20%E2%80%93%20the%20New%20Cloud%20Security%20Standard_0.pdf. Accessed on: 21/7/2015.

the procedures in case of data breach such as clarifying the damage if there is any data loss or disclosure, informing the users about the breach, and maintaining the records of this incident.[20]

Breach to users' information security during the use of the cloud services is another worrying issue for both the providers and the consumers. In fact, protecting the privacy of users is an obligation on the cloud service provider; it also upholds the reputation of the Cloud Service Provider. The users look for the Cloud Service Provider who preserves their data privacy at most. Therefore, the Cloud Service Provider must take all that necessary to prevent malicious or accidental breach into their system and to protect the personal information of the users.

In relation to this, the Cloud Service Provider bears some duty to keep their customers updated about their data management procedures and to inform them about the third parties who process their data and who can access their information.[21] This is because in practice many cloud computing companies outsource their work to third parties and allow these parties to access the users' data. Therefore, the Cloud Service Provider is obliged to inform the users about this arrangement and the arising legal relations with the third party. This information is subsequently important to grant the users the right to accept or reject this third party to maintain their personal data from disclosure by an unauthorized party. In other words, this requirement grants more protection to the data of users from disclosure by unauthorized parties.

In light of the above, it is desirable that the companies of Information Technology in Palestine adopt these standards to guarantee more protection to the Palestinian users. Conversely, this can be adopted by the legislators to be accommodated in the local laws or by-laws that regulate ICT in the commercial activities in Palestine. Besides, business associations and consumers group alike may contribute by helping to determine the best practice and specialized cloud computing standards for the Palestinian computing industry, and that includes adopting the international ISO standards in Palestine. This would necessarily lead to a better protection of the information security and privacy of the users vis-à-vis the cloud computing services in Palestine. Needless to say, they should make it open for any new and additional standards to be applied in so long as they are suitable for the Palestinian cloud computing companies and users.

Need for regulatory framework on Cloud Services

Cloud service providers provide many services in cloud computing environment, such as information processing, data storage, security, maintenance, and other works. Therefore, regulating and controlling cloud computing services is important to protect the security of users, especially if the provider plays a role in dealing with the user's information.[22]

Regulating the duties and tasks of the cloud provider on data storage is a crucial matter, because the storage contains many types of the users' personal information. The Cloud Service Provider is obliged to protect the users' data during its processing and storage, and prevent any access of this data by any unauthorized person. In addition, there is a need for regulating the duties of the Cloud Service Provider in the issue of using the users' data. The providers can use the data for the cloud purpose, and forbid using the data for other purposes such as selling them to commercial companies for advertisement purposes.

On the other hand, the laws that organize cloud computing activities in e-commerce in Palestine are insufficient. Therefore, problems will arise when we want to apply the law to organize the activities of cloud computing.[23] In short, legislating new laws that organizes the work of cloud computing in e-commerce activities is important, especially for Palestine. This is crucial to ensure clarity on the liability of cloud computing in e-commerce activities and especially in protecting the data of users during e-transaction. In line with that, laws that clarify the liability of cloud computing in cases of failure in its services or equipment are equally important.

Unfair Contract Terms

The majority of cloud computing provider uses complex contracts containing unfair terms. They use the standard contracts in realizing the interest of the cloud provider against the users and consumers in e-commerce. In addition, many cloud computing contracts are non-negotiable, and they contain disclaimers on the liability for data integrity, confidentiality, or service continuity.[24]

This unfair term has been a long-standing issue in many types of contracts. Indeed, it is equally controversial when it comes to cloud service contracts. Generally, there are many unfair terms in these contracts that exclude the liability of merchants in case of damage or failure in submitting the same agreement services, allowing unilateral changes of the contract terms and the terms of

[20] ACT | The App Association. White Paper on Cloud Privacy Standard ISO 27018. Pp, 1-4. http://actonline.org/wp-content/uploads/2015/02/ISO.pdf. Accessed on: 24/7/2015.
[21] Ibid.
[22] Saleh, A. A. (2012). A Proposed Framework based on Cloud Computing for Enhancing E-Commerce Applications. *International Journal of Computer Applications* (0975 – 8887) Volume 59– No.5. Pp, 21-25.
[23] Liu, T.
[24] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.9.2012 COM (2012) 529 final. http://www.beuc.org/publications/2013-00143-01-e.pdf. Accessed on: 4/9/2014. At: 11

arbitration. Furthermore, the contracts between the merchants and consumer contain unfair terms that do not protect the right of consumers, such as the authority in processing unnecessary data for services.[25]

One wonders what Palestinian law has to say on this issue. It is worthy to note a provision from the article 150 of the Palestinian Civil Draft Law No. 4/2012, which provides that: "If the contract is concluded by way of adhesion, and contains unfair terms, the court can modify these terms or exempts the compliance party from it in accordance with fairness and justice. Any agreement provides otherwise is void."[26] The law gives the court the authority to modify the adhesion contract to protect the weaker party. The court can modify or cancel unfair terms from the contract, and the parties cannot agree to cancel the right of the court because the authority of the court in this issue is derived from public order. In addition, the Palestinian Consumer Protection Law, No. 21/2005 provides: "The council can review the reasonableness and justice of the terms in consumption contracts and standard contracts, and recommends to the minister or the party who issues these contracts to remove unfair terms on the rights of consumer, or requires to reconsideration in these terms. The Council of Ministers releases the system that defines the standards for estimating the terms that can be considered unfair in consumption contracts."[27] This law gives the council of consumer protection the power to review the contract and to oversee the terms inside, and the council can compel the removal of unfair terms from these contracts.

Data Security And Privacy Of Cloud Computing

Cloud computing leads to concerns about the security of users in e-commerce, especially the loss the important data of **e-**commerce transaction and the threats of breach of privacy during e-commerce, because cloud platform stores all the IT resources, such as hardware, software, data, and network applications.[28] In general, security remains the main issue of cloud computing vis-à-vis users, especially via the Internet. It is therefore imperative that Internet users be provided a secure platform that will guard their personal data during their cloud computing sessions.

Cloud computing is made up of multiple technologies, such as networks, databases, operating systems, virtualization, scheduling of resource, management of transaction, load balancing, and memory management, which makes it open to security issues, such as the security of the network systems, security of data, security of memory management, and the security of sources allocation.[29] **Businesses are concerned about the security and safety of its data during cloud services. Any breach of security in cloud computing leads to financial losses for businesses and affect its reputation and customers' confidence. Service provider organizes cloud computing, and any breach of security will affect its future business.**[30] Therefore, providing high levels of security during cloud computing is important because any breach of security in clouding will affect the reputation of the merchant and provider, and effect the users via loss or breakage of their data.

Cloud computing solved many traditional security requirements, such as authority, information integrity, non-repudiation, and problems relevant to authentication, but there are many security problems that still exist, such as data confidentiality and network security.[31] The provider should provide the appropriate technical means and the procedures to protect personal data against any accident of loss, unauthorized disclosure, and access or transfer of the data via the Internet. Therefore, the provider would be liable for loss or destruction of the information during cloud computing if they did not address the technical issues and measures to protect the user's data.

In this respect, not much we can trace from the Palestinian law. Attention is then made to look at the European Union's Opinion 05/2012 on Cloud Computing[32] examines the relationship between the cloud service provider and the cloud client on the basis of EU Data Protection Directive (95/46/EC). Firstly, the cloud client determines the ultimate purpose of the processing, and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organization. The cloud client therefore acts as a data controller.[33] The Directive defines a controller as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of

[25] The European Consumer Organisation. EU Cloud Computing Strategy. BEUC Position Paper. Ref.: X/2013/014 - 28/02/2013. http://www.beuc.org/publications/2013-00143-01-e.pdf. Accessed on: 4/9/2014. At: 7
[26] This article is in parimateria with article 204 of the Jordanian Civil Law. Number: 43 of 1976
[27] The Palestinian Consumer Protection Law, number 21/2005. Article: 23
[28] Wang, D. At: 3
[29] Sen, J. Security and Privacy Issues in Cloud Computing. http://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf. Accessed on: 28/4/2014. At: 7
[30] Vincent, M., Hart, N., Morton, K. Cloud Computing Contracts, White Paper, A Survey of Terms and Conditions. http://www.itnews.com.au/pdf/Cloud-Computing-Contracts-White-Paper.pdf. Accessed on: 28/4/2014. At: 10.
[31] Hashemi, S.M., Bakhtiari, S. At: 4
[32] Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf. Accessed on: 26/8/2014
[33] See Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf . Accessed on: 26/8/2014. At: 12. See Also, Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Accessed on: 28/8/2014. At: 7

personal data."[34] Therefore, the cloud client, as a controller, must accept responsibility for abiding by data protection legislation, and is responsible and subjected to all legal duties that are addressed in Directive 95/46/EC.[35] Next, when the cloud provider supplies the means and the platform and act on behalf of the cloud client, the cloud provider is regarded as a data processor according to Directive 95/46/EC,[36] is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.[37] Moreover, there may be situations where a provider of cloud services may be considered either as a joint controller or as a controller in their own right, depending on concrete circumstances. For instance, this could be the case where the provider processes data for its own purposes."[38]

Therefore, the researcher examines the Directive 95/46/EC of the European Parliament in the issue of security in cloud computing. Article 17(1) of Directive 95/46/EC stipulates: "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[39] The technical security measures should be provided and protect the providers. If the provider works through a processor, they should choose a processor that guards technical measures and security.

Article 17(2) of Directive 95/46/EC provides: "The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures."[40] Furthermore article 17(3) of the Directive provides: "The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, and that the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor."[41]

The Directive 95/46/EC defines the processor in article 2(e), where it defines 'processor' as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.[42] The processor is subjected to instructions of the controller according to the contract that clarifies the obligations of the parties. The parties can prove the obligations or measures on the protection of the security of data by writing another equivalent form according to the article, 17(4) of Directive 95/46/EC: "For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."[43]

The contract obliges the cloud service providers to provide the customers with security. The provider can help customers evaluate the risks and open their security equipment to protect their data during cloud service. The cloud service provider are obliged to provide high levels of security for data in the process of clouding.[44] The parties can include the terms in the contract, where the vendor is obliged to notify the customers in case there were breaches in security.[45] In other word, the contract organizes the obligations of the parties in cases of cloud computing, such as the level of security and the types of information that should be protected. Therefore, the provider would be liable according to the provisions of contractual liability if there were any breaches in the security of information or losses. Therefore, the cloud service provider are obliged to provide security for customers according to the laws and the contract stipulating the obligations of the parties. The contract should include a high level of security to the customer to protect their data and information in cases of cloud computing.

The technologies play an essential role in cloud computing as it depends on multiple technologies. Therefore, the security of these platforms is an essential issue that concerns the users when they provide their personal data. In general, providing a high

[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 2/d.
[35] See Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". At: 12. See Also, Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. At: 8.
[36] Ibid. At: 8
[37] Ibid. At: 8
[38] Ibid. At: 8
[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article, 17/1
[40] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 17/2
[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 17/3
[42] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 2/e
[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 17/4
[44] Vincent, M., Hart, N., Morton, K. At: 10
[45] McDonald, S. Legal and Quasi-Legal Issues in Cloud Computing Contracts. http://net.educause.edu/section_params/conf/ccw10/issues.pdf. Accessed on: 28/4/2014

level of security during cloud computing is an essential obligation to protect the user's data, and maintain the reputation of the cloud service provider. As a rule, the provider should provide the appropriate technical means to protect personal data against any threats. In this case, the Directive 95/46/EC obliges the controller in implementing the appropriate technical measures to protect personal data against any threats; the controller is still liable when he chooses the processor. In brief, a cloud service provider is obliged to provide the customers with a high level of security according to the laws and the contract. Therefore, the provider would be liable if there were any losses or breaches in the security of information.

Liability in the Cloud

Liability in the cloud is a main challenge, especially if there are any loss or destruction of the customer's data. The problem arises when clarifying the liability of the merchant or cloud service provider. Therefore, limiting the liability for security or risks in clouding is an important issue.

An important issue for the cloud providers is their reputation; they provide the customer with services that keep their data from being lost or hacked. There are also other threats to customers of cloud computing, such as server crash or hard drive failures.[46] An example of this is the failure of Microsoft cloud in 2009. Data such as contacts, calendars, and other data of mobile phone users are stored on the cloud of Microsoft. Microsoft sent a message its cloud customers after their cloud facility failed, stating "Regrettably, based on [Microsoft's] latest recovery assessment of their systems, we must now inform you that personal information stored [in our cloud] almost certainly has been lost as a result of a server failure at [Microsoft]."[47]

The person should be able to claim compensation from cloud service provider for any damage that results from unlawful processing operations. Article 23(1) of Directive 95/46/EC provides: "Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."[48] Therefore, the provider would be liable for any damage to the customer from damage in the cloud, or if they can prove that the damage was not a result of their own negligence or wrongdoing. Article 23(2) of Directive 95/46/EC provides: "The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage."[49]

The problem is that there are many contracts containing terms that exclude the liability of the cloud provider from the loss or breach the security of the data. For example, "The Service is provided with no warranties regarding security, reliability, protection from attacks, data integrity, or data availability (including without limitation data integrity or availability related to cloud storage features of the Service)."[50]

In this term, the cloud provider escapes liability in the issue of security breach, and the users bear this liability as weak parties. In fact, the provider creates these terms and obligates the user to agree with the content without having any chance to negotiate or remove these terms. In other words, these terms are unfair as they were created by the providers and protect their interest over the interest of users. Therefore, the researcher recommends creating official and specialized committees to review the cloud contracts, especially the terms of the exclusion clauses. In addition, these committees can organize standard contracts relating to the cloud computing services, particularly the terms of the cloud providers' liability in case of security breach and privacy.

Based on these discussions, it can be concluded that, the cloud service provider would be liable in cases of breach in contract. They would also be liable if they fail to provide the same level of clouding, or in cases of breach in the security of the customers or loss of their data. The service provider is obligated, as per their contract to guard the security of their customers in cloud computing. Unfortunately, Palestinian legislations do not indicate the liability in the case of cloud computing in e-transaction. In other word, Palestine needs new legislations that organizes cloud computing, and protect the consumer's data from any threats, such as loss or damage during cloud computing. Learning from the EU Directives may provide some practical guidance to the Palestinian legislators.

Conclusion

The breach of a contract leads to the liability of the Cloud Service Providers. They would also be liable if they fail to provide the same level of clouding or in cases of breach in the security of the customers or loss of their data. The service provider is obligated, as per their contract to guard the security of their customers in cloud computing. In addition, the contract should include a high level of security to the customer to protect their data and information in cases of cloud computing. The cloud provider should provide the appropriate technical means and the procedures to protect personal data against any accident of loss, unauthorized disclosure, and access or transfer of the data via the Internet. Therefore, the provider would be liable for loss or destruction of the information during cloud computing if they did not address the technical issues and measures to protect the

[46] Calloway, T. J. Cloud Computing, Click wrap Agreements, and Limitation on Liability Clauses: A Perfect Storm. *Duke Law & Technology Review*. Vol. 11 No. 1, 164-174.
[47] Ibid.
[48] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 23/1
[49] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article: 23/2
[50] Vincent, M., Hart, N., Morton, K. At: 10

user's data. On the other hand, the cloud provider would be liable to the end user in e-commerce if there any harm that befall them due to defects in software and hardware, or if there are any infringement in data security.

At this juncture, it is very obvious that the working mechanism of cloud computing service in electronic commerce activities has not been adequately regulated. Many legal aspects of the service are far from clear. In Palestine this is more obvious because of lack of legal and regulatory infrastructure. This paper therefore exposes those potential problems and challenges posed by the cloud computing services and how the law should respond. Learning form international instruments including EU Directive and the ISO standards would certainly be helpful.

References

ACT | The App Association. White Paper on Cloud Privacy Standard ISO 27018. Pp, 1-4. http://actonline.org/wp-content/uploads/2015/02/ISO.pdf. Accessed on: 24/7/2015.

Almabhouh, Alaa Eddin. (January 2015). Opportunities of Adopting Cloud Computing in Palestinian Industries. *International Journal of Computer and Information Technology* (ISSN: 2279 – 0764). Volume 04 – Issue 01.Pp, 103-109.

Beckham, J.A., Hawa. K,. Ramson, A. F., and Sutin, A.N.(November 2014). ISO 27018 - Data Protection Standards for the Cloud. Greenberg Traurig, LLP. http://www.martindale.com/business-law/article_Greenberg-Traurig-LLP_2184114.htm. Accessed on: 24/7/2015.

Calloway, T. J. Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm. *Duke Law & Technology Review*. Vol. 11 No. 1, 164-174.

Data Protection Working Party. Opinion 05/2012 on Cloud Computing. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Accessed on: 28/8/2014.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.9.2012 COM (2012) 529 final. http://www.beuc.org/publications/2013-00143-01-e.pdf. Accessed on: 4/9/2014.

The European Consumer Organisation. EU Cloud Computing Strategy. BEUC Position Paper. Ref.: X/2013/014 - 28/02/2013. http://www.beuc.org/publications/2013-00143-01-e.pdf. Accessed on: 4/9/2014.

The European Consumer Organisation. EU Cloud Computing Strategy. BEUC Position Paper. Ref.: X/2013/014 - 28/02/2013. http://www.beuc.org/publications/2013-00143-01-e.pdf. Accessed on: 4/9/2014.

Gampala, V., Inuganti, S., Muppidi, S. (2012). Data Security in Cloud Computing with Elliptic Curve Cryptography. *International Journal on Computer Science and Engineering (IJCSE)*, ISSN: 2231-2307, Vol.2, Issue.3.

Gens, F. IDC (International Data Corporation) Predictions 2011: Welcome to the New Mainstream. http://www.ris.org/uploadi/editor/1295368911IDCPredictions2011_WelcometotheNewMainstream.pdf. Accessed on: 23/11/2015. At: 3

Hashemi, S.M., Bakhtiari, S. (February 2013). Cloud Computing and its Effects on Electronic Commerce: A Survey. *ARPN Journal of Systems and Software*. Vol. 3, NO. 2,. Pp. 25-30.

Information Integrity Solutions. ISO/IEC 27018 Prime. http://www.iispartners.com/downloads/IIS%20Primer%20on%20ISO%2027018.pdf. Acceded on: 24/7/2015.

International Standard. ISO/IEC 27018. Information technology- Security techniques- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. First edition: 2014-08-01. https://webstore.iec.ch/preview/info_isoiec27018%7Bed1.0%7Den.pdf. Accessed on: 21/7/2015

Liu, T. (2011). E-commerce Application Model Based on Cloud Computing. International Conference of Information Technology, Computer Engineering and Management Sciences (ICM). Papers presented at Nanjing, Jiangsu, 24-25 Sept (pp, 147 – 150).

McCann FitzGerald. (October2014). ISO/IEC 27018 – the New Cloud Security Standard. Pp, 1-3. http://www.mccannfitzgerald.ie/McfgFiles/knowledge/5809-ISOIEC%2027018%20%E2%80%93%20the%20New%20Cloud%20Security%20Standard_0.pdf. Accessed on: 21/7/2015.

McDonald, S. Legal and Quasi-Legal Issues in Cloud Computing Contracts. http://net.educause.edu/section_params/conf/ccw10/issues.pdf. Accessed on: 28/4/2014

Mendhe, T., Kamble, P.A.,Thakre, A. K. (2012). Survey on Security, Storage, and Networking of Cloud Computing. *International Journal on Computer Science and Engineering (IJCSE)*, ISSN: 0975-3397, Vol. 4 No. 11, 1780–1785.

Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf. Accessed on: 26/8/2014.

Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe." https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf. Accessed on: 26/8/2014

The Palestinian Consumer Protection Law. Number 21, of 2005. This law was published in the Official Gazette, number: 63, on 27/4/2006, page: 29.

The Palestinian Information Technology Association (PITA). http://www.pita.ps. Accessed on: 23/11/2015.

Palestinian Central Bureau of Statistics. (2011). Household Survey on Information and Communications Technology, 2011: Main Findings. Ramallah - Palestine. http://www.pcbs.gov.ps/PCBS-Metadata-ar-v4.2/index.php/catalog/70. Accessed on: 31/3/2015. At: 43.

Palestinian Central Bureau of Statistics. (2011). Results on ICT Business Survey 2011: About Half of economic establishments Use Computers. http://www.pcbs.gov.ps/portals/_pcbs/PressRelease/Press_En_ICTBS2011E.pdf. Accessed on: 23/11/2015.

Palestinian Central Bureau of Statistics. (2012). National Accounts at Current and Constant Prices (2009, 2010). http://www.pcbs.gov.ps/Portals/_PCBS/Downloads/book1838.pdf. Accessed on: 23/11/2015. At: 46.

Rashmi., Sahoo, G., Mehfuz, S. (August 2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, Vol. 3, No.4. Pp, 1-11.

Saleh, A. A. (2012). A Proposed Framework based on Cloud Computing for Enhancing E-Commerce Applications. A Proposed Framework based on Cloud Computing for Enhancing E-Commerce Applications. *International Journal of Computer Applications* (0975 – 8887) Volume 59– No.5. Pp, 21-25.

Sen, J. Security and Privacy Issues in Cloud Computing. http://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf. Accessed on: 25/11/2015.

Sun, Ch. (2012). Research of E-Commerce Based on Cloud Computing. *Advances in CSIE*, Vol. 2, AISC 169, pp. 15–20.

Vincent, M., Hart, N., Morton, K. Cloud Computing Contracts, White Paper, A Survey of Terms and Conditions. http://www.itnews.com.au/pdf/Cloud-Computing-Contracts-White-Paper.pdf. Accessed on: 28/4/2014.

Wihaidi, Rami. (2009). The Palestinian ICT Sector: A Three-Year Outlook. Based on Economic Indicators. The Palestine Information and Communications of Companies (PITA). http://www.lacs.ps/documentsShow.aspx?ATT_ID=2181. Accessed on: 30/6/2015. At: 10

Wang, D. (2013). Influences of Cloud Computing on E-Commerce Businesses and Industry. *Journal of Software Engineering and Applications*, Vol. 6. No. 6, 2013, pp. 313-318.

ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. http://www.iso27001security.com/html/27018.html. Accessed on: 25/11/2015