International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2494-9150 Vol-01, Issue 09, Dec 2015.

Fear of Data Privacy and Security in Cloud Computing Technology

Vinayak D. Shinde, Research Scholar, JJTU, Rajasthan, India, vdshinde@gmail.com

Abstract - Cloud computing denotes a shift away from computing as a product that is procured to computing as a service that is delivered to consumers over the Internet from large-scale data centers or "clouds." Any enterprise or organization is concerned about their data. Migration from traditional to cloud computing requires data security and privacy. At present, cloud computing service providers provide assurance about data security, but there are various terms and conditions that are placed by these service providers for cloud computing technology adoption. Multi-located data storage and services (i.e., applications) in cloud make privacy issues even worse. This study discusses thefear of data privacy and security in cloud computing technology. Although all types of sectors began to migrate in cloud computing technology, some cloud storage-related queries require discussion, especially with respect to security and privacy, which will help in reducing data security and privacy issues in cloud computing technology—thereby leading to more users stepping into cloud. We claim that success in cloud computingwill emerge when all security and privacy issues having been resolved.

Keywords—Cloud computing, Data lifecycle, Data privacy, Security and privacy issues, AWS, dropbox.com.

I. INTRODUCTION

Cloud computing denotes processing power, data, and software stored on servers that are accessible through the Internet contrasted with one's own computer. The term "cloud" is derived from the diagram of computer networks that portrayed the Internet as a cloud at the network chain's topmost position because separate computers that made its modules were copious to display separately [1–3]. One of the main cloud computing features is that the end users (customers) do not possess the technology or expertise they use. The required hardware and software are possessed by cloud computing service, whereas the user (customer)only pays suitable charges [2, 3]. Several applications of cloud computing have grown into everyday occurrences for an average Internet user [2, 3].

For users (customers), the activity of cloud computing can produce decline in cost and efficacies [2, 3]. Perhaps, in a cloud computing setup, an end user need not pay large direct principal costs for hardware or hardware's continued maintenance [2, 3]. In addition, if the user requires extra space that is interim, then he/she can request the concerned provider of cloud service to active his/her share for the moment rather than purchasing short-term extra space [2]. In other words, computer resources taken together are usually used more efficiently. Instead of having several equipment running many tasks and then dissipating the left over computing power, cloud computing offers a couple of machines to perform several tasks without dissipating computing cycles [3]. Cloud computing can be visualized as a technique to make computer resource domain flawlessly scalable.

In addition, cloud computing simultaneously creates dependency. Cloud computing service development is structured around a reinterpretation of the connection between end users and technology. The end user must depend on the service provider of cloud computing to confirm that data or information is preserved, safe, and accessible [3]. In addition, he/she must rely on the networks infrastructure that will represent the distribution and recovery paths for data flow up and down the cloud [3]. The other users are from the technology that they depend on, the more reliant the connections may become [3]. Furthermore, once a cloud computing arrangement is adopted by an end user, it may not be easy to return to a platform that is based on personal computing for data services.

The shift to computing resources as a service to be offered by isolated sources with greater access to limitless computing power exhibits not only some attractiveness to computer users with restricted resources and a need for the growth of information services but also some thoughtful issues that must be scrutinized [3].

II. CLOUD COMPUTING CHARACTERISTICS

The U.S. National Institute of Standards and Technology satisfactory captures the need to provide IT services using economies of scale [4, 5].

On-demand self-service: Users can purchase services from the service provider without any human interaction, e.g., a web portal and management interface [4]. Provisioning and de provisioning of services and related resources automatically occur at the service provider.

Ubiquitous network access: Standard mechanisms and protocols are used for accessing cloud services via the network or Internet.

Resource pooling: Resources that offer cloud services are accomplished using a standardized setup that is shared among all users [4].

Rapid elasticity: Resources can be scaled elastically and rapidly [4].

Measured service: Services are continuously measured, which support resource use optimization and reporting the extent of service used by a customer [4].

III. CLOUD COMPUTING SERVICE TYPES

There are three main service types of cloud computing:

1. **Software as a service (SaaS)** is the most conventional and well-known service category of cloud computing [2]. SaaS applications make available software function that would ideally be connected and function on the desktop of the user [2, 3]. With SaaS, on the server of the cloud computing service provider, the application is stored, and it functions through the web browser of the user via the Internet [2, 3]. SaaS examples include Gmail, Google apps, and Salesforce.com.

2. **Platform as a service (PaaS)** helps designers in designing and publishing novel web applications that are placed on the PaaS service provider's server [2, 3, 6]. Customers use the Internet to access this platform and create applications using the PaaS provider's API and gateway software [2, 3]. PaaS examples include Salesforce.com, Google app engine, Mozilla Bespin, and Zoho Creator.

3. **Infrastructure as a service (IaaS) [6]** or "utility computing" aims to avert customer needs to possess their own data centers. The service providers of IaaS provide access to customers to the web storage space and servers [2, 3]. In addition, they own and maintain the hardware, and customers pay suitable charges for space as per their requirements. IaaS examples include Amazon web services (AWS).

IV. WHY NOW?

While cloud computing is intrinsic in the way that the Internet works, as whenever a person accesses a website, that individual is having a remote server retrieve and delivers a document, cloud computing has become more predominant in recent years. There are 2.92 Billion internet users in world. The more Internet access we have, the simpler it is to use the services of cloud computing. In addition, the more we use these services, the more we want to access our data. Having one copy of a business plan on your office computer will not help you if you are away from your office. However, if you have stored it on cloud, then you can access it easily.

Advantages [7]

1. **Accessibility**: No matter where you are, you can access your data on condition that you have connection to the Internet.
2. **Low power**: When your major applications are cloud computing, the front-end computers need not be powerful. These computers must only be able to run the interface for the applications, and on the other end, the server can perform the required processing.
3. **Outsource administration**: If you shift your organization to the cloud, then you do not have to bother about preserving your own systems functioning, repaired, and secure.
4. **Reduced cost**: There are a variety of cloud computing services that are available and cost effective instead of operating the same service yourself because they are available on a large scale by cloud service providers, and they are occasionally free.
5. **Increased storage**: Since the cloud service provider possibly has many servers that host data, accumulating extra space for storage is as easy as paying extra.

Disadvantages [7]

1. **No control**: There is no control with regard to data storage location (i.e., where your data is stored). Somebody could obtain data access without your permission if they too are a part of the data center.
2. **Downtime**: If the remote server fails, you may not be able to access your data.
3. **Privacy**: Who has the right to control your data?

4. **Regulatory conformity**: If your organization has to conform to rules, will the cloud computing service provider help you to meet the necessary regulatory compliance?
5. **Long-term viability**: Can the cloud service provider be with you for a long time? Moreover, what will happen to your data if it is shared with others?
6. **Speed and latency**: Your data accessibility speed is totally dependent on your Internet connection speed.

V. WHAT IS PRIVACY?

The thought of privacy differs widely among countries, cultures, and jurisdictions. It is designed by public expectations and legal interpretations; per se, a concise definition is indefinable if not impossible. Privacy rights are related to the collection, use, disclosure, storage, and destruction of personal data or personally identifiable information (PII). Furthermore, privacy refers to the accountability of organizations to data subjects and the transparency to an organization's practice around personal information. The American Institute of Certified Public Accountants and the Canadian Institute of Charted Accountants in the Generally Accepted Privacy Principles standards define privacy as *The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information*[8–10].

VI. WHAT IS DATA LIFECYCLE?

Private data should be handled as part of the organization's data [11]. Moreover, this data should be handled from the moment the data is perceived to its final destination [11]. Private data protection should consider cloud impact on each of the phases [11].The components within these phases are as follows:

Phase 1: Data Generation

- Ownership: Who owns PII in the organization? How is the proprietorship preserved if cloud computing is used by the organization? [11–13]

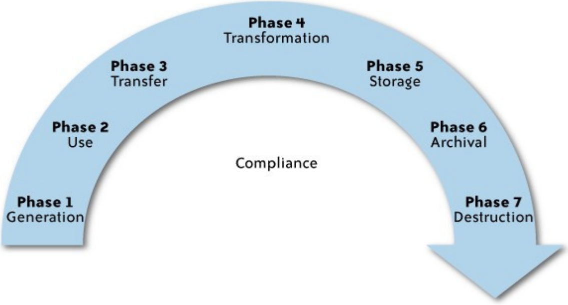


Figure 1: KPMG data lifecycle

- Classification: In what way and at what time is PII categorized? Are there any limitations of using cloud computing for particular data classes? [11, 13]
- Governance: Do we require a governance formation to confirm that PII is accomplished and safeguarded through its lifecycle when it is kept in cloud? [11]

Phase 2: Use of Data

- Internal vs. external: Is PII used only inside or outside the organization (for example, in a public cloud)?
- Third party: Is the data communicated with third parties for instance contractor support projects (CSPs)? [11, 13]
- Appropriateness: Is the usage of data coherent for which it was amassed? [11] Is the usage inside the cloud suitable based on the promises made by the organization to its subjects? [11]
- Discovery or subpoena: Is the data handled on cloud in a way that will allow the organization to abide by authorized obligations in case of lawful actions? [11]

Phase 3: Data Transfer

- Public vs. private networks: When there is transfer of information to a cloud, do the organizations use public networks and are these networks protected appropriately? (It is essential to protect PII for tackling risk and legal prerequisite levels [11].)
- Encryption conditions: Is PII encrypted? Some laws expect that the encryption of PII is possible when it is transmitted through a public network, and this exemplifies the case where a public cloud is used by the organization [11, 13].
- Access control: Are the access controls appropriate over PII when it is on cloud?

Phase 4: Data Transformation

- Derivation: Are the initial security restrictions supported when data is altered or managed on cloud? [11, 13]
- Aggregation: Is data totaled on cloud to facilitate that it is no longer associated with a distinguishable individual? [11]
- Integrity: Is PII integrity maintained when it is on cloud?

Phase 5: Data Storage

- Access control: Are there suitable controls for accessing PII when kept on cloud so that only those individuals can access need to understand it? [11]
- Structured vs. unstructured: What is the manner in which the data is stored? Will it be helpful for an organization to access it in the near future? [11]

- Confidentiality/integrity/availability: How are data confidentiality, integrity, and availability maintained on cloud?
- Encryption: Several rules and regulations mention that certain PII types should be only be stored when encrypted. Is this requirement fulfilled by CSPs?

Phase 6: Data Archival

- Legal and compliance: PII may have particular requirements that command how long data must be stored and archived. Do CSPs fulfill these requirements?
- Off-site considerations: Do CSPs provide the capability for long-term storage that supports archival requirements?
- Media concerns: Is it possible that information stored on media be accessible in future? Is there a possibility that the information stored on portable media would be easily lost? Who controls the media? What is the capacity of an organization to recuperate such media from CSPs? [11]
- Retention: How long will it be possible to retain data by CSPs? Is the retention time the same as that of the organization's retention time? [11, 14]

Phase 7: Data Destruction

- Secure: Do CSPs destroy PII attained by customers steadily to avoid potential contravention of information?
- Complete: Is the information entirely destroyed? Does the damage entirely obliterate the data?

The impact varies based on the type of cloud model that is used by the organization, the stage of private data on cloud, and the organization's nature. The subsequent analysis offers some of these considerations; however, all organizations should consider carrying out a privacy impact assessment before beginning a cloud computing enterprise that comprises personal information [11].

VII. WHERE YOU SEE CLOUD COMPUTING TECHNOLOGY?

Today cloud computing technology is used in different sectors such as social networking, e-mail services, documents/spreadsheets/hosting services, backup services, banking and financial services, healthcare services, government agencies, and educational organizations. Based on their needs, every organization is engaged with either SaaS, PaaS, or IaaS cloud service delivery model.

Corporate and government entities that are small or large in size use services provided in the public cloud to address various application needs such as customer relationship management, collaboration, and e-mail. Organizations repeatedly limit the use of the public cloud to non-mission critical applications and non-sensitive information because control and transparency are low. Moreover, public cloud services are used for servers, storage, backup infrastructure, and application development.

Leveraging cloud computing advantages, the public cloud allows organizations to speedily access applications, offload supporting infrastructure cost, and free limited IT staff for more valuable activities. In addition, it allows IT departments to rapidly implement applications and promptly scale application environments during peak demand periods, which results in superior business agility and efficiency. Similarly, public cloud services are used by consumers to streamline software use; share, store, and protect content; and allow access from any device that is connected to web.

Due to organizational cultures, safety, or supervisory apprehensions, certain organizations are unable to shift immediately into public clouds, but they can shift easily to private clouds [6]. A private cloud—known as an "internal" or "corporate" cloud—exists in the company environment (firewall) whose accessibility or availability is frequently restricted to the employees of the company [6]. For private clouds, the Gartner Institute has defined five key characteristics [6]: (i) offering resources (infrastructure and applications) as services, (ii) flexibility and scale that meet client demands, (iii) resource sharing among several users, (iv) measurement and payment as per the service use, and (v) use of technologies and Internet protocols to access cloud resources[6, 15–17]. In reality, there are supplementary cloud platforms and services that are being established on a daily basis [18]. The advancement of the cloud has viewed several enterprises progress from private to public cloud and now toward hybrid cloud [18]. Moreover, approximately all cloud environments inside a pubic cloud have a connection that helps in connecting back to the central data center [18]. Therefore, all public clouds are partially hybrid at some point in time [18]. Furthermore, the hybrid cloud offers end users with additional services as well as advantages [18]. A recent report by Gartner specified that cloud computing usage is increasing, and by 2016, this will increase to become the mass of new IT spend [18]. For cloud, 2016 will be an important year as private cloud instigates to surrender to hybrid cloud [18]. By 2017, approximately fifty percent of large enterprises will possess hybrid cloud dispositions [18, 19].However, do organizations certainly benefit from hybrid cloud? [18] What are some rational use cases and what does the future hold? [18] The healthcare organizations; marketing and multimedia organizations; and organizations that are constrained by acquiescence, protocols, and other aspects that have formerly prohibited from shifting to the cloud are adopting hybrid cloud computing [18].

VIII. ISSUES

When data and applications of the users are kept on central servers, these users fail to maintain complete control of that information [3, 20–22]. With the increasing cloud computing popularity, precarious and intermittently sensitive data that were once securely kept on personal computers now reside on online company servers [3, 23, 25]. Examples of such data include user e-mails, banking data, and complete backups of individuals' hard drives [3]. This incident creates various risks to users [3].

One of the major risks associated with storing data on cloud is the probability of data accessibility by unsolicited third parties [3]. Though there are some services of cloud computing that encode user data when stored, others store data in clear text format, thereby leaving it susceptible to a security contravention [3]. In addition, data stored on cloud might be offered to vendors. For instance, many e-mail providers permit subordinate advertising uses for e-mail broadcastings [3]. Late stre ports evidenced that many cloud computing service users enunciated concerns about the fact that a cloud computing service provider would divulge their data to others[3, 7, 23, 25]. As per a report by the Pew Internet & American Life Project, ninety percent users of cloud application are of the opinion that they would be worried if a company that hoards their data vended it to someone else(for example, a third party) [3, 24]. Eighty percent users of cloud application are of the opinion that they would be worried if a company used their photographs (snapshots) or other data in marketing campaigns, and sixty-eight percent users of cloud application are of the opinion that they would be worried if a company that provided these services analyzed their information and afterward revealed advertisements (hoardings) to them based on their activities [3, 24].

Legal rights and supervisory authority for protecting cloud computing user privacy are indistinct. Data stored on cloud may be dependent on a lesser amount of rigorous legal protection than that on a personal computer. Under the Electronic Communications Privacy Act, cloud data may be dependent on a reduced standard for rule implementation to obtain access to it than if the data were kept on a personal computer. Furthermore, the terms and conditions of service for cloud computing services say that these terms and conditions of service will maintain and release information to law implementation when served with legal process. Health information services that store the medical information of a user may not be dependent on the privacy protections of the Health Insurance Portability Protection Act [26]. When it is obvious that user data is protected, the service providers of cloud computing restrain their accountability to the user as a condition of providing the service that abandons users with limited alternatives as to whether their data is either unprotected or lost [3].

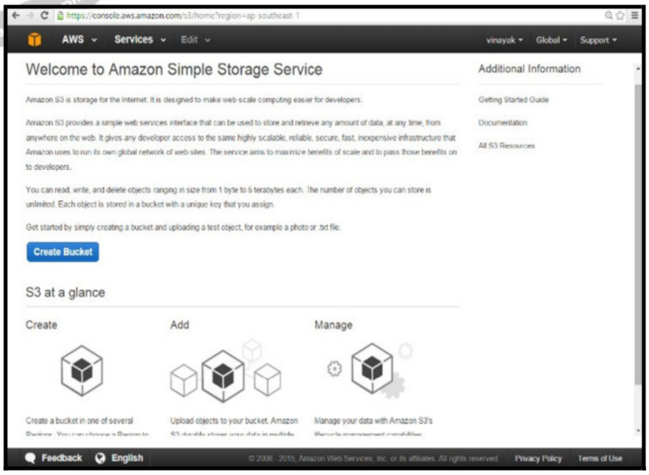
The storage of data on cloud indicates that availability to that data is entirely dependent on the terms and conditions of the cloud computing service provider. The terms and conditions of service allow the cloud computing service provider to dismiss the service at whatever time. Conversely, account deletion may not truly remove the stored data from the provider's servers. There could also be a possibility of a data hostage scenario where it is authoritative that a user gains access to online information, but the data holder rejects that access without initially receiving a payment. There are also thoughtful concerns about the dependability of cloud computing service. As mentioned above, if the cloud computing service fails, the users would have slight legal recourse [3].

IX. CASE STUDIES

1) AWS

AWS offers several cloud computing services. The services allow users to securely" manage and store numerous data types. In addition, AWS includes services such as identity, payment, database, and messaging.

Amazon supports AWS as a reliable cloud computing option, but its agreement states that "AWS reserves the right to refuse service, terminate accounts, and remove or edit content in its sole discretion." [27, 28]



Welcome to Amazon Simple Storage Service

Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for developers.

Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits on to developers.

You can read, write, and delete objects ranging in size from 1 byte to 5 terabytes each. The number of objects you can store is unlimited. Each object is stored in a bucket with a unique key that you assign.

Get started by simply creating a bucket and uploading a test object, for example a photo or .txt file.

S3 at a glance

Create

Create a bucket in one of several

Add

Upload objects to your bucket. Amazon

Manage

Manage your data with Amazon S3's

Additional Information

Getting Started Guide

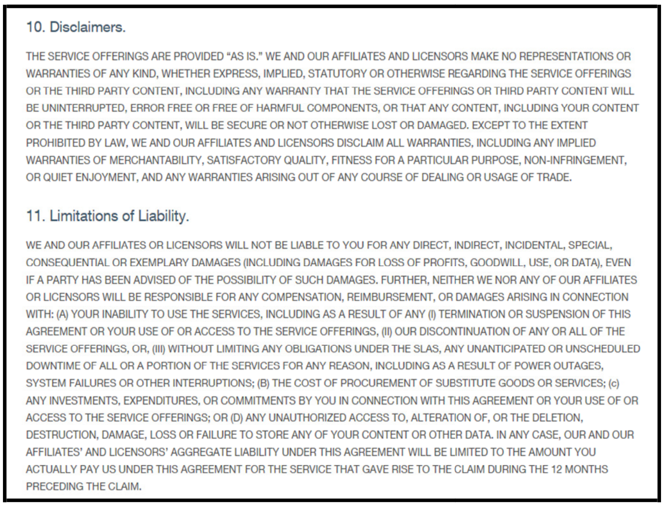
Documentation

All S3 Resources

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Figure 2: Amazon S3 webpage [3]

Furthermore, as additional protection for itself, the terms and conditions of AWS, i.e., "disclaimer of warranties and limitations of liability," state that



10. Disclaimers.

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

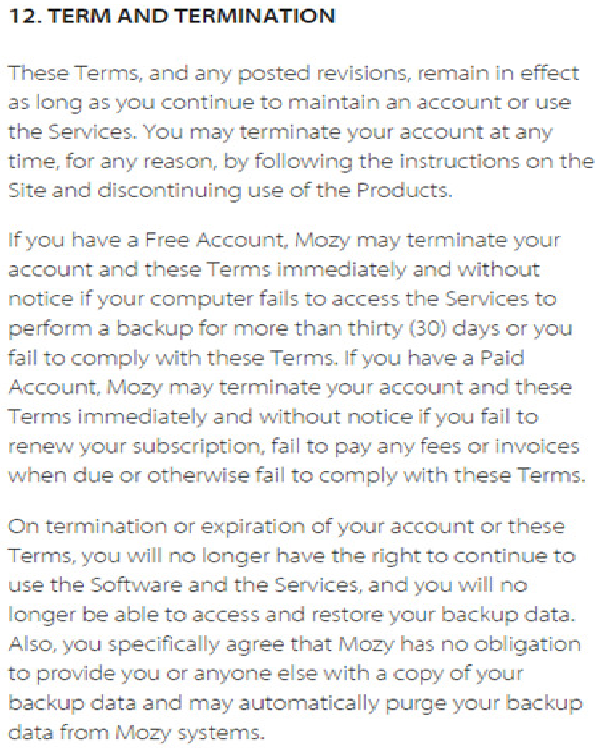
11. Limitations of Liability.

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

Figure 3: AWS disclaimer on website [3]

Amazon restricts all legal actions that may arise over its cloud computing services to King County Washington [3].

2) Mozy.com



12. TERM AND TERMINATION

These Terms, and any posted revisions, remain in effect as long as you continue to maintain an account or use the Services. You may terminate your account at any time, for any reason, by following the instructions on the Site and discontinuing use of the Products.

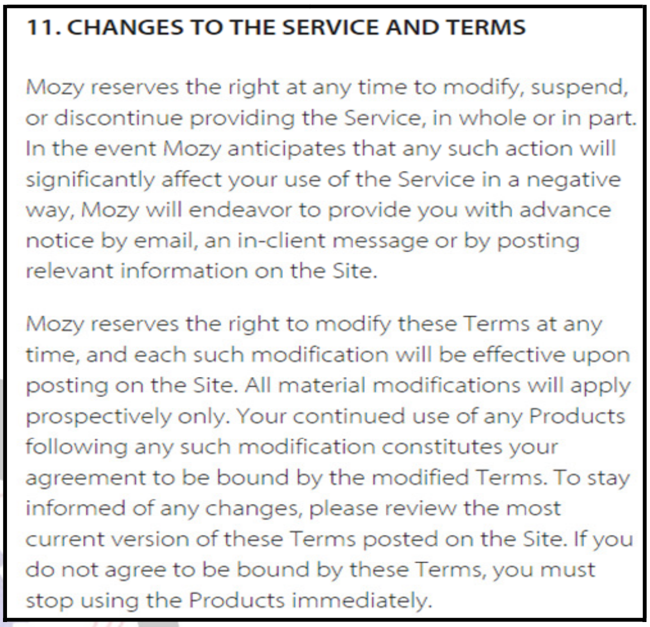
If you have a Free Account, Mozy may terminate your account and these Terms immediately and without notice if your computer fails to access the Services to perform a backup for more than thirty (30) days or you fail to comply with these Terms. If you have a Paid Account, Mozy may terminate your account and these Terms immediately and without notice if you fail to renew your subscription, fail to pay any fees or invoices when due or otherwise fail to comply with these Terms.

On termination or expiration of your account or these Terms, you will no longer have the right to continue to use the Software and the Services, and you will no longer be able to access and restore your backup data. Also, you specifically agree that Mozy has no obligation to provide you or anyone else with a copy of your backup data and may automatically purge your backup data from Mozy systems.

Figure 4: Term and termination of Mozy.com on website [3]

It offers users cloud computing services to backup pictures, documents, accounting records, or any other information that is stored on a personal computer. It reserves broad rights "at any time to modify, suspend, or discontinue providing the service or any part thereof in its sole discretion with or without notice."

Mozy.com is a part of EMC Corporation, Washington, which considers signing up for the service as an agreement of the terms. The customer may end the agreement by "destroying the software and closing the account" but does not address what happens to the information that stays in the company's hands. Account closure does not imply that information assembled or accumulated will be seized [6, 29].



11. CHANGES TO THE SERVICE AND TERMS

Mozy reserves the right at any time to modify, suspend, or discontinue providing the Service, in whole or in part. In the event Mozy anticipates that any such action will significantly affect your use of the Service in a negative way, Mozy will endeavor to provide you with advance notice by email, an in-client message or by posting relevant information on the Site.

Mozy reserves the right to modify these Terms at any time, and each such modification will be effective upon posting on the Site. All material modifications will apply prospectively only. Your continued use of any Products following any such modification constitutes your agreement to be bound by the modified Terms. To stay informed of any changes, please review the most current version of these Terms posted on the Site. If you do not agree to be bound by these Terms, you must stop using the Products immediately.

Figure 5: Changes to the service and terms by Mozy.com [3]

The company defines personal "as any data from which it is practical to directly determine an individual's identity." Furthermore, under the terms and conditions, users are conveyed that "you agree to indemnify, defend, and hold harmless and its suppliers from any and all loss, cost, liability, and expense arising from or related to your data, your use of the service..."[29].

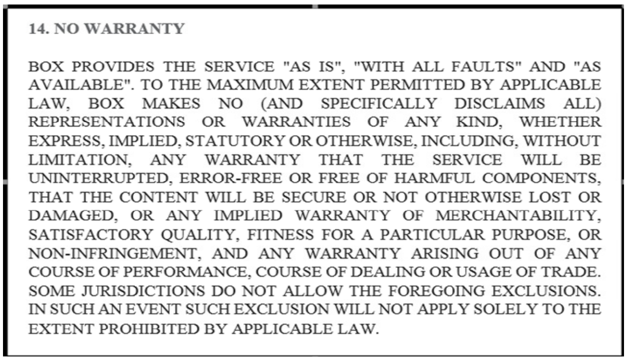
3) WebMD

Medical information services, such as WebMD, provide tools to users that help in establishing medical information accounts. These accounts can be used to record details regarding health conditions, symptoms, medications, search for medical professionals, and details about the type of medical advice obtained.

WebMD's terms and conditions of use state that "information provided to them by e-mail, blog posting, uploading photos or video, or submitting information to 'public areas' becomes WebMD's property" [30].

4) Box.com

Box.com is an important enterprise cloud storage. It transforms the process of sharing, managing, and collaborating your valuable corporate information. Without any compromise on security and user friendliness, it allows each and every employee to work securely within teams with customers and partners anywhere. It can be used as a secure content platform to keep confidential documents out of e-mail and away from unconfident consumer services [31].

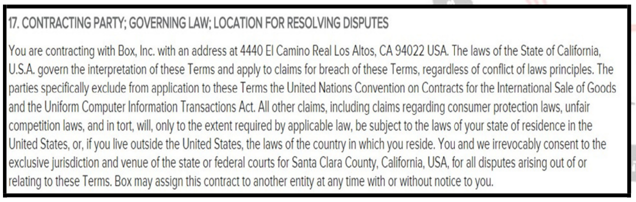


14. NO WARRANTY

BOX PROVIDES THE SERVICE "AS IS", "WITH ALL FAULTS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, BOX MAKES NO (AND SPECIFICALLY DISCLAIMS ALL) REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY THAT THE SERVICE WILL BE UNINTERRUPTED, ERROR-FREE OR FREE OF HARMFUL COMPONENTS, THAT THE CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED, OR ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, AND ANY WARRANTY ARISING OUT OF ANY COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE. SOME JURISDICTIONS DO NOT ALLOW THE FOREGOING EXCLUSIONS. IN SUCH AN EVENT SUCH EXCLUSION WILL NOT APPLY SOLELY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

Figure 6: No warranty term by Box.com [3]

Even it is the king among all giant cloud storages, its terms and conditions provide no warranty statement about continuous, error free, or free of harmful components, content security, lost, or damaged data. In addition, it states that if there are any disagreements concerning box services, users should agree to the instructions or rules of the exclusive jurisdiction and venue of the state or federal courts of Santa Clara, California, USA.



17. CONTRACTING PARTY; GOVERNING LAW; LOCATION FOR RESOLVING DISPUTES

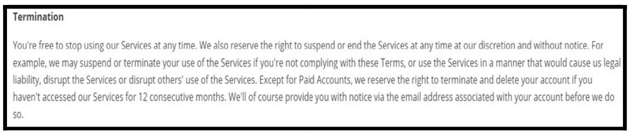
You are contracting with Box, Inc. with an address at 4440 El Camino Real Los Altos, CA 94022 USA. The laws of the State of California, U.S.A. govern the interpretation of these Terms and apply to claims for breach of these Terms, regardless of conflict of laws principles. The parties specifically exclude from application to these Terms the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act. All other claims, including claims regarding consumer protection laws, unfair competition laws, and in tort, will, only to the extent required by applicable law, be subject to the laws of your state of residence in the United States, or, if you live outside the United States, the laws of the country in which you reside. You and we irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts for Santa Clara County, California, USA, for all disputes arising out of or relating to these Terms. Box may assign this contract to another entity at any time with or without notice to you.

Figure 7: Location for resolving disputes by Box.com [3]

5) Dropbox.com

Dropbox is a place to store all your pictures, documents, videos, and files [32]. Whatever you add to it will quicklydisplay on your computer, smartphone, and even the *Dropbox* website providing 24 × 7 accessibility [32]. Using the *Dropbox* application is fast and convenient. In fact, using *Dropbox* on your computer is like using any other folder on your hard drive, except the files you drag in your *Dropbox* folder automatically synchronize online and to any other computers or mobile devices linked to your account. *Dropbox* is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and teamwork.

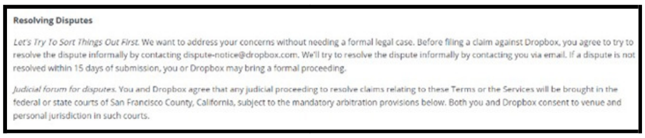
As per the terms and conditions of Dropbox, it is free to terminate services, but it does not specify what happens next when a person's account is terminated where important data is stored [33].



Termination

You're free to stop using our Services at any time. We also reserve the right to suspend or end the Services at any time at our discretion and without notice. For example, we may suspend or terminate your use of the Services if you're not complying with these Terms, or use the Services in a manner that would cause us legal liability, disrupt the Services or disrupt others' use of the Services. Except for Paid Accounts, we reserve the right to terminate and delete your account if you haven't accessed our Services for 12 consecutive months. We'll of course provide you with notice via the email address associated with your account before we do so.

They also mention that any legal dispute that cannot be mutually solved requires to follow the instructions of the federal or state courts of san Francisco, California, USA.



Resolving Disputes

Let's Try To Sort Things Out First. We want to address your concerns without needing a formal legal case. Before filing a claim against Dropbox, you agree to try to resolve the dispute informally by contacting dispute-notice@dropbox.com. We'll try to resolve the dispute informally by contacting you via email. If a dispute is not resolved within 15 days of submission, you or Dropbox may bring a formal proceeding.

Judicial forum for disputes. You and Dropbox agree that any judicial proceeding to resolve claims relating to these Terms or the Services will be brought in the federal or state courts of San Francisco County, California, subject to the mandatory arbitration provisions below. Both you and Dropbox consent to venue and personal jurisdiction in such courts.

X. DISCUSSION

So what, what does this tell us? All the organizational stakeholders should be a part of the cloud discussion and conscientiousness, i.e., IT, legal, information security, and all the relevant business groups. In addition, those stakeholders who are involved in investigating a potential cloud relationship and negotiating the terms of the relationship with a cloud provider should consider and ask the following questions both internally and the vendor before signing any contract.

- What type of data will be on cloud?
- Where do the data subjects reside?
- Where will the data be stored?
- Where are the servers?
- Will the data be transferred to other locations, and if so, when and where?
- Can certain types of data be restricted to specific geographic areas?
- What is our compliance plan for cross-border data transfers?

Are the abovementioned questions sufficient? No, but these questions lay a good foundation.

The other issues are as follows: how do we build natural cutoff points in cloud computing? When is the cloud computing group responsible for misrepresentation? When is the cloud computer user responsible for exposed data and selection of a careless vendor? When is an individual cloud resource provider responsible for misrepresenting the secure processing of transactions delegated to them? The industry of cloud computing has a natural spur to build for itself a security computing standard that each of its service members must either meet or exceed. Consequently, the client purchaser of cloud computing services obtains a cloud quality seal that can be matched against their sensitive data processing needs. Acquiescence with this seal creates a natural accountability point for cloud members as well as an industry-wide marketing point to potential customers. Such seals could also be used in a variety of global regions to advocate for reasonable accommodation in emergent law and pattern.

XI. CONCLUSION

As a cloud service customer problem, the following steps would be useful. First, sensitive data should be encrypted and defined as per client's satisfaction. Second, to process this data, processing systems must provide satisfactory proof of encrypted data, processing, and application integrity for system processing cloud available data. Third, the vendors of cloud computing must be able to regionally restrict data location, or the client may refuse to buy cloud computing services that do not officially state the allowed regional data location. As a matter of fact, regional data requirements are similar to export controlled library books where a book might be checked out of a regional library but may not leave the country even as the reader moves freely about inside the country processing the information in that book. Fortunately, computer software can be made deliberately forgetful, so export controlled information will never leave the country in the reader's long-term memory even after the book gets checked in the library. The failure to comply with such a requirement would amount to a breach of good faith contractual agreement. With some consideration to the content of cloud computing seal requirements, standards meeting or exceeding numerous present and emerging computing laws can be maintained. This is no further complex than the present state of affairs by non-cloud computing companies. Whether by plan or default inside each international corporation, there is an effective working understanding of a cloud computing seal that each of them uses to navigate and govern its approach to the present patch work of laws governing sensitive data. The business model of cloud computing will depend on its ability to provide quality assurance and subcontracting cost advantage. At the individual level, we might observe noticeable quality indicators in sensitive data handling of our individual records as more comforting than the present state of affairs.

REFERENCES

[1] http://searchstorage.techtarget.com/magazineContent/Cloudy-future-for-storage-Editorial

[2] Bansal, Nidhi. "Investigation to implicate data on clouds." arXiv preprint arXiv:1202.1366 (2012).

[3] https://epic.org/privacy/cloudcomputing/

[4] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities", COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 1540-7993/11, MARCH/APRIL 2011.

[5] Mell, Peter, and Tim Grance. "Effectively and securely using the cloud computing paradigm." NIST, Information Technology Laboratory (2009): 304-311.

[6] http://www.ibm.com/developerworks/rational/

[7] http://www.unc.edu/courses/2010spring/law/357c/001/cloudcomputing/benefits.html

[8] http://www.aicpa.org/InterestAreas/Pages/default.aspx

[9] https://en.wikipedia.org/wiki/Generally_Accepted_Privacy_Principles

[10] https://protect.iu.edu/online-safety/program/index.html

[11] http://mscerts.programming4.us/default.aspx

[12] https://www.studypool.com/discuss/1226448/PIA-PII-Model-in-Cloud-Computing

[13] http://www.slideshare.net/ISMAILRACHDAOUI/cloud-security-state-of-the-art

[14] https://www.gpo.gov/fdsys/pkg/FR-2011-06-08/pdf/2011-14055.pdf

[15] http://www.slideshare.net/VerticalSolutionsRLNelson/demystifying-the-cloud-for-gp-2013

[16] http://www.slideshare.net/VerticalSolutionsRLNelson/sage-pfw-retirement-planning

[17] http://www.gartner.com/newsroom/id/ 1035013 accessed on 20/08/2015.

[18] http://www.datacenterknowledge.com/archives/

[19] http://www.gartner.com/newsroom/ id/2613015, Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016, Analysts Examine Cloud Strategies and Adoption at Gartner Symposium/ITxpo 2013 October 21-24 in Goa, India.

[20] http://gsuinternetlaw.blogspot.in/#!

[21] http://www.cnbc.com/id/100557330

[22] http://www.nbcnews.com/technology/

[23] https://epic.org/alert/EPIC_Alert_16.06.html

[24] http://www.jdsupra.com/legalnews/complaint-and-request-for-injunction-re-62357/

[25] Pearson, Siani. “Taking account of privacy when designing cloud computing services.” Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE Computer Society, 2009.

[26] Gunn, Patrick P., Allen M. Fremont, Melissa Bottrell, Lisa R. Shugarman, Jolene Galegher, and Tora Bikson. “The Health Insurance Portability and Accountability Act privacy rule: a practical guide for researchers.” Medical care 42, no. 4 (2004): 321-327.

[27] Jansen M Silalahi, "Jansen M SilalahiDRAFTING A CLOUD COMPUTING CONTRACT", University of Oslo, Dec 2011 http://www.academia.edu/3208923/ Drafting_a_Cloud_Computing_Contract.

[28] https://aws.amazon.com/agreement last accessed on 20/08/2015.

[29] https://mozy.com/about/legal/terms last accessed on 20/08/2015.

[30] www.webmd.com/about-webmd-policies/about-terms-and-conditions-of-use last accessed on 20/08/2015.

[31] https://www.box.com/legal/termsofservice/ last accessed on 20/08/2015.

[32] https://www.youtube.com/watch?v=w38OBtCxKg0

[33] https://www.dropbox.com/terms last accessed on 20/08/2015.