On The Privacy Of Cloud Computing

Harry Katzan, Jr., Savannah State University, USA

ABSTRACT

*Cloud computing is **a** model for providing on-demand access to computing service via the Internet. In this instance, the Internet is the transport mechanism between a client and a server located somewhere in cyberspace, as compared to having computer applications residing on an "on premises" computer. Adoption of cloud computing practically eliminates two ongoing problems in IT service provisioning: the upfront costs of acquiring computational resources and the time delay of building and deploying software applications. The technology is not without a downside, which in this case is the privacy of business and personal information. This paper provides a conspectus of the major issues in **cloud computing privacy** and should be regarded as an introductory paper on this important topic.*

Keywords: Cloud computing, software architecture, software-as-a-service, platform-as-a-service, infrastructure-as-a-service, private cloud, public cloud, community cloud, hybrid cloud, privacy, trustworthy computing, security.

INTRODUCTION

It seems as though most computer users would like privacy and information security while having convenient access to interlinked computing services both on-premises and in the cloud. In this instance, the cloud is a metaphor for the Internet, which can be used as the delivery vehicle for computing services and the storage of information. Advocates of cloud computing are faced with two major problems, that is, in addition to the usual problem of transferring one's resources from one operational environment to another. The first of the major problems is the ongoing feeling that we are experiencing the "déjà vu all over again" syndrome. Many of us have gone through an avalanche of new technological advances intended as solutions to our administrative and operational problems – at least, the ones involving management and information systems. Some of the technical innovations we have experienced include scalable main-frame computers, advanced operating systems, time sharing, client/server, online systems, mini computers, personal computers, artificial intelligence, hand-held computers, the Internet and the World Wide Web, mobile computers, social networking, and by the time this paper is published, there will no doubt be several more entries to add to the list. So one has reason to be skeptical of someone writing that cloud computing is worthy of serious attention. Of course, we think it is, for obvious reasons.

The second major issue is privacy, and it stems from the fact that with cloud computing, data and programs are stored off-premises and managed by a service provider. When a third party gets a hold of your data, who knows what is going to happen to it. Many proponents of cloud computing conveniently characterize it as analogous to the electric utility. The basic idea is that the private generators of the twentieth century were replaced by the electricity grids of today without undue concern. It is easy to imagine, however, that the measurement of electricity usage would have been of concern to some people in the early 1900s. Although similar in some respects, cloud computing is different in one important way. The cloud will typically handle information, which is the basic unit of exchange, about which security and privacy are of paramount concern. With electricity, there is no interest in individual electrons. With information, the key issues are identity, security, and privacy. The side issues are one's inherent identity attributes (such as age, gender, and race), accountability (for online computing activities), and anonymity (in order to preserve free speech and other forms of behavior for the parties involved). The main consideration may turn out to be a matter of control, because from an organizational perspective, control over information has historically been with the organization that creates or maintains it. From a personal perspective, on the other hand, a person should have the wherewithal to control their identity and the release of information about themselves, and in the latter case, a precise determination of to whom it is released and for what reason. Who owns the data? Is it the person about whom the data pertains? Is it the organization that prototypically manages the data? Or, is it the cloud

provider that physically stores the data somewhere out in cyberspace? Consider your financial information. Is it your property or is it your bank's business property? We will try to provide a perspective on this important issue in the following sections. Privacy issues are not fundamentally caused by cloud computing, but they are exacerbated by employing the technology for economic benefit. To put it as diplomatically as possible, if a business employs cloud computing to save money on its IT bill, should it be allowed to do so at the "privacy" expense of its customers?

CLOUD COMPUTING CONCEPTS

Cloud computing is an architectural model for deploying and accessing computer facilities via the Internet. A cloud service provider would supply ubiquitous access through a web browser to software services executed in a cloud data center. The software would satisfy consumer and business needs. Because software availability plays a major role in cloud computing, the subject is often referred to as *software-as-a-service* (SaaS). Conceptually, there is nothing particularly special about a cloud data center, because it is a conventional web site that provides computing and storage facilities. The definitive aspect of a cloud data center is the level of sophistication of hardware and software needed to scale up to service a large number of customers. Cloud computing is a form of service provisioning where the service provider supplies the network access, security, application software, processing capability, and data storage from a data center and operates that center as a utility in order to supply on-demand self service, broad network access, resource pooling, rapid application acquisition, and measured service. The notion of measured service represents a "pay for what you use" metered model applied to differing forms of customer service.

Cloud Service Characteristics

The operational environment for cloud computing supports three categories of informational resources for achieving agility, availability, collaboration, and elasticity in the deployment and use of cloud services that include software, information, and cloud infrastructure. The *software category* includes system software, application software, infrastructure software, and accessibility software. The *information category* refers to large collections of data and the requisite database and management facilities needed for efficient and secure storage utilization. The *category of cloud infrastructure* is comprised of computer resources, network facilities, and the fabric for scalable consumer operations. We are going to adopt a description of a cloud framework that necessarily includes three forms of description: terminology, architectural requirements, and a reference model. The description generally adheres to the National Institute of Standards and Technology (NIST) cloud-computing paradigm. (Mell 2009b, Brunette 2009)

Agility generally refers to the ability to respond in a timely manner to market and product changes through business alignment, which is achieved by decreasing the lead time to deploy a new application by reducing or eliminating the effect of training, hardware acquisition, and software acquirement. Thus, the IT department is able to respond more quickly to business needs. *Availability* concerns two aspects of computer utilization: the time that the facilities are available for use and the scope of the resources that are available. Cloud computing facilitates *collaboration* through network access, provided that the software tools for end user cooperation are available. *Elasticity* is the characteristic of cloud services that permits computing and storage capability to be scaled up to meet demands on an on-demand basis through resource pooling.

Based on this brief assessment, we can characterize cloud computing as possessing the following characteristics: (Nelson 2009)

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

The benefit of having lower costs and a less complex operating environment is particularly attractive to small-to-medium-sized enterprises, certain governmental agencies, research organizations, and many countries.

Cloud Computing Utilization

There are four main actors – so to speak – in cloud computing: the cloud service provider, the software service provider, the customer, and the user. Each of the actors represents centers of computer-related activity that can overlap to some degree. The *cloud service provider* (CSP) owns the infrastructure, hardware, software, and network facilities needed to supply cloud computing services managed by a cloud operating system. The CSP performs a function known as *hosting* that can be used to run computer programs, referred to as applications. This facility, known in some circles, as a *cloud platform* (CP), can be regarded as an application service that runs in the cloud. More specifically, a cloud platform provides services to applications in the same manner that "software as a service" programs provide services to clients using the cloud as a transport medium. A cloud platform is as much about operating in the cloud, as it is about developing applications for the cloud. *A software service provider* develops applications that are used by customers to obtain computing services. The SSP can be an independent software vendor (ISV) or an organization that develops a software package that uses the CP as a delivery vehicle for computing and provides application services to customers. ISV software can be used by many customers in the usual fashion for software deployment. When it is shared during operation to achieve economy-of-scale, it is regarded as a multi-tenant model, wherein each customer is one of the tenants. The *customer* (C) is typically an enterprise that is comprised of several employees that use the application and are regarded as users. The *user* (U) is probably going to be a person that uses the cloud computing service via a web browser in one of the following capacities: as an employee of an organization that is contracted to use SaaS provided by an ISV or acquired independently to run in the cloud on a cloud platform; or as a user of third-party SaaS developed by an ISV or the CSP. The four relevant scenarios are summarized by the following schema:

CSP – CP – ISV – C – U
CSP – CP – ISV – U
CSP – CP – C – U
CSP – CP – U

For example, you will be using scenario CSP – CP – ISV – C – U if your company has acquired an operational package from a software vendor and is hosting that software in the cloud. Similarly, you will be using scenario CSP – CP – U if you are using an office package provided by a CSP and accessed via your browser. This form of conceptualization is important from a privacy point-of-view, because each exchange between modules represents a touch point for privacy concerns.

Cloud Platform

A cloud platform provides the facility for an application developer to create applications that run in the cloud or use cloud platform services that are available from the cloud. Chappell lists three kinds of cloud services: SaaS user services, on-premises application development services (attached services), and cloud application development services. (Chappell 2009) An *SaaS application* runs entirely in the cloud and is accessible through the Internet from an on-premises browser. *Attached services* provide functionality through the cloud to support service-oriented architecture (SOA) type component development that runs on-premises. *Cloud application development services* support the development of applications that typically interact while running in the cloud and on-premises.

A cloud platform can be conceptualized as being comprised of three complementary groups of services: foundations, infrastructure services, and application services. The *foundation* refers to the operating system, storage system, file system, and database system. *Infrastructure services* include authorization/authentication/security facilities, integration between infrastructure and application services, and online storage facilities. *Application services* refer to ordinary business services that expose "functional" services as SOA[1] components. Cloud platforms are a lot like enterprise-level platforms, except that they are designed to scale up to support Internet-level operations.

[1] SOA is an acronym for Service-Oriented Architecture that denotes the development and operation of applications assembled from software components residing in the cloud.

CLOUD ARCHITECTURE

Cloud architecture is a collection of three categories of information resources for the deployment and use of cloud services that include software, information, and cloud infrastructure. (Katzan 2009) The software category includes system software, application software, infrastructure software, and accessibility software. The information category refers to large collections of data and the requisite database and management facilities needed for efficient and secure storage utilization. The category of cloud infrastructure includes compute resources, network facilities, and the fabric for scalable consumer operations. We are going to adopt an ontological formulation to the description of a cloud framework that necessarily includes three classes of information: terminology, architectural requirements, and a reference model. The description generally adheres to the National Institute of Standards and Technology (NIST) cloud-computing paradigm. (Mel op cit)

Service Models

The cloud service models give a view of what a cloud service is. It is a statement of being. A cloud service system is a set of elements that facilitate the development of cloud applications. (Youseff 2009) Here is a description of the three layers in the NIST service model description: (Mel op cit.)

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

The three service model elements should be deployed in a cloud environment with the essential characteristics in order to achieve a cloud status.

Service Deployment Models

The essential elements of a cloud service system are given above. In order to develop enterprise-wide applications, a domain ontological viewpoint has to be assumed with deployment models from the following list: (Mel op cit.)

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Most cloud software service application domains will be synthesized from a combination of the deployment models.

CLOUD SECURITY

The scope of cloud security is huge by any objective measure. One ordinarily thinks of cloud security in terms of authorization, authentication, accountability, end-to-end trust, and so forth. However, it is important to view cloud security concerns in a broader context of data protection, disaster recovery, and enterprise continuity. The storage of customer data may be useful for operations and research but also opens the door for misuse and violation of privacy policy. Government regulations, such as the FFIEC (Federal financial Institutions Examination Council), HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standards), are in place and strict adherence to the guidelines by cloud service providers can only be achieved through systems design and effective auditing, (Web Hosting Fan 2009) Accordingly, even though we are going to concentrate on the former, it is important to keep the latter in mind through PCI DSS, SOX, and HIPAA compliance[2]. This can be achieved through ISO/IEC 27001:2005 certification and SAS 70 Type I and II attestations. (Shinder 2009) In this section, we are going to develop an operational basis for cloud computing privacy based on security.

Identity

Identity is a means of denoting an entity in a particular namespace and is the basis of security and privacy – regardless if the context is digital identification or non-digital identification. We are going to refer to an identity object as an *entity*. An entity may have several identities and belong to more than one namespace. An identity denotation is based on attributes as suggested by Figure 1.

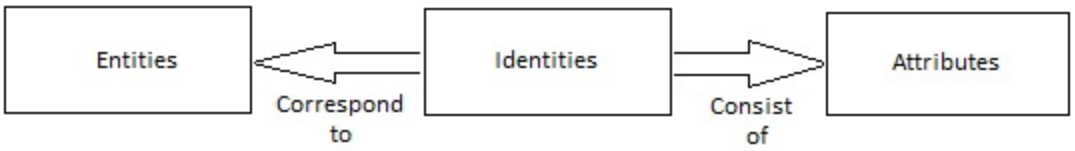

Figure 1. Conceptual relationship between entities, identities, and attributes

A pure identity denotation is independent of a specific context, and a federated identity reflects a process that is shared between identity management systems. When one identity management system accepts the certification of another, a phenomenon known as "trust" is established. The execution of trust is often facilitated by a third party that is acknowledged by both parties and serves as the basis of digital identity in cloud services.

Access to computing facilities is achieved through a process known as authentication, whereby an entity makes a claim to its identity by presenting an identity symbol for verification and control. Authentication is usually paired with a related specification known as authorization to obtain the right to address a given service.

Authentication

In a cloud computing environment, an SaaS service provider is commonly faced with two situations: the single tenant model and the multi-tenant model. In the single tenant model, typified by the [CSP – CP – C – U] and

[2] ISO/EC 27001:2005 specifies standards for a documented Information Security Management System. SAS 70 is a statement on auditing standards developed by the American Institute of Certified Public Accountants. SOX, which stands for the Sarbanes-Oxley Act of 2002, signifies the public company accounting reform and investor protection act, developed in response to business failures with the objective of assistance to the investment community.

[CSP – CP – U] scenarios, given previously, a single sign-on to the cloud service is ordinarily required. This means that the end user would then have to log on to the local computer and then log on to the application service at the cloud platform. This is typically the case with consumer cloud services and customer-developed application software. When the application requires an additional sign-on, it must maintain its own user accounts – a process known as *delegated administration*. This instance is depicted in Figure 2.

When authentication requires a sign-on to an enterprise system running on the cloud and then on to a specific application, a multiple sign-on would ordinarily be required. With a decentralized authentication system, as suggested by Figure 3, the user would sign-on to an authentication server that would issue a token accepted by a federated server as proof of identity, required by specific applications. An SaaS provider with thousands of customers would prefer a decentralized solution in lieu of establishing a trust relationship with each of its customers.

Common authenticators are something you know, something you have, something you are, and where you are.

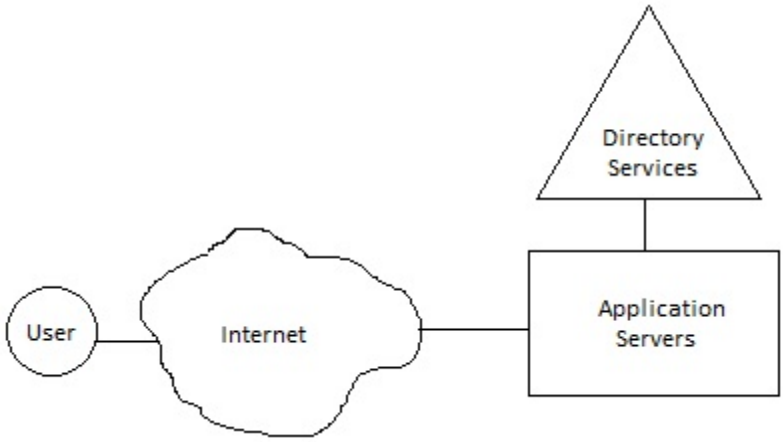

Figure 2. Centralized authentication system

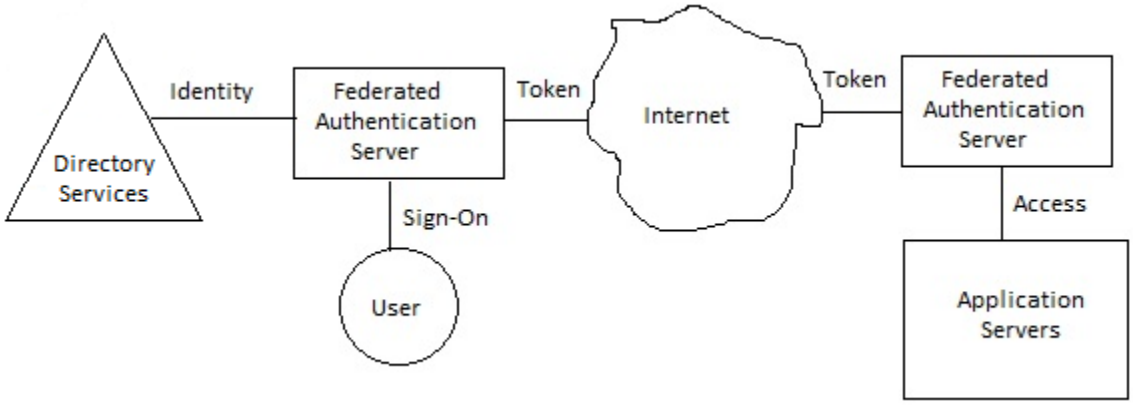

Figure 3. Decentralized authentication system

Authorization

Typically, *authorization* refers to permission to perform certain actions. In cloud computing, users are assigned roles that must match corresponding roles associated with a requisite SaaS application. Each SaaS application contains a set of roles pertinent to the corresponding business function. Access is further controlled by

business rules that specify conditions that must be met before access is granted. The role/business-rule modality also applies to storage in the cloud, and this is where the practice of privacy kicks in.

In general, the combination of identification and authentication determine who can sign-on to a system – that is, who is authorized to use that system. Authorization, often established with access control lists, determines what functions a user can perform. A related measure, known as accountability, records a user's actions. Authorization cannot occur without authentication.

In general, there are two basic forms of access control: discretionary access control, and mandatory access control. With discretionary access control (DAC), the security policy is determined by the owner of the security object. With mandatory access control (MAC), the security policy is governed by the system that contains the security object. Privacy policy should, in general, be governed by both forms of access control. DAC reflects owner considerations, and MAC governs inter-system controls.

Accountability

Accountability is determined by audit trails and user logs that are prototypically used to uncover security violations and analyze security incidents. In the modern world of computer and information privacy, accountability would additionally incorporate the recording of privacy touch points to assist in managing privacy concerns. Although the Internet is a fruitful technology, it garners very little trust. Why? It is very cumbersome to assign responsibility for shortcomings and failure in an Internet operational environment. Failure now takes on an additional meaning. In addition to operational failure, it is important to also include "failure to perform as expected," as a new dimension.

Trustworthy Computing

Trustworthy computing refers to the notion that people in particular and society as a whole can trust computers to safeguard things that are important to them. Medical and financial information are cases in point. Computing devices, software services, and reliable networks are becoming pervasive in everyday life, but the lingering doubt remains over whether or not we can trust them. Expectations have risen with regard to technology such that those expectations now encompass safety, reliability, and the integrity of organization that supply the technology. Society will only accept a technological advance when an efficient and effective set of policies, engineering processes, business practices, and enforceable regulation are in place. We are searching for a framework to guide the way to efficacy in computing.

It is generally felt that a framework for understanding a technology should reflect the underlying concepts required for its development and subsequent acceptance as an operational modality. A technology should enable the delivery of value rather than constrain it, and that is our objective with trustworthy computing. Security has changed with the advent of the Internet and the well-publicized threats to computing and storage facilities. In the past, security was primarily concerned with keeping harmful people out. In the modern world of the Internet, the objective is to enable the right people to access the right information in a trusted environment. Thus, security is an enabler for greater freedom and confidence in information systems.

As with many utilities, trustworthy computing should be intuitive, controllable, reliable, and predictable. In order to achieve these lofty goals, we are going to look to the framework developed at Microsoft (Mundie 2002) consisting of goals, means, and execution. The set of *goals* reflects a subject's perspective and is comprised of security, privacy, reliability, and business integrity considerations. The set of *means* refers to the computer industry's viewpoint and includes secure-by-design, secure-by-default, secure-in-deployment, fair-information principles, availability, manageability, accuracy, usability, responsiveness, and transparency. *Execution* concerns the manner in which an organization does business and includes intent, implementation, evidence, and integrity. One approach to using the framework is through the concept of a *trusted stack* constructed from five important elements: secure hardware, a trusted operating system, trusted applications, trusted people, and trusted data. (Charney 2008)

A simple view of trustworthy computing is that it is comprised of security, privacy, and usability. Usability and security have been introduced. All that is required to achieve essential trust in cloud computing is privacy.

CLOUD PRIVACY

The cloud will typically process and store information about which privacy is of paramount concern. The main issue is identity, which serves as the basis of privacy or lack of it, and undermines the trust of individuals and organizations in other entities. The key consideration may turn out to be the integrity that organizations adopt when handling personal information and how accountable they are about their information practices. From an organizational perspective, control over information should remain with the end user or the data's creator with adequate controls over repurposing. From a personal perspective, the person should have the wherewithal to control his or her identity as well as the release of socially sensitive identity attributes. Who owns the data? Is it the person about whom the data pertains? Is it the organization that prototypically stores the data? Or, is it the cloud provider that physically stores the data somewhere out in cyberspace? As an example, is your financial information (as personal data) your property or is it your bank's business property?

Key Factors in Privacy Protection

One of the beneficial aspects of the present concern over information privacy is that it places the person about whom data are recorded in proper perspective. Whereas such a person may be the object in an information system, he or she is regarded as the subject in privacy protection. This usage of the word *subject* is intended to imply that a person should in fact have some control over the storage of personal information.

More specifically, the *subject* is the person, natural or legal, about whom data are stored. The *beneficial user* is the organization or individual for whom processing is performed, and the *agency* is the computing system in which the processing is performed and information is stored. In many cases, the beneficial user and the subject are members of the same organization. In most instances, however, this will not be the case. For example, the agency may be a service company, and the subject may be a creditor.

In general, the beneficial user obtains value from the data processed and has some control over the manner and time span in which the processing is performed. The agency need not be aware of the end use of the information or how and when the processing is performed.

The heart of the issue is *privacy protection*, which normally refers to the protection of rights of individuals. While the concept may also apply to groups of individuals, the individual aspect of the issue is that which raises questions of privacy and liberty

Privacy Theory

Privacy refers to the claim of persons to determine when, how, and to what extent information about themselves is communicated to others. Much of the literature is concerned with the physical state of being private. The four states of being private are solitude, intimacy, anonymity, and reserve. *Solitude* implies physical separation from the group. *Intimacy* implies participation in a small unit that achieves corporate solitude. *Anonymity* implies freedom from identification and surveillance, which may be informational or physical. *Reserve* implies the creation of a psychological barrier that protects the individual from unwanted intrusion. (Katzan 1980)

The states serve to provide personal autonomy, emotional release, self evaluation, and limited and protected communication. Privacy is needed to realize basic personal and organizational objectives. Also, there is a universal tendency of individuals to invade the privacy of others and of society as a whole to engage in surveillance to enforce its norms.

Privacy Domain

Personal information is being collected about individuals through information and communication technology inherent in most social and economic activities. When we search the Web, our search phrases are being

stored for possible analysis and review. (Conti 2009) When we drive our cars, our license plate numbers and locations are stored by law enforcement. When we purchase items with a credit card, a record of our activity is available to organizations with authority. The list could go on and on, but is well summarized by Ann Cavoukian[3]:

Our digital footprints are being gathered together bit by bit, megabyte by megabyte, terabyte by terabyte, into personas and profiles and avatars – virtual representations of us, in a hundred thousand simultaneous locations. … novel risks and threats are emerging from this digital cornucopia. Identity fraud and theft are the diseases of the Information Age, along with new forms of discrimination and social engineering made possible by the surfeit of data.

There are other considerations to the subject of privacy. The majority of companies doing business online and not-online have privacy policies in place that do little to protect consumer privacy. (ACLU 2010, p. 8) The policies give wide latitude to the companies and essentially provide nothing more than informing the consumer of what do, as if telling constitutes legality. The consumer is given few choices to control personal information. In fact, the current situation concerning privacy is that the consumer wants greater control over their information, and a 2009 study found that 69% of adult Internet consumers want the legal right to know everything that a company knows about them. (ACLU op cit.)

Privacy Assessment

The Federal Bureau of Investigation (U.S.A.) lists seven criteria for evaluating privacy concerns for individuals and for designing cloud computing applications[4]: (FBI 2004)

- What information is being collected?
- Why is the information being collected?
- What is the intended use of the information?
- With whom will the information be shared?
- What opportunities will individuals have to decline to provide information or to consent to particular uses of the information?
- How will the information be secure?
- Is this a system of records?

Since privacy is a fundamental right in the United States, the above considerations obviously resulted from extant concerns by individuals and privacy rights groups. In a 2009 Legislative Primer, the following concerns are expressed by the Center for Digital Democracy: (CDD 2009, p. 2)

Tracking people's every move online is an invasion of privacy. Online behavioral tracking is even more distressing when consumers aren't aware who is tracking them, that it's happening, or how the information will be used. Often consumers are not asked for their consent and have no meaningful control over the collection and use of their information, often by third parties with which they have no relationships.

Online behavioral tracking and targeting can be used to take advantage of vulnerable consumers. Information about a consumer's health, financial condition, age, sexual orientation, and other personal attributes can be inferred from online tracking and used to target the person for payday loans, sub-prime mortgages, bogus health cures and other dubious products and services. Children are an especially vulnerable target audience since they lack the capacity to evaluate ads.

Online behavioral tracking and targeting can be used to unfairly discriminate against consumers. Profiles of individuals, whether accurate or not, can result in "online redlining" in which some people are offered certain consumer products or services at higher costs or with less favorable terms than others, or denied access to goods and services altogether.

[3] *Privacy in the Clouds* by Ann Cavoukian, Information and Privacy Commissioner of Ontario (Cavoukian 2009), p. 3.
[4] Actually, there are eight items, but the eighth concerns FBI operations. Please see the reference.

Online behavioral profiles may be used for purposes beyond commercial purposes. Internet Service Providers (ISPs), cell phone companies, online advertisers and virtually every business on the web retains critical data on individuals. In the absence of clear privacy laws and security standards these profiles leave individuals vulnerable to warrantless searches, attacks from identity thieves, child predators, domestic abusers and other criminals. Also, despite a lack of accuracy, employers, divorce attorneys, and private investigators may find the information attractive and use the information against the interests of an individual. Individuals have no control over who has access to such information, how it is secured, and under what circumstances it may be obtained.

Based on these issues, the primer includes the following recommendations for legislative consideration: (CDD op cit., p. 4)

- *Individuals should be protected even if the information collected about them in behavioral tracking cannot be linked to their names, addresses, or other traditional "personally identifiable information," as long as they can be distinguished as a particular computer user based on their profile.*
- *Sensitive information should not be collected or used for behavioral tracking or targeting. Sensitive information should be defined by the FTC and should include data about health, finances, ethnicity, race, sexual orientation, personal relationships and political activity.*
- *No behavioral data should be collected or used from children and adolescents under 18 to the extent that age can be inferred.*
- *There should be limits to the collection of both personal and behavioral data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.*
- *Personal and behavioral data should be relevant to the purposes for which they are to be used.*
- *The purposes for which both personal and behavioral data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes, and with any change of purpose of the data the individual must be alerted and given an option to refuse collection or use.*
- *Personal and behavioral data should not be disclosed, made available or otherwise used for purposes other than those specified in advance except: a) with the consent of the individual; or b) by the authority of law.*
- *Reasonable security safeguards against loss, unauthorized access, modification, disclosure and other risks should protect both personal and behavioral data.*
- *There should be a general policy of openness about developments, practices, uses and policies with respect to personal and behavioral data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*
- *An individual should have the right: a) to obtain from a behavioral tracker, or otherwise, confirmation of whether or not the behavioral tracker has data relating to him; b) to have communicated to him data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.*
- *Consumers should always be able to obtain their personal or behavioral data held by an entity engaged in tracking or targeting.*
- *Every entity involved in any behavioral tracking or targeting activity should be accountable for complying with the law and its own policies.*
- *Consumers should have the right of private action with liquidated damages; the appropriate protection by federal and state regulations and oversight; and the expectation that online data collection entities will engage in appropriate practices to ensure privacy protection (such as conducting independent audits and the appointment of a Chief Privacy Officer).*
- *If a behavioral targeter receives a subpoena, court order, or legal process that requires the disclosure of information about an identifiable individual, the behavioral targeter must, except where otherwise prohibited by law, make reasonable efforts to a) notify the individual prior to responding to the subpoena, court order, or legal process; and b) provide the individual with as much advance notice as is reasonably practical before responding.*

- *The FTC should establish a Behavioral Tracker Registry.*
- *There should be no preemption of state laws.*

Accordingly, it would seem that some form of data governance is in order to protect the privacy rights of subjects.

Privacy Analysis of Cloud Computing

In order to integrate the cloud computing and privacy issues, the *World Privacy Forum* has come up with a set of findings that are summarized in the following list[5]:

- Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and government information.
- A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider.
- For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider.
- Disclosure and remote storage may have adverse consequences for the legal status of or protections for personal or business information.
- The location of information in the cloud may have significant effects on the privacy and confidentiality protection of information and on the privacy obligations of those who process or store the information.
- Information in the cloud may have more than one legal location at the same time, with differing legal consequences.
- Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters.
- Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.
- Responses to the privacy and confidentiality risks of cloud computing include better policies and practices by cloud providers, changes to laws, and more vigilance by users.

Some of the open items in cloud computing privacy that immediately come to mind are listed as follows:

- A business sharing information with a cloud provider.
- Consequences of third party storage for individuals and business.
- Information disclosure to private parties.
- Location of cloud data and local law.
- Change of a cloud provider.
- Cloud provider disclosure obligations.
- Audits, security, and subpoenas.

Based on this analysis, it would seem that consumer-based cloud services would be good candidates for public and community clouds. For business, education, and government, private and hybrid clouds are prudent options until the legal questions can be resolved.

QUICK SUMMARY

- Cloud computing is a means of accessing computer facilities via the Internet. (The *cloud* is a metaphor for the Internet.)
- Cloud service facilities are characterized by four key factors: necessity, reliability, usability, and scalability.
- Software-as-a-service (SaaS) is software deployed as a hosted service and accessed over the Internet.

[5] See Gellman (2009, p. 6) for a description of the findings. This is the sole reference to this subject.

- A cloud platform is based on an operating system that runs in the cloud and provides an infrastructure for software development and deployment.
- Cloud privacy includes a set of complex and comprehensive issues, and users and providers should proceed with caution when moving to the cloud.

ACKNOWLEDGEMENT

Thanks to Margaret Katzan for reading the manuscript and the reviewers for insightful comments and suggestions.

AUTHOR INFORMATION

Professor Harry Katzan, Jr., teaches at the Savannah State University, the cornerstone of business research in the Southeastern United States. He has written extensively in computer science.

REFERENCES

1. ACLU of Northern California. 2010. Cloud Computing: Storm Warning for Privacy? www.dotrights.org, (downloaded 3/11/2010).
2. Brunette, G. and R. Mogull (ed). 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009.
3. Cavoukian, A. 2009. Privacy in the Clouds. Toronto: Information and Privacy Commission of Ontario (www.ipc.on.ca).
4. Center for Digital Democracy (CDD). 2009. Online Behavioral Tracking and Targeting: Legislative Primer September 2009. www.democraticmedia.org/privacy-legislative-primer. (downloaded 3/11/2010).
5. Chong, F. and G. Carraro. 2006. Architecture Strategies for Catching the Long Tail. Microsoft Corporation.
6. Chappell, D. 2009. Introducing the Windows Azure Platform. Microsoft Corporation.
7. Charney, S. 2008. Establishing End to End Trust. Microsoft Corporation.
8. Conti, G. 2009. *Googling Security*. Upper Saddle River, NJ: Addison-Wesley.
9. Federal Bureau of Investigation. 2004. Privacy Impact Assessment. www.fbi.gov/biometrics.htm. (downloaded 2/20/2010).
10. Gellman, R. 2009. Privacy in the Clouds: Risks to Privacy and Confidentiality form Cloud Computing. World Privacy Forum (February 23, 2009).
11. Katzan, H. 1980. *Multinational Computer Systems: An Introduction to Transnational Data Flow and Data Regulation*. New York: Van Nostrand Reinhold Co.
12. Katzan, H. 2009. Cloud Computing Economics: Democratization and Monetization of Services. *Journal of Business & Economics Research*, 7(6):1-11.
13. Mell, P. and T. Grance. 2009a. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Information Technology Laboratory, Version 15, 10-7-09. (http://www.csrc.nist.gov/groups/SNS/cloud-comjputing/index.html)
14. Mell, P., Badger, L., and T. Grance. 2009b. Effectively and Securely Using the Cloud Computing Paradigm. National Institute of Standards and Technology, Information Technology Laboratory, 10-7-09. (http://www.csrc.nist.gov/groups/SNS/cloud-comjputing/index.html)
15. Mundie, C., de Vries, P., Haynes, P., and M. Corwine. 2002. Trustworthy Computing. Microsoft Corporation.
16. Nelson, M. 2009. Cloud Computing and Public Policy. Briefing Paper for the ICCP Technology Foresight Forum. JT03270509, DATI/ICP(2009)17.
17. Shinder, D. 2009. Microsoft Azure: Security in the Cloud. WindowSecurity.com (downloaded 1/27/2010).
18. Web Hosting Fan. 2009. The Security and Privacy Concerns of Cloud Computing. September 24, 2009. www.webhostingfan.com/page/13 (downloaded 3/2/2010).
19. Youseff, L., Butrico, M., and D. Da Silva. 2009. Toward a Unified Ontology of Cloud Computing. (Available from the following: (lyouseff@cs.uscb.edu), (butrico@us.ibm.com) , and (dilmasilva@us.ibm.com).