Privacy in the Clouds:
Risks to Privacy and Confidentiality from Cloud Computing

Prepared by Robert Gellman
for the World Privacy Forum

February 23, 2009

Brief Summary

This report discusses the issue of cloud computing and outlines its implications for the privacy of personal information as well as its implications for the confidentiality of business and governmental information. The report finds that for some information and for some business users, sharing may be illegal, may be limited in some ways, or may affect the status or protections of the information shared. The report discusses how even when no laws or obligations block the ability of a user to disclose information to a cloud provider, disclosure may still not be free of consequences. The report finds that information stored by a business or an individual with a third party may have fewer or weaker privacy or other protections than information in the possession of the creator of the information. The report, in its analysis and discussion of relevant laws, finds that both government agencies and private litigants may be able to obtain information from a third party more easily than from the creator of the information. A cloud provider's terms of service, privacy policy, and location may significantly affect a user's privacy and confidentiality interests.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group. It focuses on a range of privacy matters, including financial, medical, employment, and Internet privacy. The World Privacy Forum was founded in 2003.

Table of Contents

I. Introduction and Summary of Findings

Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information. A principal goal of this analysis is to identify privacy and confidentiality issues that may be of interest or concern to cloud computing participants. While the storage of user data on remote servers is not new, current emphasis on and expansion of cloud computing warrants a more careful look at its actual and potential privacy and confidentiality consequences.

Cloud Computing Today: Issues and Implications

A considerable amount of cloud computing technology is already being used and developed in various flavors (e.g., private, public, internal, external, and vertical).[1] Not all types of cloud computing raise the same privacy and confidentiality risks.[2] Some believe that much of the computing activity occurring today entirely on computers owned and controlled locally by users will shift to "the cloud" in the future. Whether this will turn out to be the case is uncertain and not especially important here. This analysis does not support or oppose cloud computing. The continuing development and maturation of cloud computing services is an undeniable reality.

The definitional borders of cloud computing are much debated today. For present purposes, *cloud computing* involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking sites, and many more.

Any information stored locally on a computer could be stored in a cloud, including email, word processing documents, spreadsheets, videos, health records, photographs, tax or other financial information, business plans, PowerPoint presentations, accounting information, advertising campaigns, sales numbers, appointment calendars, address books, and more. The entire contents of a user's storage device may be stored with a single cloud provider or with many cloud providers. Whenever an individual, a business, a government agency, or other entity shares information in the cloud, privacy or confidentiality questions may arise.

---

[1] Researchers and others are still sorting out the proper classification and terminology for describing cloud computing. See, e.g., Lamia Youseff et al, *Toward a Unified Ontology of Cloud Computing,* <http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf>. Last accessed Feb. 19, 2009.

[2] For example, a user who publishes photographs using a cloud provider's facilities may face few risks because the photos are already public. However, a business that stores unpublished financial results with a provider that reserves the right to read, use, or make public any information on the provider's facilities faces a risk of premature release of information or use of that information by the cloud provider in ways that could violate securities law.

Some definitions of terms will help to clarify the discussion here:

- A customer or potential customer of a cloud computing service is a *user*. The user may be an individual, business, government agency, or any other entity.

- The organization that offers the cloud computing service is a *cloud service provider,* or *cloud provider*. A cloud *provider* may be an individual, a corporation or other business, a non-profit organization, a government agency or any other entity.

- A cloud service provider is one type of *third party* that maintains information about, or on behalf of, another entity.

A typical information exchange in cloud computing occurs when a user shares information with the cloud provider. Can any and all information be legally shared in a cloud service? With cloud computing, many factors affect the answer to this fundamental question. The shortest answer to the question, however, is that for some information and for some users, sharing may be illegal, may be limited in some ways, or may affect the status or protections of the information shared.

Generally, an individual is free to share his or her personal information with a cloud provider. For a business, disclosing the personal information of customers or employees, or other business information to a cloud provider is often unrestricted by law because no privacy law or other law applies. For example, privacy laws do not cover most marketing records in the United States. Even when privacy laws apply to particular categories of customer or employee information, disclosure to a cloud provider may not be restricted.

For a federal agency, various laws may have bearing on the decision to employ a cloud provider. For example, the Privacy Act of 1974[3] imposes standards for the collection, maintenance, use, and disclosure of personal information. The use of cloud computing for personal information held by a federal agency may violate the Privacy Act of 1974, especially if there is no contractual arrangement between the agency and the cloud provider. If a cloud provider offers services to the public on behalf of agencies, other Privacy Act requirements may apply, as may security obligations under various federal laws and policies. Federal record management and disposal laws may also be relevant.[4]

This document analyses and illustrates some of the key privacy and confidentiality consequences of cloud computing. No attempt is made to be comprehensive or to consider all potentially relevant laws. This document does not review state laws that may impose stronger or additional protections for personal information. The focus in this analysis is primarily on the privacy and confidentiality consequences of cloud providers located in the United States, with some discussion of international implications.

[3] 5 U.S.C. § 552a.
[4] See, e.g., 44 U.S.C. chapters 31 & 33.

Findings

This analysis of cloud computing finds the following:

- **Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information.** This document identifies multiple and complex privacy and confidentiality issues that may be of interest or concern to cloud computing participants. While storage of user data on remote servers is not a new activity, the current emphasis on and expansion of cloud computing warrants a more careful look at the privacy and confidentiality consequences.

- **A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider.** Those risks may be magnified when the cloud provider has reserved the right to change its terms and policies at will. The secondary use of a cloud computing user's information by the cloud provider may violate laws under which the information was collected or are otherwise applicable to the original user. A cloud provider will also acquire transactional and relationship information that may itself be revealing or commercially valuable. For example, the sharing of information by two companies may signal a merger is under consideration. In some instances, only the provider's policy will limit use of that information. Many users are likely not aware of the details set out in the terms of service for cloud providers or of the consequences of sharing information with a 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.** Procedural or substantive barriers may prevent or limit the disclosure of some records to third parties, including cloud computing providers. For example, health record privacy laws may require a formal agreement before any sharing of records is lawful. Other privacy laws may flatly prohibit personal information sharing by some corporate or institutional users. Professional secrecy obligations, such as those imposed on lawyers, may not allow the sharing of client information. Sharing information with a cloud provider may undermine legally recognized evidentiary privileges. Records management and disposal laws may limit the ability of a government agency to use cloud computing for official records.

- **Disclosure and remote storage may have adverse consequences for the legal status of or protections for personal or business information.** For example, a trade secret shared with a cloud provider may lose some of its legal protections. When a person stores information with a third party (including a cloud computing provider), the information may have fewer or weaker privacy protections than when the information remains only in the possession of the person. Government agencies and private litigants may be able to obtain information from a third party more easily than from the original owner or creator of the content. A cloud provider might even be compelled to scan or search user records

to look for fugitives, missing children, copyright violations, and other information of interest to government or private parties. Remote storage may additionally undermine security or audit requirements.

- **The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.** Any information stored in the cloud eventually ends up on a physical machine owned by a particular company or person located in a specific country. That stored information may be subject to the laws of the country where the physical machine is located. For example, personal information that ends up maintained by a cloud provider in a European Union Member State could be subject permanently to European Union privacy laws.

- **Information in the cloud may have more than one legal location at the same time, with differing legal consequences.** A cloud provider may, without notice to a user, move the user's information from jurisdiction to jurisdiction, from provider to provider, or from machine to machine. The legal location of information placed in a cloud could be one or more places of business of the cloud provider, the location of the computer on which the information is stored, the location of a communication that transmits the information from user to provider and from provider to user, a location where the user has communicated or could communicate with the provider, and possibly other locations.

- **Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters.** Some jurisdictions in the United States require computer technicians to report to police or prosecutors evidence of child pornography that they find when repairing or otherwise servicing computers. To the extent that cloud computing places a diverse collection of user and business information in a single location, it may be tempting for governments to ask or require cloud providers to report on particular types of criminal or offensive behavior or to monitor activities of particular types of users (e.g., convicted sex offenders). Other possibilities include searching for missing children and for music or software copyright violations.

- **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.** The law badly trails technology, and the application of old law to new technology can be unpredictable. For example, current laws that protect electronic communications may or may not apply to cloud computing communications or they may apply differently to different aspects of cloud computing.

- **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.** If the cloud computing industry would adopt better and clearer policies and practices, users would be better able to assess the privacy and confidentiality risks they face. Users might avoid cloud computing for some classes of information and might be able to select a service that meets their privacy and confidentiality needs for other categories of information. For those risks that cannot be addressed by changes in policies

and practices, changes in laws may be appropriate. Each user of a cloud provider should pay more – and indeed, close – attention to the consequences of using a cloud provider and, especially, to the provider's terms of service.

II. When Can a Business Share Information with a Cloud Provider?

The United States has several privacy laws applicable to particular types of records or businesses. Some of these laws establish privacy standards that have bearing on a decision by a business to use a cloud provider. Others laws do not. Some laws specifically allow a business to share personal information with another company that provides support services to the business. Specific statutory references to the use of a service provider have no apparent pattern in privacy laws. Some privacy laws have them; some do not.

For example, **the Gramm-Leach-Bliley Act**[5] restricts financial institutions from disclosing a consumer's personal financial information to a non-affiliated third party. Disclosure to a service provider is generally not restricted. However, the terms under which information is disclosed and the rights acquired by service providers could make a difference to the legality of the disclosure or subsequent use.

The same conclusion applies to video rental records protected by the **Video Privacy Protection Act**[6] and to cable television subscriber records protected by the **Cable Communications Policy Act**.[7] These particular laws may not directly prevent the use of a cloud provider.

Other laws, however, *do* limit the use of a cloud provider. The next section analyzes the consequences of laws affecting decisions about using cloud computing for business data. Both procedural and substantive barriers to the use of cloud computing exist for some records and some businesses.

HIPAA and Business Associate Agreements

For most health records, procedural requirements apply to the disclosure of health records subject to the federal health privacy rule[8] issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA privacy rule establishes a comprehensive scheme regulating the use and disclosure of individually identifiable health information by covered entities. (Covered entities are principally health care providers and health plans.)

[5] 15 U.S.C. § 6802.
[6] 18 U.S.C. § 2710.
[7] 47 U.S.C. § 551.
[8] 45 C.F.R. Part 164.

Before a covered entity may transfer protected health information to a service provider, the entity and the provider must enter into a *business associate agreement*.[9] While a business associate is not directly subject to the HIPAA rule currently, the agreement between the business associate and the covered entity would essentially require the business associate to comply with the same standards that apply to the covered entity.

A hospital subject to HIPAA could not decide to store patient records in a storage facility offered by a cloud provider without a business associate agreement with the cloud provider. In some cases, the substantive requirements of HIPAA will directly conflict with a cloud provider's terms of service. A service provider cannot use or disclose health records in a way that conflicts with the HIPAA standards.[10] Thus, a HIPAA-covered entity could violate HIPAA by storing patient records at a cloud provider with a terms of service that allow the provider to publish any information stored on its facilities.

Tax Preparation Laws

Customers of tax preparers enjoy some statutory and regulatory privacy protections. These customer protections in turn limit the ability of a tax preparer to use a cloud provider. It is difficult to see how a tax preparer could comply with the IRS rules and still disclose tax return information to a cloud provider. A tax preparer could not use a foreign cloud provider without taxpayer consent, and even then, disclosure of a Social Security Number (SSN) could well be impossible.

For companies that offer tax return preparation services through online facilities with online storage of taxpayer information, Internal Revenue Service rules expressly limit disclosure of tax return information.[11] Disclosure of tax return information by a tax preparer to another person in the same firm as the preparer is permissible.[12] However, disclosure by one tax return preparer to another tax return preparer outside the United States requires taxpayer consent.[13] Disclosure to a contractor of the tax preparer for specified activities is permissible as long as employees of the contractor receive notice of the tax law's rules for the use and disclosure of tax return information.[14] Disclosure of a taxpayer's Social Security Number to a return preparer outside the

[9] Id. at §§ 164.502(e), 164.504(e). A covered entity that hires a third party to act merely as a conduit for protected health information (e.g., the US Postal Service or a private courier) does not need a business associate agreement. A conduit transports information but does not access it except infrequently as necessary for the performance of the service, or as required by law. In theory, a cloud provider could possibly be a conduit for HIPAA purposes, but much depends on the terms of service. If the cloud provider reserves any rights to review, use, disclose, or post information submitted by a user, the provider will not qualify as a conduit.

[10] Other health privacy laws may also impose limits on information sharing. See, e.g., Confidentiality of Alcohol and Drug Abuse Patient Records Regulation, 42 C.F.R. Part 2. Whether any of these disclosure restrictions would be triggered if the patient information were encrypted is beyond the scope of this analysis.

[11] 26 U.S.C. §§ 6713, 7216; 26 C.F.R. § 301.7216.

[12] 26 C.F.R. § 301.7216-2(c)(2).

[13] 26 C.F.R. § 301.7216-2(c)(3).

[14] 26 C.F.R. § 301.7216-2(d)(2).

United States is prohibited even with taxpayer consent, subject to an exception not likely to be practical for a cloud provider.[15]

Violence Against Women Act

The statutory scheme regulating domestic violence service providers under the 2005 amendments to the Violence Against Women Act[16] appears to prohibit all disclosures not compelled by statute or a court, except disclosures with the consent of the data subject.[17] Disclosure to a cloud provider or to any service under any terms or conditions appears prohibited by this strict non-disclosure standard.

Legally Privileged Information

When information is legally privileged, the sharing of that information with a cloud provider might affect the validity of the privilege. The law of privilege is complicated and varies from privilege to privilege (e.g., doctor-patient, lawyer-client, priest-penitent) and from state to state. For some privileges, the communication of privileged information to a third party can undermine or vitiate the privilege. For example, if a reporter stores notes or drafts of a story at a cloud provider's website, any privilege that the reporter had may be undermined.

Whether the storage of a privileged communication or document with a cloud provider actually affects privilege may depend in part on the terms under which the service is offered. If the cloud provider merely stores data and disclaims the right or ability to look at the stored information, the argument for privilege notwithstanding the disclosure may be stronger.

However, if the cloud provider has the right to read, disclose, or transfer information entrusted to it, the argument for privilege may be hard to make. If the provider has the ability to use the content of documents to make decisions about the user (e.g., which advertisements to serve to the user), the argument for privilege may be even harder to sustain.

For example, if a physician or patient shares a record containing a confidential communication with a cloud provider and the cloud provider uses the information in that record to serve an advertisement to the patient, the viability of the privilege may be fatally undermined.

Professional Secrecy Obligations

A person who has a fiduciary or professional obligation to a client may have limitations on disclosure that extend far beyond the conditions necessary to qualify for privilege. This could include a lawyer, doctor, broker, or other professional. For example, as reflected in the American

[15] 26 C.F.R. § 301.7216-3(b)(4).
[16] Public Law 109-162 as amended by Public Law 109–271.
[17] 42 U.S.C. § 13925(b).

Bar Association Model Rules of Professional Conduct, part of a lawyer's duty is to protect information relating to the representation of a client. It applies to "virtually all information coming into a lawyer's hands concerning a client."[18]

None of the exceptions to the non-disclosure obligation appears to cover disclosure to a cloud or other service provider.[19] The ABA rule allows disclosures impliedly authorized in order to carry out the representation, but whether a lawyer's use of a cloud provider would qualify under this standard is debatable. The cloud provider's terms of service might make a significant difference to the interpretation of the professional obligation. If the provider can use or disclose the lawyer's record, any sharing may breach the professional obligation.

III. Consequences of Third Party Storage for Individuals and Businesses

Even when no laws or obligations block the ability of a user to disclose information to a cloud provider, disclosure may still not be free of consequences. Information stored with a third party (including a cloud computing provider) may have fewer or weaker privacy protections than information in the possession of the creator of the information. Government agencies and private litigants may be able to obtain information from a third party more easily than from the creator of the information. The expanded ability of the government and others to obtain information from a third party affects both businesses and individuals.

Compelled Disclosure to the Government

For information that would have otherwise been in the sole possession of a user, the transfer of the information to a cloud provider creates new opportunities for the information to end up in government hands without notice to the user and without the user having an opportunity to object. For many users, the loss of notice of a government demand for data is a significant reduction in rights.

United States v. Miller

A seminal court case about the privacy of information held by a third party is *United States v. Miller*.[20] Miller was convicted of federal crimes based in part on evidence obtained from his banks. The government served subpoenas on the banks, and neither the banks nor the government notified Miller about the demand for or production of the records. Miller argued that

[18] Hazard & Hodes, The Law of Lawyering §9.7 (2003 & Supp. 2004) (3rd edition).
[19] ABA Model Rules of Professional Conduct, Rule 1.6(b)(1)-(6). Disclosure with client consent would be permissible.
[20] 425 U.S. 435 (1976).

the government's obtaining and use of his bank records violated his Fourth Amendment rights against unreasonable searches and seizures.

The Supreme Court found that the government's demand on the banks did not affect any Fourth Amendment interests of the depositor. The Court stated expressly that the records were not respondent's private papers but were business records of the banks that were voluntarily conveyed to the banks and exposed to bank employees in the ordinary course of business. Thus, the records were not entitled to the Fourth Amendment's protection against the compulsory production of private papers.

While there are some aspects of *Miller* that may be unique to banking, the case stands generally for the proposition that an individual's personal record held by a third party does not have the same constitutional privacy protection as applies to the same record held by the individual. From a privacy perspective, this proposition is unsettling because of the volume of personal information necessarily held by third parties today. Third parties that maintain personal information include banks, credit card companies, utilities, health care providers, insurers, various kinds of websites, transit authorities, government agencies, and others.

Shortly after the Supreme Court decided *Miller*, the Congress took steps to overturn the decision in part. The Right to Financial Privacy Act[21] limits the ability of the Federal Government to obtain customer financial records from banks. The Act requires the government to notify a bank customer of its subpoena, summons, or formal written request for the customer's bank records and provides the customer with an opportunity to challenge the demand in court prior to disclosure. The law also allows for delay of notice under specified conditions, it includes numerous exceptions to notice, and it offers a customer limited grounds for challenging governmental process. The ultimate value to customers of the law's notice and opportunity to challenge is debatable. Nevertheless, the law establishes a narrow statutory precedent that limits government access to third party records in the interest of privacy.

Electronic Communications Privacy Act (ECPA)

In an electronic environment, the Electronic Communications Privacy Act of 1986[22] (ECPA) provides some protections against government access to electronic mail and other computer records held by third parties (e.g., Internet service providers).

ECPA sought to bring the constitutional and statutory protections against the wiretapping of telephonic communications into the computer age. ECPA is a difficult law to understand and apply, in part because the law is old and relies on a model of electronic mail and Internet activity that is generations behind current practice and technology. Most observers agree that ECPA is significantly out-of-date in at least some ways. Nevertheless, ECPA reflects a legislative recognition that some Internet activities deserve protection from the *Miller* proposition that there is no reasonable expectation of privacy in records maintained by third parties. The difficulty with ECPA is figuring out what those protections apply to and when.

[21] 12 U.S.C. §§ 3401-3422.
[22] The parts of ECPA most relevant to this discussion are found in 18 U.S.C. §§ 2510-2522, 2701-2712.

Distinctions recognized by ECPA include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service. Case law and scholarly discussions continue to address and debate the proper application of the ECPA's distinctions to current Internet activities. The courts have struggled in applying ECPA to situations not contemplated by the law's drafters.

The precise characterization of an activity can make a significant difference to the protections afforded under ECPA. For example, if an "electronic communications service" holds a text message in "electronic storage", then law enforcement requires a probable cause warrant to obtain access. If a "remote computing service" stores the same text message on behalf of the subscriber, then law enforcement does not need a warrant, and a subpoena is sufficient. Whether a search engine or social networking site is a remote computing service remains in dispute.

The privacy protections available under ECPA for the wide range of cloud computing activities are difficult to predict. Indeed, simply identifying all cloud computing applications would be a significant challenge by itself. Factors that may affect the proper application of ECPA to cloud computing activities include:

1) The precise characterization of the activity as a communication or as storage (which itself may come in several flavors), complicated by the recognition that an activity can move from being a communication to being a stored communication depending on time and possibly other factors,

2) Whether the information in question is content or non-content (e.g., header or transaction information),

3) The nature of the service, e.g., whether it is an electronic communication service or a remote computing service,

4) The terms of service established by the cloud provider,

5) Any consent that the user has granted to the provider or others,

6) The identity of the service provider, for example, if the cloud provider is itself a government agency, the provider's obligation would be different from those of a non-governmental cloud provider, and the rights of users would also be different.

It is unlikely that anyone could provide a definitive opinion about the privacy protections available for information in the cloud against a government or other demand for disclosure. The protections might or might not be greater than those otherwise available for records held by a third party. The significant uncertainty that surrounds protections against government demands for information held by cloud providers is the point here.

USA PATRIOT Act

The federal government's authority to compel disclosure of records held by cloud providers extends beyond ECPA. The USA PATRIOT Act,[23] as originally enacted in 2001 and amended in 2005, includes provisions allowing the FBI access to any business record. Although a court order is required, the FBI's authority under the USA PATRIOT Act is sufficient to extend to a record maintained by a cloud provider.[24]

Other provisions of the Act expanded the government's ability to use a National Security Letter (a form of administrative subpoena) to obtain records.[25] The authorities that are found in the USA PATRIOT Act weaken some of the privacy protections previously found in ECPA, and they generally expand the government's ability to compel disclosure. Those who receive an order to disclose information under these authorities are highly limited in their ability to reveal that they received the order. That means that a user who provided records to a cloud provider for storage or processing is not likely to know that the government obtained the records.

Disclosure to Private Parties

The government is not the only entity that might seek to obtain a user's record from a cloud provider. A private litigant or other party might seek records from a cloud provider rather than directly from a user because the cloud provider would not have the same motivation as the user to resist a subpoena or other demand. Disclosures to third parties by a cloud provider could create problems with other laws, principles, and interests.

HIPAA and compelled disclosures

The HIPAA health privacy rule imposes some limits on compelled disclosures. A legal demand by a private party to a cloud provider for disclosure of protected health information would have to follow the procedures set out in the rule governing judicial and administrative proceedings.[26] In general, the rule means that anyone seeking access via a court order, subpoena, discovery request, or the like must notify the patient, and the patient has an opportunity to object to the disclosure. The necessity under HIPAA for a business associate agreement means that a cloud provider should be on notice that it maintains patient records to which specific procedures apply if the provider receives an order for disclosure of a record that the provider holds on behalf of a covered entity. While the burden of those procedures falls on the person seeking the records,

[23] Public Law 107-56.
[24] 50 U.S.C. § 1862.
[25] 18 U.S.C. §§ 2709, 3511(b).
[26] 45 C.F.R. § 164.512(e).

demands for records held by a cloud provider for a covered entity can raise more complex problems of control and compliance.

In contrast to HIPAA, other personal information shared by a business with a cloud provider is not likely to have similar requirements for an agreement between the business and the provider. When a cloud provider allows anyone to use its facilities without any contractual or other prearrangement, the provider may know little or nothing about the information that a user puts in the cloud. If a cloud provider is not contractually obliged to consult with the user, is not motivated to consult with the user, or is actively prevented from notifying the user, any subsequent disclosure by way of court order or subpoena may have unwanted consequences for the user or for the ultimate data subject.

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) imposes limits on the use of credit reports by a user of credit report to a *permissible purpose*.[27] If a creditor stores a credit report with a cloud provider, and a third party obtains the report from the cloud provider, the legal limit on use could be violated.

An FCRA violation could also occur if the cloud provider uses the stored credit report for an improper purpose. The FCRA imposes a restriction on credit report users, but it does not have a mandatory procedure comparable to the HIPAA business associate agreement that would inform a cloud provider that it has information subject to disclosure limits. Thus, a credit grantor that casually stores records with a cloud provider could unexpectedly confront a legal problem.

Other privacy laws

Other privacy laws that impose limits on the use and disclosure of personal information could also be violated by activities of a cloud provider. Consider a cloud provider that stores information on behalf of a company subject to a privacy law, such as the Video Privacy Protection Act that limits some disclosures of customer data. If the cloud provider's terms of service allow the provider to see, use, or disclose the information, the cloud provider's actions could result in a violation of the law.

For example, a cloud provider's general reservation of rights might give the provider the ability to read records about a user's customer, and then to use the information to market directly to the customer in violation of a privacy law applicable to the user. The cloud provider may have no notice or way to determine if information stored with it is subject to legal restrictions. It may not care. Use of information by a cloud provider could expose the user to liability because its actions

[27] 15 U.S.C. § 1681b(f). The FCRA also imposes limits on disclosure of credit reports by credit bureaus. 15 U.S.C. § 1681b. A credit bureau is less likely to use a cloud provider to store credit reports than an end user of credit reports is.

resulted in an invasion of the privacy interests of individuals that a law obliged the user to protect.

These types of situations are more likely to arise when a cloud provider operates under terms of service that reserve for the provider broad rights to use or disclose information shared by a user. Problems may also arise when a user (e.g., corporate or government employee) makes an ad hoc decision to share data with a cloud provider without adequate legal review of the terms of service or consideration of any applicable restrictions on data.

Bankruptcy of a cloud provider

In the case where a cloud provider files for bankruptcy, the ability of a bankruptcy trustee to dispose of the provider's assets or to change the use and disclosure terms for information assets could have significant consequences for users. Bankruptcy law provides limited procedural protections for customers if the debtor had a privacy policy prohibiting the transfer of personally identifiable information to unaffiliated persons.[28] If the bankruptcy affected the privacy interests of customers of a provider's users, the limited bankruptcy procedural protection might not apply at all. In the case of a cloud provider that did not have a privacy policy because it only provided services to business, that procedural protection would not apply for lack of a debtor privacy policy.

Trade secrets

Storage of trade secrets with a cloud provider could have legal consequences. Consider a company that owns a trade secret and that places the trade secret in a document disclosed to a cloud provider. This scenario presents two different types of risks.

First, according to the Uniform Trade Secrets Act,[29] a trade secret must be, among other things, "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Whether disclosure of the trade secret to a cloud provider would violate the obligation to make reasonable effort to maintain secrecy is debatable. Arguably, even if the terms of service established by the cloud provider recognize the confidentiality of information given to the cloud provider, it might not be enough to avoid that debate. However, terms of service that give the cloud provider rights to see, use, or disclose information would provide a strong basis for an argument that the trade secret no longer exists.

Second, consider a private litigant that seeks to obtain records from a cloud provider rather than from the owner. The owner would be able to resist a subpoena for the trade secret by seeking to quash the subpoena. However, the cloud provider would not necessarily be under any obligation to resist a subpoena or to notify the main party at interest that it received a subpoena.

---

[28] 11 USC §§ 332, 363.

[29] <http://www.law.upenn.edu/bll/archives/ulc/fnact99/1980s/utsa85.htm>. Last accessed Feb. 19, 2009.

IV. Other Cloud Computing Issues

Several other aspects of cloud computing affect privacy and confidentiality interests. The most important of these are the terms of service and privacy policy established by a cloud provider. The location of data, ownership of the cloud provider, use of transactional information, and other issues are considered here.

Terms of Service and Privacy Policy

From a privacy and confidentiality perspective, the terms of service may be the most important feature of cloud computing for an average user who is not subject to a legal or professional obligation. The discussion above and throughout this analysis repeatedly addresses the relevance of a provider's terms of service to privacy and confidentiality protections.

Scope of rights claimed by cloud service providers

It is common for a cloud provider to offer its facilities to users without individual contracts and subject to the provider's published terms of service. A provider may offer different services, each of which has distinct terms of service. A cloud provider may also have a separate privacy policy. It is also possible for a cloud provider to conduct business with users subject to specific contractual agreements between the provider and the user that provides better protections for users. The contractual model is not examined further here.

If the terms of service give the cloud provider rights over a user's information, then a user is likely bound by those terms. A cloud provider may acquire through its terms of service a variety of rights, including the right to copy, use, change, publish, display, distribute, and share with affiliates or with the world the user's information. There may be few limits to the rights that a cloud provider may claim as a condition of offering services to users.

The scope of the rights claimed by a cloud provider could affect the legality of information sharing by a user. The actual use by a cloud provider or by anyone that the cloud provider transferred the information to could violate a statute in a way that could create liability on the part of the original user. If a user fails to safeguard data properly and a third party uses information in violation of a legal duty, the user could be both civilly and criminally liable. Much might depend on the specific standards in the statute, but the possibility may be unnerving to some.

Changeable terms of service

It is common for an Internet company establishing terms of service or a privacy policy to reserve the right to change the terms or the policy without limit. If so, then a user may not be able to take comfort when a cloud provider does not currently claim rights over the user's data. A cloud provider could change the terms of service and privacy policy at any time.

Merely returning to the cloud provider's website might constitute acceptance of the new terms so a user may not even have a practical opportunity to remove information from the provider's site before the new terms become effective. For a user who concluded that sharing documents under a cloud provider's terms of service did not violate any of the user's legal obligations, a change in the terms of service could create legal or other liabilities for the user.

Even if a user discovers unacceptable new terms and closes an account with the provider, the provider may still have rights over backup copies of the user's information still in the provider's control. A cloud provider's terms of service can also make it procedurally cumbersome for a user to fully terminate the user's relationship with the provider. It is always possible that terms of service or a privacy policy could be found to be unconscionable, unenforceable, unfair, or deceptive. However, that may be small consolation to a user forced to engage in expensive litigation to preserve the user's rights over the user's own information.

Termination of services

The terms of service may allow a cloud provider to terminate services to a user at any time. The result could be that a user who did not maintain a full backup of information stored in the cloud may lose the information permanently. This could present a significant problem to any business or individual simply because of the loss of data. The loss may be especially troublesome for a business required to document its activities and for a government agency that has an obligation under law not to dispose of records without following required procedures.

Location of Cloud Data and Applicable Law

The location of a cloud provider's operations may have a significant bearing on the law that applies to a user's data. The actual location may or may not appear in the provider's terms of service. Even if the provider discloses the location of records, the provider may change it, possibly without any notice. The same data may be stored in multiple locations at the same time. A provider who promises to maintain user data in a specific jurisdiction (e.g., the United States) may reduce some of the location risks that a user may face.

The European Union's Data Protection Directive[30] offers an example of the importance of location on legal rights and obligations. Under Article 4 of the Directive, a national data protection law applies when a controller located in the territory of Member State processes personal information. A cloud provider in an EU Member State could bring personal data obtained from a non-EU based user under a European data protection law. Once EU law applies to the personal data, the data remains subject to the law, and the export of that data will thereafter be subject to EU rules limiting transfers to a third country. Thus, if a U.S. company gave its data to a cloud provider based in France, French data protection law would attach, and the export of the data back to the United States could be restricted or prohibited. In addition, the subjects of the data would acquire rights of notice, access, correction, etc. under French law. *Once an EU Member State's data protection law attaches to personal information, there is no clear way to remove the applicability of the law to the data.*

It may be possible to argue that the cloud provider is not a controller with respect to a user's data because it is a mere processor only transiting the data through a Member State. That argument is uncertain on its own, and it is an even more difficult argument if the cloud provider reserves in its terms of service the right to use, disclose, or otherwise process the data. Indeed, it is possible depending on those terms for the cloud provider to be the effective controller of a user's data for EU purposes. If so, the cloud provider would be obliged to undertake the data protection obligations of a controller with respect to the use's data. If so, the situation is likely to be undefined because of the lack of any relevant understanding between the user and the cloud provider respecting data protection obligations. Any resulting litigation is likely to be novel and lengthy.

Other legal consequences aside from the application of data protection rules could also follow from location choices. Consider, for example, if the law of trade secrets in the jurisdiction where a user's data is stored is less protective of information than the law in the jurisdiction where the user is physically located. A litigant might be able to select a forum to dispute the trade secret claim or otherwise rely on the trade secret standards of a jurisdiction unanticipated by a user. It is also possible that data held in another country would be more accessible to government access than the user could expect at home.

Other location issues are foreseeable. For example, a United States cloud provider of services to a firm or an individual may itself subcontract to or avail itself of the service of another cloud provider. That second-degree cloud provider may be located in another country or another state in the United States. The user may be unaware of the existence of a second-degree provider or the actual location of the user's data. Indeed, it may be impossible for a casual user to know in advance or with certainty which jurisdiction's law actually applies to information entrusted to a cloud provider. These uncertainties complicate the ability of a user to determine the protections that apply to data entrusted to a cloud provider.

[30] 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, <http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf> and <http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf>. Last accessed Feb. 19, 2009.

For some, cloud computing may be a sword and for others, cloud computing may be a shield. Arguably, uncertainty about location could provide a practical benefit to someone trying to keep data beyond the reach of a government or litigant. The model is *onion routing*. *Onion routing* is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through multiple network nodes called onion routers. Each onion router removes a layer of encryption to uncover routing instructions and sends the message to the next router where the activity repeats until the message reaches its final destination.[31]

Intermediary nodes do not know the origin, destination, and contents of the message. One could envision a series of *onion cloud providers* who move information through various jurisdictions to make it hard for governments or litigants to find or obtain the information of a user of onion cloud providers. Each attempt to force a cloud provider to turn over a user's information might have to use compulsory powers in multiple jurisdictions, first to find the data's actual location and then to obtain the data. The ability of a government or private litigant to pursue a user's data through multiple jurisdictions might not be easy, fast, or possible.

Ownership and Transfer of a Cloud Provider

Who owns a cloud provider? The provider's terms of service may not reveal the real owner. The actual owner could be under the control of a subsidiary of a competitor, a U.S. government agency, a foreign agency, or an Internet news service. If a government agency owns the provider, terms of service that allow sharing with affiliates could result in all of the user's information being obtained by prosecutors or intelligence agencies without further notice or process.

A variety of circumstances could lead to the transfer of a cloud provider's operations, together with all user information maintained by the provider. These include sale of the cloud service, sale of the cloud company, a merger, seizure by the government for non-payment of taxes, and bankruptcy. Some bankruptcy issues have been discussed above. It is also possible that a user's information will be considered a corporate asset and available for sale or transfer through the bankruptcy process to other parties. This may be more likely if the terms of service give the provider rights regarding the user's information. Another possibility is that bankruptcy will terminate the cloud provider entirely with little or no notice.

Under any transfer scenario, a user may not have any advance notice of the transfer and therefore no opportunity to remove records before the transfer. For an individual, the transfer of records from one cloud provider to another could result in the conglomeration of personal information that the individual sought to keep separate or away from a particular company. A new owner who is a creditor of a user might seize valuable information or documents (e.g., photographs).

For a business, a transfer could result in result in records suddenly being stored in a state or country that imposes privacy or other obligations on a user or in a location that has other consequences for the legal status of information. The combination of unlimited transfer by a

[31] An example of an onion router is EFF's Tor. <http://www.torproject.org/>. Last accessed Feb. 19, 2009.

cloud provider with the ability of the provider to instantaneously change terms of service could produce a result that is highly unfavorable to a user.

Consider the corporate user that carefully chose a particular cloud provider because the provider did not reserve the right to read user files and had no affiliation with the corporate user's competitors. If the chosen cloud provider was sold to another organization and the terms of services changed under the provider's reservation of the right to change the terms, the corporate user could find its' confidential, internal documents accessible by a competitor.

Transactional, Relationship, and Other Information

Most of the discussion here relates to the consequences for information that a user placed with a cloud provider. Any use of a cloud provider will also generate transactional, relationship, and other information about the user or other third parties. Transactional information may include data about dates, times, locations, equipment, activities, and other characteristics of a user and of any other person who the user allowed to access the user's information.

For example, if a user places a draft document with a cloud provider and allows three colleagues to access the document, the system would have transactional information on the user and the user's colleagues. The same information could also show relationships among the four individuals and their institutional affiliations. In some circumstances, a cloud provider could provide the provenance of a document that might not be readily available from any other source.

In other circumstances, transactional information may reveal substantive activities. For example, if two publicly owned companies considering a merger share documents with each other through a cloud provider, the transactional and relationship information might reveal confidential plans even if the provider does not read the actual documents.

Another concern could arise from what might be called secondary use of information by a cloud provider. Consider, for example, a cloud provider that says that it will not market to a user based on the user's information. A user's information might contain useful data about others, and a cloud provider's seemingly reassuring promise may not be so reassuring after all. It is conceivable that the cloud provider can still market to non-users who show up in the user's records, especially if the non-users can be identified in some way.

If, for example, a cloud provider reads the taglines of a user's photographs and learns that a John Doe (who is not a user of the service) in one of the photos skis, the provider may then use or sell knowledge of John Doe's skiing interest for marketing purposes. If not restricted, secondary use of documents, photographs or other information entrusted by a user to a cloud provider has broad potential to expand the use of information in ways the user did not anticipate.

For transactional information, relationship information, and secondary uses of information, a cloud provider's privacy policy may be more important than its terms of service. A user may have better privacy protections when a cloud provider more strictly adheres to fair information

practices, a set of internationally recognized practices for addressing the privacy of information about individuals.[32]

Subpoenas

Possibilities of compelled disclosure by the government or a private litigant have already been discussed. Companies involved in litigation can use the process of discovery to obtain records of other parties to the litigation in the possession of cloud providers. A cloud provider, like any third party, could promise to notify a user of a subpoena and delay responding to the subpoena to allow the user to intervene.

Privacy policies at some websites promise to provide notice of subpoenas to users when legally permissible to do so, but the practice is far from universal and the promises are often highly qualified. Even if a cloud provider's terms of service make a promise about notice, the promise may be limited or subject to change. Terms of service may waive any liability for failure to notify.

The more activity that a user conducts in the cloud, the greater the risk of third party disclosure is. Consider the user who employs a cloud provider to provide a complete backup for the user's hard disk. The provider would, in essence, maintain a full record of the user's computer activities. Anyone seeking access from the provider might obtain all of the user's records. For example, in a divorce, a lawyer for one party might seek useful information such as documents, videos, photographs, email, and other data from the other party's cloud provider.

Audits and Security

Requirements for auditing of corporate records might make it difficult or impossible for some users to store some information with a cloud provider because of an inability to audit the use of the information.[33] Audits and other data integrity measures may be important if a user's local records differ from the records maintained on the user's behalf by a cloud provider.

Determining which version of a record stored in multiple locations is the correct version may be complex. Security requirements for information may also create problems because of the inability of the user to assess the provider's security, to audit security for compliance, or to determine whether the level of security meets statutory or regulatory security requirements.

[32] For a history of fair information practices, see <http://bobgellman.com/rg-docs/rg-FIPshistory1-6.pdf>. Last accessed February 19, 2009.
[33] See, e.g., Alan Murphy, *Cloud Security: A New Level of Trust*, Virtual Data Center Blog at <http://thevirtualdc.com/?p=134>. Last accessed Feb. 19, 2009.

Possible Cloud Provider Disclosure Obligations

It is possible that cloud providers will have obligations to monitor users in some cases. For example, some jurisdictions in the United States require computer technicians to report evidence of child pornography that they find when repairing or otherwise servicing computers to police or prosecutors. Whether cloud providers have similar obligations is beyond the scope of this analysis, but it is conceivable that cloud providers could be obliged to report about the activities of users. Reporting might also be required for evidence of money laundering, fraud, bribery, child abuse, child abduction, or many other illegal activities. A copyright owner might ask or compel the cloud provider to scan all of a user's files (or, perhaps, all files of all users) seeking to find copyrighted material.

If the government is looking for a fugitive, terrorist, missing child, or other individual, it might ask a cloud provider to search all user photos and data for the individual. The government could also seek to scan available photos for evidence useful in criminal trials. Some governments might be able to ask or compel a provider to scan all photos when entered into the provider's system for information of interest to the government.

To the extent that cloud computing places a diverse collection of user and business information in a single location, it may be tempting for governments to ask or require cloud providers to report on particular types of criminal or offensive behavior or to monitor activities of particular types or categories of users (e.g., convicted sex offenders). The possibility that a cloud provider could be obliged to inform a government or a third party about user activities might be troubling to the provider as well as to its users. Other possibilities include searching for missing children and for music or software copyright violations.

V. Policy Observations

Cloud computing is well underway and appears to be expanding rapidly. There has been a good deal of public discussion of the technical architecture of cloud computing and the business models that could support it. Debate about the legal and policy issues regarding privacy and confidentiality raised by cloud computing has not kept pace. The findings set out at the beginning of this document are a contribution to the debate, as are the following policy observations.

- **Responses to the privacy and confidentiality risks of cloud computing include better policies and practices by cloud providers, more vigilance by users, and changes to laws.**

  If the cloud computing industry adopted better and clearer policies and practices, users would be better able to assess the privacy and confidentiality risks they face. For some

individuals, the actual risks involved with cloud computing may be minor or insignificant. Other individuals might have stronger concerns. For example, some users may be anxious to maintain full ownership of photographs and may not want to grant a cloud provider any rights over their photos. Other users, especially those in corporations or government, might have different and stronger reasons to protect sensitive or valuable information. Those who use cloud computing for some activities and not others may find it hard to keep confidential data from migrating to applications in the cloud.

- **The cloud computing industry could establish standards that would help users to analyze the difference between cloud providers and to assess the risks that users face.**

  The cloud computing industry could be doing a lot more to explain its services. One approach may be to group cloud services into types or categories based on levels of protections. For example, there might be two basic classes of cloud providers. One class of provider would promise never to use or disclose information. It might employ mandatory or optional encryption that prevents the provider from examining content of user information. In addition, the same class of provider might make stronger and more permanent commitments about not making substantive changes in the terms of service that would affect a user's privacy or confidentiality interests. Strong security obligations might also be a part of the package of obligations. Commitments made by "class one" providers could be subject to independent audit and certification. The second class of cloud provider might make no or fewer promises regarding the content of user information and might retain a broader ability to change the terms of service. Of course, there may be a need for additional classes of cloud providers to meet different needs. Helping users find the appropriate level of protection will be important.

- **Users should pay more attention to the consequences of using a cloud provider and, especially, to the provider's terms of service.**

  Standardization of terminology and terms of service would help users to understand the risks and consequences of using a cloud provider. At present, however, the best a user can do is to select a cloud provider carefully based on its terms of service and privacy policy. Reading and understanding the terms of service may be the single most important thing for an individual to do before using a cloud provider. Regrettably, the terms of service are often complex, and may require a high level of interest and persistence to thoroughly parse and understand. An alternative is to avoid cloud providers altogether until better protections for users are available. A business or agency should be fully aware of any privacy or other obligations that attach to data being shared with a cloud provider.

- **For those risks not addressable solely through policies and practices, changes in laws may be needed.**

  For example, Congress could amend ECPA to address the shortcomings in the law and to determine what protections apply to user records. Other legislative responses could

address ambiguities in privacy or other laws. It is possible to speculate about a statute establishing specific standards for cloud providers, including civil and criminal penalties for violations of the standards. States could also enact relevant legislation, although the effect of state law on an interstate or international activity is uncertain. It is also uncertain what the prospects are for a legislative response in the near-term future.

Whether an industry self-regulatory approach would work is uncertain. Other industry self-regulatory efforts focused on privacy have lapsed, failed entirely, or been heavily criticized by consumers as too one-sided in favor of industry. A good faith effort offers the hope of addressing some issues effectively. Neither self-regulation nor legislation is likely to offer a complete response to the privacy and confidentiality issues raised by cloud computing.

These policy suggestions are offered to further the debate about the risks of cloud computing for privacy and confidentiality. Users of cloud providers would benefit from greater transparency about the risks and consequences of cloud computing, from fairer and more standard terms, and from better legal protections. The cloud computing industry would also benefit.

VI. Credits

Report Author:

Robert Gellman, Privacy and Information Policy Consultant, <http://www.bobgellman.com>.

Contributor:

- Pam Dixon, Executive director, World Privacy Forum, read and commented on the report drafts and also edited the document.

Thanks to:

- Lee Tien read and commented on an early report draft and provided comments.
- Anna Slomovic read and commented on an early report draft and provided comments.
- Professor Takato Natsui (Professor, School of Law, Faculty of Law, Meiji University, Japan) raised some of the questions about cloud computing discussed here. This report was written following a discussion panel Professor Natsui chaired that focused on cloud computing. The panel discussion was held at the International Privacy and Security

Conference in Tokyo, Japan in November 2008 (IPSC2008) <http://www.ipsc2008.org/en/index.html>. (The IPSC conference was co-hosted by the World Privacy Forum and the following Japan-based organizations: The Institute of Electronics, Information and Communication Engineers (IEICE), Social Implications of Technology and Information Ethics, the Japan Society of Security Management, and the Information Network Law Association.) Thank you also to the panel members.

For More Information

PDF version of full report is located at:
<http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf >.

For updates to this report and other documents related to the report, see the World Privacy Forum's Cloud Privacy page at:
<http://www.worldprivacyforum.org/cloudprivacy.html>.

For further information contact

World Privacy Forum
www.worldprivacyforum.org
info2009@worldprivacyforum.org
+1 760.436.2489

The World Privacy Forum is a 501 (C) (3) non-profit, tax-exempt organization. Its focus is on public interest research and consumer education relating to privacy topics.

Version history

First public release:
Version 1.1
Released February 23, 2009.