Boston University School of Law

Scholarly Commons at Boston University School of Law

Faculty Scholarship

1-2010

Cloud Computing: Storm Warning for Privacy?

Nicole Ozer

Chris Conley
Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship

 Part of the Computer Law Commons, and the Privacy Law Commons

Recommended Citation

Nicole Ozer & Chris Conley, *Cloud Computing: Storm Warning for Privacy?* (2010).
Available at: https://scholarship.law.bu.edu/faculty_scholarship/3580

This Report is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.

Cloud Computing: Storm Warning for Privacy?

A publication of the ACLU of Northern California
Available online at www.DotRights.org

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

"Cloud computing"—the ability to create, store, and manipulate data through Web-based services—is growing in popularity. Cloud computing itself may not transform society; for most consumers, it is simply an appealing alternative tool for creating and storing the same records and documents that people have created for years. However, outdated laws and varying corporate practices mean that documents created and stored in the cloud may not have the same protections as the same documents stored in a filing cabinet or on a home computer. Can cloud computing services protect the privacy of their consumers? Do they? And what can we do to improve the situation?

Cloud Computing: Storm Warning for Privacy? is the first in a series of issue papers by the ACLU of Northern California that discuss new technology trends and their consequences. This paper examines the current state of legal and technical privacy protections for consumers of cloud computing services and explores opportunities for consumers, businesses, and policymakers to work together to update and enhance these protections.

Part I of this paper provides background information on cloud computing. Part II examines the privacy concerns that arise from the use of cloud computing services and Part III surveys the current state of privacy protections for consumers of these services. Finally, Part IV identifies opportunities for legal, technological, and social mechanisms to be reinforced so that Internet consumers are not forced to lose control of their information when they use cloud computing services.

For more information about cloud computing and other online privacy and emerging technology issues, please visit the ACLU of Northern California's Demand Your dotRights campaign website at **www.dotRights.org**.

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

CONTENTS

AUTHORS: Nicole A. Ozer, Chris Conley

Thank you to Tamar Gubins, David Hari O'Connell, Christopher Soghoian, Aaron Brauer-Rieke, Monique Pham, and the staff of the ACLU Technology and Liberty Project for their assistance with this issue paper.

COVER DESIGN: Gigi Pandian, ACLU of Northern California

For more information about cloud computing and other online privacy issues, please contact the Technology and Civil Liberties Program at the ACLU of Northern California and visit our online privacy Web site at www.dotrights.org.

The ACLU of Northern California wishes to thank the following funders for their support of this publication:

Block v. eBay cy pres fund

California Consumer Protection Foundation

Consumer Privacy Cases cy pres fund

Rose Foundation for Communities and the Environment

The David B. Gold Foundation

Published by the ACLU of Northern California, January 2010

Electronic copy available at: https://ssrn.com/abstract=1611820

Electronic copy available at: https://ssrn.com/abstract=1611820

INTRODUCTION

"Cloud computing" services—tools accessed via the Internet that allow consumers to create, edit, and store documents (such as private photos and videos, calendars and address books, diaries and journals, and budgets and financial spreadsheets) online—are growing in popularity as Internet speeds increase and the cost of data storage drops. Companies are offering a wide range of cloud computing services, ranging from "free" basic applications for the general public to sophisticated and well-supported services designed for corporations and even governments.[1] Many popular offline applications, including Microsoft Office and Adobe Photoshop, now offer cloud computing editions with familiar interfaces. Other tools allow consumers to "drag and drop" files to or from online storage exactly as though the storage site were just another folder or hard drive. Once documents are online, consumers can access and share them from any Internet-enabled device. From the consumer perspective, cloud computing services make the transition from offline to online activities increasingly seamless.

Unfortunately, while consumers can easily carry their information into the cloud, the privacy protections for that personal information may not transition as easily. The Fourth Amendment requires law enforcement officials to obtain a warrant from a judge before entering a person's home and searching her file cabinet or computer hard drive for documents and related information, but courts have yet to definitively determine how these privacy protections apply to cloud computing documents. Furthermore, many existing privacy statutes were written decades ago and may not apply to documents stored with online services like cloud computing that were not anticipated when these laws were drafted. In addition, when documents are stored in a filing cabinet or on a home computer, the owner of the documents often has the opportunity to challenge a demand to hand over those documents—but a cloud computing service may not have the ability or incentive to resist such demands or even to notify the document owner if her documents are demanded by a third party.

As cloud computing becomes increasingly popular and the boundary between personal devices and the Internet "cloud" becomes less meaningful, consumers and companies alike will benefit from protections that ensure that documents created and stored using cloud computing services carry the same rights and protections as documents created or stored elsewhere.[2] These rights and protections will preserve the privacy of consumers, strengthen loyalty and trust in cloud computing services, prevent costly litigation, and encourage the use of beneficial technologies like cloud computing to create, edit, share, and store documents.

Part I of this paper provides background information on cloud computing. Part II examines the privacy concerns that arise from the use of cloud computing services and Part III surveys the current state of privacy protections for consumers of these services. Finally, Part IV identifies opportunities for legal, technological, and social mechanisms to be reinforced so that Internet consumers are not forced to lose control of their information when they use cloud computing services.

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

In several areas of the paper we have more questions than answers. It is our hope that this issue paper will help to support a robust conversation between consumers, businesses, and policymakers to address these important questions about cloud computing and develop plans to address potential gaps in the existing legal framework for protecting privacy and freedom of expression.

Part I: Understanding Cloud Computing

"Cloud computing" is an increasingly popular buzzword, though it has been inconsistently used. Some definitions are so broad that it can be difficult to distinguish cloud computing from general Internet use.[3] For the purposes of this issue paper, we define cloud computing as "outsourcing" computing functions traditionally controlled directly by a consumer—operating and maintaining hardware, installing and running software, storing data—to a third-party service via the Internet.[4] The most common cloud computing services allow Internet consumers to use a Web browser to create a spreadsheet or presentation,[5] store and manipulate photos,[6] store medical records,[7] organize and play multimedia files,[8] back up data,[9] or maintain calendars or address books.[10] Business-oriented cloud computing services allow companies to manage customer relations,[11] store data, or run their own applications on remote computers.[12] (The definition in this paper excludes Web-based email and social networking services that broader definitions might include.)

For example, Google Docs and Microsoft Office Live are online suites of office applications for consumers that are similar to Microsoft's Office suite (Word, Excel, and PowerPoint). Like Microsoft Office, these online suites enable consumers to create and edit documents through a graphical interface. However, rather than installing software on a personal computer and storing the created documents on a hard drive, a Google Docs or Microsoft Office Live consumer accesses the application through her Web browser and saves her documents on a remote server controlled by a third party.

Computer consumers are increasingly taking advantage of cloud computing services. According to a 2008 Pew Internet & American Life Project memorandum (Pew memo),[13] at least 40% of American Internet consumers, and at least 59% of such consumers in the 18-29 age range, have engaged in some form of cloud computing activity (as defined above) by either storing data online or using Web-based software applications.[14] The rise of cloud computing can be ascribed at least in part to efforts by cloud computing providers to make their services as consumer-friendly as possible. Cloud computing consumers enjoy the convenience of accessing their information from any Internet-connected device, the ability to share documents and information with others, and the security of protection from data loss.[15]

For the consumer, the transition from local applications and storage to cloud computing services can be nearly seamless. In effect, the cloud may be seen simply as an extension of a personal computer or device. From technical and legal perspectives, however, moving to cloud computing has significant ramifications. Relocating the storage and processing of a consumer's data and personal information from a consumer's own computer to a third party's servers impacts her ability to retain control over information, potentially exposing far more private details

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

about that consumer's life than she might realize and possibly undermining the privacy protections she expects for her private information.

Part II: Why is Privacy Important for Cloud Computing?

Privacy is both an individual and a social good. As individuals, privacy gives us the autonomy to address sensitive issues without fear of exposure, the ability to explore facets of our personality and individuality, and the power to form close bonds with some by excluding others.[16] Privacy allows a healthy society to experiment and grow, and safeguards the balance between individual liberties and government powers. As such, privacy is a fundamental building block of a robust democracy. But this privacy, autonomy, and control over personal information, so essential to American society, may be at risk as consumers increasingly place private data in the hands of third-party cloud computing services—and consumers are increasingly concerned about this.[17]

Consumers of cloud computing services have a simple message for their service providers: "Let's keep the data between us."

Privacy Risks of Cloud Computing

Cloud computing services may hold a consumer's diaries, business records, photographs, calendars, address books, medical records, and many other sensitive documents – documents that the consumer regards as private. The information contained in such documents can implicate every part of a consumer's life – her family and friends, politics and religion, interests and activities – and requires meaningful safeguards to protect her privacy and freedom of action.

Moreover, cloud computing activity – like any Internet activity – generates additional information that a provider might collect, such as the identity of each consumer who accesses content stored online and the time and place they do so. For example, when a consumer accesses Google Docs, "Google records information such as account activity (e.g., storage usage, number of log-ins, actions taken), data displayed or clicked on (e.g., UI elements, links), and other log information (e.g., browser type, IP address, date and time of access, cookie ID, referrer URL)."[18] Collecting this information raises questions about privacy even when done independently; when linked to other cloud computing activity, it threatens to reveal far more about a consumer than she might imagine. For example, IP addresses and login times could be used to determine when and where a user was—and who else has used that same computer—if she logs into a cloud computing service away from home.

In addition, some cloud computing service providers may "subcontract" parts of the service to additional third parties who then may have some degree of access to private data. For example, some companies like Amazon provide hosting services that allow other companies to use their servers to run web applications and store data[19]—but claim the right to disclose this data under certain circumstances. The Amazon Web Services

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

Agreement states that Amazon may disclose data to "comply with…the request of a governmental or regulatory body, subpoenas or court orders." [20] Language like this demonstrates that it is important that each link in the chain have robust privacy and security safeguards or consumers may find that their personal information is vulnerable. [21]

Cloud computing consumers are "very concerned" by scenarios in which companies:

- **Turn their data over to law enforcement (49% of consumers);**
- **Keep copies of files even after they try to delete them (63%);**
- **Analyze data in the cloud for targeted advertisements (68%);**
- **Use cloud documents in marketing campaigns (80%); and**
- **Sell files to others (90%).[22]**

Consumers Are Worried About Cloud Computing Privacy

Cloud computing consumers are increasingly aware of—and alarmed by—the risks associated with creating and storing their documents in the cloud. Thus, discussions about cloud computing privacy are not merely academic; they reflect the views and concerns of real consumers. Unless these concerns are addressed, privacy fears may limit adoption of cloud computing tools overall.

According to a 2008 survey, cloud computing consumers "show high levels of concern when presented with scenarios in which companies might use their data for purposes consumers may or may not fully understand ahead of time" and "worry over control of the information they store online."[23] The survey summarized the underlying message of cloud consumers to companies as, "Let's keep the data between us."[24]

Consumers are right to be concerned about what goes on in "the cloud." Abstracting away the technical details makes computing easier and more convenient for many, but without transparent sharing policies and meaningful consumer controls, cloud computing could weaken a consumer's ability to maintain control over her own information. Unfortunately, the legal protections that consumers should be able to rely on for information stored with cloud computing services are currently uncertain.

Part III: Legal Privacy Protection and Cloud Computing

The law has long recognized the importance of privacy as both a breathing space for personal autonomy and a necessary constraint on the power of the government.[25] Most privacy law, however, was written or decided decades ago, before the advent of the Internet and other communications technologies. The combination of outdated law and rapidly evolving technology results in inconsistent and uncertain privacy protections. This lack of clear and up-to-date law harms everyone involved: consumers, businesses, and the government.

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

Because privacy law is badly outdated, the legal protections that apply to information stored with or collected by cloud computing services are unsettled. For example, it is unclear whether the Constitution prevents law enforcement access to cloud computing data without a judicially-approved search warrant, or whether and to what extent the current patchwork of statutory privacy laws provide additional privacy protection. For now, consumers, cloud computing providers, and the government alike are acting in a legal domain filled with grey areas.

Ultimately, this lack of legal clarity benefits no one. Consumers are unsure how or whether using cloud computing services affects their privacy and anonymity. Providers are hampered in attracting consumers who worry their privacy won't be properly protected, and are hamstrung by confusion about whether they legally may, must, or must not disclose consumer information in various circumstances. Even law enforcement officials are harmed when this confusion leads providers to resist legitimate requests for information.

There are three basic categories of legal protection for information stored with cloud computing providers: Constitutional protections, statutory protections, and privacy policies. Each of these three is currently unclear or inadequate to protect the interests of consumers and cloud computing providers. Courts, policymakers, and companies all need to use the tools at their disposal to clarify and extend these legal protections to ensure the privacy of information stored with cloud computing providers.

Constitutional Protections: Cloud Computing and the Third Party Doctrine

Privacy is an essential civil liberty protected both by the United States Constitution[26] and several state constitutions, including the California State Constitution.[27] The federal constitutional protection for private records is housed in the Fourth Amendment, which prohibits "unreasonable searches and seizures."[28] The Supreme Court, in a long history of decisions, has extended this protection beyond the home to any location where an individual has a "reasonable expectation of privacy."[29]

Legal decisions have conferred a reasonable expectation of privacy on many of the closest analogues to cloud computing. For example, the Fourth Amendment protects various forms of containers, including:

- Personal containers, such as purses, even if left with another for safekeeping;[30]
- Physical storage facilities such as safety deposit boxes[31] and rented storage lockers;[32]
- Personal computers, in some cases even if the computer is completely under the control of another;[33] and,
- Files on networked computers.[34]

Since cloud computing is really a modern version of a storage locker or personal computer hard drive, it makes sense for cloud computing consumers to expect that their data will have the full protection of the Fourth Amendment and be protected against warrantless searches.

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

However, questions arise about the constitutional protections for online data, including cloud computing records, because of a legal doctrine called the "business record doctrine," also termed the "third party doctrine." The business record doctrine, which was established in a pair of pre-Internet Supreme Court cases, holds that there is no reasonable expectation of privacy, and thus no Fourth Amendment privacy protection and warrant requirement, when a person turns over information to a third party business.[35] In relinquishing exclusive control over the information, the person "assume[s] the risk" that the third party might voluntarily pass on this information, and thus can no longer reasonably consider the information private.[36] Based on this doctrine, law enforcement officials have claimed that records of online activities are not protected by the Fourth Amendment.[37]

The tension between these two approaches to the Fourth Amendment has yet to be resolved, and lawyers and the courts continue to address the issue of constitutional protections for online data. Two courts have held that email messages stored in a Web mail account and text messages stored with a service provider retain full Fourth Amendment protection,[38] suggesting the same protection should apply to cloud computing documents. But the question remains open, particularly where the provider accesses the consumer's content in some manner (such as to provide recommendations, scan files for viruses or check for spelling or grammatical errors, or generate targeted advertising based on the content) rather than solely storing it at the consumer's behest.

Adding further complexity, state constitutional protections may apply even where federal constitutional protections do not. For example, the California Supreme Court has explicitly rejected the third party doctrine as a limitation on the right to privacy in the state constitution.[39] Thus, the privacy protections for a cloud computing user could differ depending on the state where she lives or where her data is stored.

While the legal landscape is unsettled, consumer expectations—the basis of constitutional privacy protections—are not. Internet consumers treat cloud computing services as the modern equivalent of storage lockers, safe deposit boxes, filing cabinets, and (most recently) home computers and personal hard drives. They expect these documents and any associated information to remain private—and strongly express their concerns about scenarios where their data is shared with others, as discussed above. Like papers or other objects residing in these storage facilities, information stored with cloud computing services merits the full protection of the Fourth Amendment and state constitutional privacy provisions.

Statutory Protections: Cloud Computing, ECPA, and Other Laws

Federal and state laws provide additional sources of privacy protection. Such "statutory law" can be particularly important in providing greater certainty in a situation, like cloud computing, where technology has advanced and constitutional protections have not yet been tested. Unfortunately, many of the statutory laws that might apply to cloud computing services were written decades ago, before the Internet even existed, and thus provide questionable protection for cloud computing consumers as well.

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

In particular, the Electronic Communications Privacy Act (ECPA)[40] should—but does not—clearly define the statutory protections applicable to cloud computing services. ECPA is a federal statutory law that provides specific protections for electronic communications (in transit or in storage) to supplement any protections offered by the Fourth Amendment. But ECPA does not clearly state whether documents stored with many cloud computing services are protected at all. ECPA, as currently written, provides protection where content is stored with a service "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[41] It is not clear whether sites that provide collaboration and sharing functions or employ a targeted advertising business model based on information contained in documents are covered by this clause.

Even if ECPA does cover cloud computing records in a specific situation, the protections that it provides are insufficient to properly safeguard the privacy of sensitive documents being stored with cloud computing services. ECPA allows law enforcement officers to either (a) demand content (such as cloud computing documents) from a provider with a subpoena or court order, rather than the search warrant required by the Fourth Amendment, if the target of the search is notified or (b) refuse to notify the consumer at all, and possibly prohibit the service from notifying the consumer, if law enforcement demands content via a search warrant.[42] Government entities can also demand transactional records from cloud computing services – records that may also contain private information – without either obtaining a warrant or notifying the consumer.[43]

Beyond ECPA, there are questions about whether other specific privacy laws or regulations fully protect consumers of cloud computing services. For example, the Health Insurance Portability and Accountability Act (HIPAA)[44] is designed to protect the privacy of health records. However, HIPAA applies to health care providers, health care clearinghouses, and health plans (insurers). Do HIPAA protections apply to cloud computing services that store consumer health records? Similarly, does the Video Privacy Protection Act[45] (VPPA), which provides statutory protection for video rental records and "other similar material," protect records of audiovisual material shared or retrieved through a cloud computing service?[46]

Without comprehensive federal privacy legislation, consumers are left with a patchwork of sector specific privacy law to safeguard their rights. It is now unclear whether even this patchwork of laws adequately covers innovations related to cloud computing. Given the already weak and now increasingly uncertain protections in ECPA and other statutory privacy laws, the time is now to take a thorough look at statutory privacy protections and update privacy law to keep pace with the modern online world.

Privacy Policies

Internet consumers want greater control over their own information. A 2009 study found that 69% of adult Internet consumers want the legal right to know everything that a company knows about them, and 92% want the right to demand that their personal records be deleted.[47] A separate study in 2008 found that many Internet

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

consumers were “very concerned” about the possibility that their personal information could be shared with law enforcement or other third parties without their knowledge or consent.

Unfortunately, while the majority of companies doing business online now have privacy policies, the reality is that most of these policies do little, if anything, to actually protect consumer privacy. Many policies are just paragraph after paragraph of statements reserving broad latitude for the company to collect vast amounts of information about a consumer, keep it for an extended period of time, and use it in any way that the company can imagine. The consumer is given few methods to control her own information and often no assurance that the company will protect information from inappropriate demands for information from third parties. Further steps must be taken to ensure that “privacy policies” are worthy of that name.

Part IV: Reinforcing Privacy Protections for Cloud Computing

As cloud computing continues to develop and expand, it is critical to establish mechanisms—legal, technological, and social—to protect the privacy of consumers. Courts and policymakers need to recognize the realities of modern Internet use and information storage and satisfy the continued expectations of privacy and free speech, regardless of whether the information is created and stored online or offline. Companies should invest in privacy-friendly technologies and practices that put consumers in control of their own private information. They should also support legal reform to update the outdated constitutional and statutory understandings of online privacy. Internet consumers also have a role to play: by using their collective voice, they can demand stronger protections and meaningful control from companies and policymakers. By doing so, these groups can pave the way for use of cloud computing by ensuring that legal, technological, and social mechanisms adequately safeguard privacy and free speech.

Legal Reform: Privacy Laws Don’t Auto Update

Technology has developed at an astounding rate in the past two decades and the law has not kept pace. The law needs to evolve to match today’s new online world and continue to properly safeguard the privacy and free speech rights of individuals.

Constitutional Privacy Protections Should Apply Online as well as Offline.

Cloud computing services, like their real-world analogues, deserve the full protection of the Fourth Amendment and state constitutional privacy protections. The line between cyberspace and the “real world” is rapidly fading, and businesses, policymakers, and the public should reject any attempt to create an artificial distinction between records stored in a locker or

> “Privacy does not end at the doorstep; it also cannot end at the edge of the cloud.”

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

on a personal computer and records stored with a cloud computing provider. Privacy does not end at the doorstep; it also cannot end at the edge of the cloud.[48]

Existing Statutory Privacy Law Needs a Technological Upgrade

Statutory electronic privacy law should be updated to make it clear that a warrant supported by probable cause is required for any law enforcement access to records stored with a cloud computing provider. The definitions in ECPA should also be redrafted to apply to advertising-based business models and add-on online services. Privacy protections should apply to cloud computing services even if a provider is accessing stored content to deliver specific services or targeted advertising.

Lawmakers also need to reevaluate the distinction between "content" and "non-content" information and establish robust standards for secondary information collected by cloud computing providers that reveals sensitive details about Internet users. Information about a user's activities—such as when and from where the user logs in, which documents the user views and for how long, and who the user shares documents with—also contains private information that should be protected by law.

Laws Should Require Notice and Oversight of Demands for Cloud Computing Records

Statutory privacy law should also require that a consumer be notified prior to any disclosure by a provider of any documents or records. In the offline world, such a law was typically unnecessary, as notice to the subject of a search was often unavoidable when third parties demanded documents stored in a file cabinet or on a personal computer. This notice, which gives individuals the ability to defend their own rights, needs to be written into law in the online world where an individual's documents or records could be obtained from a cloud computing provider without the individual ever knowing.

In addition, the law should require that all demands for online information, including cloud computing documents and records, be recorded and compiled so that policymakers and the public are aware of the scope of such requests. It is very difficult for consumers to feel confident about utilizing cloud computing platforms if they are left to worry that their personal information is far more vulnerable in the cloud than it is on their hard drive or in their filing cabinet because they have no basic information about disclosure rates. This lack of notice can lead some consumers to underestimate the implications of using such services, while others might have more fear than necessary.

Current law requires that law enforcement agencies compile and publish statistics about the nature and number of wiretaps orders obtained and used to intercept communications in real time[49] —but there is no such requirement for the also-invasive practice of obtaining access to online information via search warrants, subpoenas, and other means. Few companies will provide any data about how often personal information is requested and disclosed to third parties. For example, Google, which operates both Google Docs and Picasa photo services, has continually refused to state the number of requests it receives for consumer information or its number of

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

disclosures. This problem is systemic.[50] No company currently provides consumers with statistics about disclosure rates to third parties.

To ensure that consumers have the information that they need to trust that their information is safe, there should be a mechanism in place to require all online companies to keep a record of all information requests and to submit an annual report to a federal agency such as the Federal Trade Commission. An annual report should detail:

- The number of Federal warrants, State warrants, grand jury subpoenas, civil and administrative subpoenas, and court orders received in the previous year;
- The number and types of action taken by the company for each category of request;
- The number of individuals whose personal information was disclosed by the provider by category of request;
- The type of personal information disclosed by category of request; and
- The total amount of money received by the company to fulfill each category of request.

The agency should then make all reports accessible to the public in an online, searchable format within a reasonable time after filing. Any company with an online privacy policy should also create a prominent hyperlink from the disclosure section of its privacy policy to its latest report.

As cloud computing continues to develop and expand and the boundary between personal devices and the Internet "cloud" becomes less meaningful, it is imperative that privacy laws and policies are updated so that consumers have the transparency they need to make informed choices and feel confident that their personal information is being protected.

Business Practices: Companies Can Lead the Way

Businesses have an important role to play in helping to safeguard the privacy of their consumers. Right now, consumers are very concerned about their information being used in ways that they did not intend.[51] This concern is not good for the public or for business. Businesses have the most to gain from a public that trusts cloud computing because more people will use the technology if they trust that their personal information will remain private.[52] Through robust privacy practices and support for necessary upgrades to privacy laws and technical development, businesses can help ease the transition and give consumers confidence that their information will be safe if they use a cloud computing service.

Services Should Establish and Follow Robust Privacy Practices

Businesses have the opportunity to proactively address much of this consumer concern by establishing and following robust privacy practices. A "privacy policy" that does little to protect privacy is not adequate. Companies should re-dedicate themselves to following the core principles of the Fair Information Practices: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.[53] This means providing meaningful notice about how information is used and to whom it is

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

disclosed, collecting and retaining only the information that is needed to provide services, giving consumers real choice about how any personal information collected about them will be used, properly safeguarding consumer information from disclosure and misuse, and enabling consumers to control, modify, and delete their own records and accounts.[54] Providing consumers with meaningful control and protection for their personal information will help give consumers the confidence to utilize cloud computing and may also help companies avoid negative press, government investigations, and costly lawsuits.[55]

Providers should protect their consumers' information with all available technical tools

Consumers expect that data stored with a cloud service provider will remain private; providers have a business incentive to ensure that it does. By designing a service with technical measures to protect consumers—tools that allow consumers to manage and protect their own information, encryption and anonymity protocols to protect information by default, and access controls and data security measures to prevent breaches and inappropriate disclosures—cloud computing providers can establish a platform where consumers are in a position to control their own information and can feel more confident storing private content.

The first step in giving consumers control is to build a robust and usable interface to allow consumers to manage their own content and records. Consumers should be able to view and control their entire record—not merely the documents that they upload, but any additional records that the service may retain about consumer action or the actions of others with whom the consumer has shared documents. Building such an interface is much easier if it is part of the design process of the service and not tacked on as an afterthought or in response to consumer demands for greater control and transparency.

Anonymization and encryption can also protect consumers by reducing the risk of disclosure of information that is captured and stored by the service. Anonymization procedures need to go beyond removing obvious markers, however, and ensure that data is irreversibly de-identified—which, again, requires forethought to ensure that "anonymization" procedures are not wholly inadequate.[56]

Finally, creating a solid data security plan protects both customers and providers. Data breaches can be disastrous, leading to lawsuits, fines, and lost trust.[57] To avoid these outcomes, providers should use access controls to prevent unauthorized access to content by both employees and third parties and take additional steps such as promptly deleting data that is no longer necessary in order to reduce the risk of breach. Such practices will help safeguard both customer privacy and the provider's bottom line.

> "The more 'locks' a provider puts in the consumer's control, the less likely it is that third parties will be asking providers for the keys."

Providing technical measures that protect and secure consumer information may carry both practical and legal significance. Practically, the measures suggested above – and others that may emerge – reduce the likelihood of breach or unnecessary disclosure. In addition, these mechanisms may strengthen the legal positions of both

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

consumers and providers by making it clear that the consumer, and not the provider, is the party with access to and control over any stored content. The more “locks” a provider puts in the consumer’s control, the less likely it is that third parties will be asking providers for the keys.[58]

Consumer Action: Demand Your dotRights!

If privacy laws and practices are to be brought into the modern era, consumers must provide the political and commercial will to make it happen. As a united force, Internet consumers have the political power to force policymakers to update privacy laws and regulations and the financial power to force companies to build privacy and free speech protection into product design and business models. Consumers are currently paying a very high price for many online services—control of their personal information. It is time to demand that protections for privacy and free speech be part of the foundation for cloud computing services, not an afterthought.

CONCLUSION

Moving from filing cabinets and personal computers to cloud computing appears to offer many advantages. But outdated privacy laws, inadequate privacy policies, and lack of technological tools allowing for consumers to control their own information signal stormy skies for privacy. The time is now for policymakers, businesses, and consumers to work together to safeguard privacy and help cloud computing reach its full potential. For more information about cloud computing, please visit the ACLU of Northern California’s online privacy Web site at www.dotRights.org.

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

ENDNOTES

[1] *See* Thomas Claburn, *Google's 'Gov Cloud' Wins $7.2 Million Los Angeles Contract*, INFO. WEEK, Oct. 28, 2009, http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=221100129.

[2] PEW INTERNET & AMERICAN LIFE PROJECT, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES [hereinafter PEW MEMO], Sep. 2008, *available at* http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx?r=1.

[3] *See id.* ("For everyday consumers of the internet and computers, cloud computing is any online activity, such as accessing data or using a software program, which can be done from different devices regardless of the on-ramp to the internet.").

[4] *Cf.* Jeff Dorsch, *What Is Cloud Computing?*, BIZMOLOGY, http://www.bizmology.com/2008/10/17/what-is-cloud-computing/ ("The simple definition is that it involves using Web-based computing tools and storing information on remote servers maintained and operated by another company.").

[5] *E.g.*, Google Docs, http://docs.google.com/; SlideShare, http://slideshare.com.

[6] *E.g.*, Flickr, http://flickr.com/; Snapfish, http://snapfish.com/; Adobe Photoshop Express, http://www.photoshop.com/.

[7] *E.g.*, Microsoft HealthVault, http://healthvault.com/; Google Health, http://google.com/health/.

[8] *E.g.*, Lala.com, http://lala.com.

[9] *E.g.*, Mozy, http://mozy.com/.

[10] *E.g.*, Yahoo! Calendar, http://calendar.yahoo.com/; Plaxo, http://plaxo.com/.

[11] *E.g.*, SalesForce.com, http://salesforce.com/.

[12] *E.g.*, Amazon Elastic Computing Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[13] *See* PEW MEMO, *supra* note 2, at 5.

[14] *Id*. This study found that 40% of consumers used multiple cloud computing services under their definition, which includes Web-based email, and thus used at least one cloud computing service under ours. More specifically, the study found that 34% of Internet consumers store personal photos online, 29% use online applications, 7% store personal videos, 5% pay for file storage, and 5% use online hard drive backup services. *Id.* at 1. Among consumers in the 18–29 age range, 50% store personal photos. 39% use online applications, 14% store personal videos, 9% pay to store computer files, and 7% back up hard drives to an online site. *Id*. at 5.

[15] *Id.* Other factors cited include ability to access information on any Internet-connected device, ability to share information with others, and protection from data loss.

[16] One scholar notes that once people know they are being "observed and recorded, their habits change; they change." 150 years ago sociologist Jeremy Bentham theorized that prisoners would self-censor their behavior if they believed they were under surveillance but did not know exactly when and where they were observed. According to Bentham, under such a system the "only logical option was to conform." 4 JEREMY BENTHAM, *Plan for a Penitentiary Inspection-House*, *in* THE WORKS OF JEREMY BENTHAM 37 (John Bowring ed., 1962) (1843).

[17] 59% of adults in a 2008 study had refused to provide information to a business or company because they thought it was not necessary. 68% of consumers in 2000 were "not at all comfortable" with companies that create profiles that link browsing and shopping habits to identity, with 82% "not at all comfortable" when profiles include income, driver's license numbers, credit data, or medical status. PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at* http://dotrights.org/business/primer/node/2. A 2009 study found that 92% of adult Internet consumers want the legal right to

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

demand that their personal records be deleted. Joseph Turow, et al., *Americans Reject Tailored Advertising*, 4 (2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[18] Google Docs Privacy Policy, http://google.com/google-d-s/privacy.html (last visited Nov. 12, 2009).

[19] See Amazon Web Services, http://aws.amazon.com/.

[20] *See* Amazon Web Services Customer Agreement, Jan. 20, 2010. http://aws.amazon.com/agreement/ (last visited Jan. 22, 2010).

[21] *See* Matthew D. Sarrel, *The Darker Side of Cloud Computing*, PC MAG., Sep. 25, 2008, http://www.pcmag.com/article2/0,2817,2330921,00.asp:

> And worse, there are clouds within the cloud—your provider may subcontract with another provider for data storage, and that provider might also subcontract for data storage management. Your provider may not even be able to tell you where your data is, or even which country it is in and whether the laws that apply to you regarding data security and breach disclosure even apply in that twice-removed jurisdiction.

[22] *See* PEW MEMO, *supra* note 2, at 4, 10.

[23] *Id. at 10.*

[24] *Id.*

[25] The modern legal understanding of privacy evolved in large part from Justice Brandeis's lengthy dissent in *Olmstead v. United States*. 277 U.S. 438 (1928) (Brandeis, J., dissenting). According to Brandeis:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Id. at 478.

[26] *Cf. id.*

[27] CAL. CONST, Art. 1 § 1.

[28] U.S. CONST. amend. IV.

[29] *See* Katz v. United States, 389 U.S. 347, 361 (1967).

[30] In *United States v. Most*, this was extended to a plastic bag accidentally left with a grocery clerk, although other courts may not extend protection that far. 876 F.2d 191 (D.C. Cir. 1989). In addition, while a jointly used container may allow other consumers to consent to a search, *see* United States v. Matlock, 415 U.S. 164 (1974) (right to consent derives from common authority over premises or property), a private storage container does not lose Fourth Amendment protection simply because it is located in a common area. *See* United States v. Block, 590 F.2d 535 (4th Cir. 1978) (locked footlocker in common area retains Fourth Amendment protection).

[31] *Cf.* United States v. Spilotro, 800 F.2d 959 (9th Cir. 1985) ("[T]here is no question that defendant … has standing to challenge the search of his … safe deposit box.").

[32] *See* United States v. Karo, 468 U.S. 705, 721 n.6 (1984).

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

[33] *E.g.*, United States v. Barth, 26 F.Supp.2d 929 (W.D. Tex. 1998).

[34] Fourth Amendment protection granted unless there is a clear policy of monitoring network use. *See* United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007); United States v. Simons, 206 F.3d 392 (4th Cir. 2000).

[35] *See* United States v. Miller, 425 U.S. 435 (1976) (banking records are not protected by the Fourth Amendment); Smith v. Maryland, 442 U.S. 735 (1979) (records of dialed phone numbers are not protected by the Fourth Amendment).

[36] *Smith,* 442 U.S. at 744.

[37] *See, e.g.*, US DOJ Computer Crime and Intellectual Property Section, SEARCHING & SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, 1.B, Sept. 2009, *available at* http://www.cybercrime.gov/ssmanual/01ssma.html.

[38] Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008) (Web email); Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008), *cert. granted sub nom.* City of Ontario v. Quon, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332) (text messages).

[39] People v. Chapman, 36 Cal. 3d 98, 106-7 (1984) (affirming a right to privacy in unlisted telephone directory information even though the information was "shared" with the third-party telephone company); People v. Blair, 25 Cal. 3d 640, 651-555 (1979) (finding a reasonable expectation of privacy in hotel phone records and credit card charge records); Burrows v. Superior Court, 13 Cal. 3d 238, 244-45 (1974) (finding a privacy right in bank records).

[40] 18 U.S.C. §§ 2701–12 (2008).

[41] *Id.* §§ 2702(a)(2)(B), 2703(b)(2)(B).

[42] 18 U.S.C. § 2703(b), (e) (2008). Under certain circumstances, law enforcement agents can defer the required notice if they demand information with a subpoena or court order rather than a warrant. *See id.* §§ 2703(b)(1)(B), 2705.

[43] *Id.*§ 2703(c).

[44] 45 C.F.R. §§ 160–64.

[45] 18 U.S.C. § 2710 (2008).

[46] *Compare* Kurt Opsahl, *Court Ruling Will Expose Viewing Habits of YouTube Consumers*, July 2, 2008, http://www.eff.org/deeplinks/2008/07/court-ruling-will-expose-viewing-habits-youtube-us (arguing that the VPPA encompasses records of YouTube consumers) *with* e-consultancy, *YouTube Consumers Learn the Hard Way that Online Privacy Doesn't Exist*, July 7, 2008, http://www.e-consultancy.com/news-blog/365921/youtube-consumers-learn-the-hard-way-that-online-privacy-doesn-t-exist.html (arguing that the VPPA likely does not apply to records of YouTube consumers).

[47] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[48] As Judge Martin put it in his *Warshak* dissent, "If I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless." Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (Martin, J., dissenting).

[49] 18 U.S.C. § 2519 (2008).

[50] Few companies have even provided partial information about disclosure. Verizon only recently admitted that it receives "tens of thousands of requests" annually from law enforcement. David Kravets, *Google Talks Transparency, But Hides Surveillance Stats*, WIRED, Dec. 17, 2009, http://www.wired.com/threatlevel/2009/12/google-talks-out-its-portal/. Facebook has admitted it receives up to 20 law enforcement requests per day but has not provided consumers with any information about

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

disclosures to third parties in the civil context. Nick Summers, *Facebook's 'Porn Cops' Are Key to Its Growth*, NEWSWEEK , May 18, 2009, *available at* http://www.newsweek.com/id/195621.

[51] *See* PEW MEMO, *supra* note 2, at 11.

[52] *See generally Privacy Practices*, PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at*, http://dotrights.org/business/primer/; *see also* Yvonne Jones, *Editorial Correspondence*, WIRED, Sept. 2009, at 20 ("Facebook's changes to its privacy settings killed my affection for the company . . . it's revoking one of the things I valued most about it and in the process ensuring that I trust it less.").

[53] Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Jan. 18, 2010).

[54] *See* Joseph Turow, et al., *Americans Reject Tailored Advertising* (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[55] *See* PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at* http://dotrights.org/business/primer/.

[56] *See, e.g.*, AOL, PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at*, http://dotrights.org/business/primer/node/37 (describing a 2006 incident in which AOL made public "anonymized" search results which were not, in fact, properly anonymized, accidentally releasing identifiable search records of hundreds of thousands of consumers) *and* Arvin Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *available at* http://www.cs.utexas.edu/~shmat/shmat_netflix-prelim.pdf (describing how the researchers' "de-anonymized" anonymized Netflix-consumer movie reviews that had been released by Netflix).

[57] *See generally* PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at* http://dotrights.org/business/primer/.

[58] *See* Peter Wayner, *You Know About Backups. Now, Do It Online*, N.Y. TIMES, Oct. 22, 2008, *available at* http://www.nytimes.com/2008/10/23/technology/personaltech/23basics1.html ("Intronis, for instance, has never received a subpoena for stored data and couldn't provide the information even if it did. 'We don't consider ourselves as having access to customer's data. It's not even a thought,' said Mr. Webster.").

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820

A Publication of the ACLU of Northern California

January 2010

www.dotrights.org
www.aclunc.org/tech

Electronic copy available at: https://ssrn.com/abstract=1611820
Electronic copy available at: https://ssrn.com/abstract=1611820