Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing

November 30, 2010

Consumer Protection in Cloud Computing Services

Consumer Protection in Cloud Computing Services

Introduction

Consumers, businesses and government agencies increasingly are storing data and using services "in the cloud." This has profound implications for consumer protection. Consumers are entrusting family photos, documents, and personal information to others, in an environment where expectations, best practices, and even the law are unclear. Businesses may outsource processes to the cloud without fully contemplating the implications for their customers' privacy. The growing use of the cloud creates new challenges for consumer protection and privacy, but it also intensifies problems that have long existed.

The Pew Internet and American Life Project identified a range of consumer benefits from cloud services. Consumers have already widely adopted cloud services, but they are not always aware of what a cloud-based service actually is, or the wider implications of storing data in the cloud. For instance, storing information in the cloud creates rich transactional data that may be monitored by service providers or law enforcement. When cloud services are identified to them, consumers say that they use these services because they are convenient, because they can access data from whatever computer they are using, because they are less likely to lose data in the event of a computer failure, and because cloud services make it easier to share data.[1]

Consumers can benefit in other ways as well. For example, cloud services can free consumers from the tedious task of setting-up or maintaining IT resources – allowing them to focus solely on whatever task the IT platform enables them to accomplish. The cloud is likely to have a democratizing effect on security, giving access to new features too complex for many users to deploy themselves. New efficiencies inherent in the cloud model will allow businesses to start small and quickly provision

[1] John Horrigan, *Use of Cloud Computing Applications and Services*, Pew Research Center's Internet & American Life Project, http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx

more resources as needed, resulting in savings and fewer service outages.[2] Government agencies may also be able to save taxpayer money by using cloud computing services.

Cloud computing itself is difficult to define, but it would be unwise to allow that difficulty to impede efforts to address consumer protection and privacy problems.

Many of the challenges cloud computing creates or intensifies center around control over information. Practically speaking, the cloud's popularity means that more and more information is vested among an array of companies that might not even be known by or have a direct relationship with the consumer. For instance, consumers may sign-up for a web service that lets them easily share photos with friends (direct relationship) – but the photo sharing service, in turn, may employ a cloud service to provide flexible storage capacity (indirect relationship). These providers must have processes and practices in place to ensure data integrity, availability, and security.

Transferring control of data can result in lower legal barriers against law enforcement and civil litigant access to information. This is especially true in the United States, where the Fourth Amendment to the Constitution protects data on devices in possession of an individual but where such protections are generally lessened if data are transferred to a third-party.

There is also the matter of the cloud provider itself gaining access to stored data. Consumers may perceive cloud services like a storage locker: information is placed online in a vault and only the consumer has the authority and ability to "look" at it. That may be true for some cloud models. But in others, the cloud provider may be opening the locker to view its contents, and even monitoring transactional data to see how those contents are used. Sometimes service providers need to access data to facilitate a customer request or ensure that the service is functioning properly (technical

---

[2] Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing, Electrical Engineering and Computer Sciences*, UC Berkeley, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf; World Economic Forum, *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, 2010, available at http://www.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf

justification). In other instances, service providers may scan hosted data for a secondary use that helps funds the provision of the service (business justification). In fact, the provider's business model may depend upon analysis and decision making based upon consumer data.

Unresolved, concerns about cloud computing are likely to prevent widespread adoption of valuable and efficient services. Providers may also face stringent regulatory interventions because of the opaque nature of data security measures and lack of clarity on the actual location of cloud data. These issues led a German Data Protection Authority to conclude recently that cloud providers must locate their services within the European Union, and that personal data should not be placed in cloud services.[3]

Summary of Recommended Best Practices

This report makes recommendations for best practices for business-to-consumer cloud computing services. Our goal is that these best practices will diffuse deeply into the business community, so that companies considering the outsourcing of customer data to the cloud will also consider them in their decision making:

- **Law Enforcement Access to Data.** Where not prohibited by law, users should receive notice of criminal and civil requests for information.
- **Secondary Uses.** Secondary use must be clearly disclosed and identified as "technical justifications" or "business justifications" for use of data.
- **Portability and Interoperability.** Portability is key for competition in cloud services; cloud service operators should not interfere with interoperability.
- **Data Security.** Cloud service providers must demonstrate operational safeguards and security mechanisms through expert audit and certification.

[3] Andrea Schuessler, *EU Data Protection: German State DPA: Non-EU Clouds Off Limits, Personal Data Should Never Be Sent to Cloud*, 9 BNA Privacy & Security Law Report 950, Jun. 28, 2010, citing Cloud Computing and Data Protection, at https://www.datenschutzzentrum.de/cloud-computing/

- **"Free" Services.** "Free" services should have the same consumer protection standards as for-fee services.
- **Deletion.** Consumers should be able to delete information they upload to the cloud.
- **Transparency.** Basic information such as such as the level of service provided, the business model of the cloud service provider, what legal protections apply to data, and who to contact if questions arise should be provided. The report includes a model disclosure for this information.

These recommendations emerged from a two-day retreat convened by the nonprofit organization Consumer Federation of America focusing on cloud computing challenges.[4] The participants in the retreat included persons from consumer and privacy organizations, academia, government, and business, from both the US and Europe. While a few of the participants chose not be included in the list that appears in Appendix C because of legal or other constraints, all were fully engaged in the process and contributed to the outcome. Regarding those who are listed, their listing is not an individual or organizational endorsement of every statement made in the report. The recommended best practices, however, represent the consensus view of the participants on those issues. As noted above, there was consensus that secondary uses should be clearly disclosed, but there was disagreement over whether secondary uses should be left to contract, limited where the consumer is not likely to understand the use, or flatly prohibited.

Background

Cloud computing is difficult to define.[5] A recent report by the World Privacy Forum describes it as involving "the sharing and storage by users of their own

[4] This retreat took place at New York University School of Law in New York City on June 20-22, 2010. The reporter for the group and author of this report was Chris Hoofnagle, Senior Fellow at the Berkeley Center for Law & Technology.

[5] The National Institute of Standards and Technology defines it as, "…a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This is NIST's 15th version of this definition.

information on remote servers owned or operated by others and accessed through the Internet or other connections."[6] Popular cloud-based consumer services include webmail (such as Gmail and Hotmail), photo sharing sites (such as Flickr), and even social networking sites (such as Facebook and MySpace).

Consumer protection and privacy concerns in cloud computing largely focus upon control over information. That is, the lack of physical control over data entrusted to cloud providers creates potential legal and technical challenges. Retreat participants focused on vesting control of data to another as an organizing principle for these best practices.

Cloud providers themselves are careful to define services as fitting into several categories: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). However, it is unclear whether these distinctions hold in practice (some companies offer packages constituting several or all of these services) or whether consumers honor these distinctions (consider the Gmail user employing the email service to store large files instead of or in addition to communicating with others). Reducing uncertainty in the cloud space may require principles to cover all of these platforms despite their differences.

Both consumer groups[7] and technology leaders[8] have called for legal reform to increase the privacy and security guarantees in cloud computing. A thumbnail sketch of the legal landscape elucidates the underlying need for this reform.

U.S. federal privacy law, which has not been updated substantively since 1986, leads to uneven protections for data in the cloud. Data stored on the user's hard drive is subject to the full protections of the Fourth Amendment, meaning that in most circumstances, the government would need to convince a judge to grant permission to access the data. However, once data are transferred to the cloud, Fourth Amendment

---

[6] World Privacy Forum, *Cloud Computing and Privacy*, n.d., available at http://www.worldprivacyforum.org/cloudprivacy.html

[7] Alan Weissberger, *ACLU Northern CA: Cloud Computing – Storm Warnings for Privacy?*, the Viodi View, http://viodi.com/2009/02/13/aclu-northern-ca-cloud-computing-storm-warning-for-privacy/

[8] Microsoft, *Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing*, 2010, www.microsoft.com/presspass/presskits/cloudpolicy/default.aspx

protections may no longer have effect. Under the "third party doctrine," data knowingly and voluntarily transferred to a third party (such as a cloud service provider) may lose its Fourth Amendment shield. In place of the Fourth Amendment, an outdated and weaker framework of statutory protections takes over. Under this framework, cloud data protections depend upon context.

Robert Gellman summarized the cloud legal landscape in 2009: "Distinctions recognized by ECPA [Electronic Communications Privacy Act of 1986] 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."[9]

These distinctions have created increasing uncertainty for both consumer and business users of cloud-provided services. Business models that have evolved since 1986 mix storage and communications services, and many sites enable users to communicate as an incidental offering to some other service. Gellman continues: "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."[10]

While a consumer-business coalition has organized to reform and update ECPA,[11] legislative change moves more slowly than the spread of new services. In the

[9] Bob Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 2009, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf
[10] *Id*
[11] The Digital Due Process Coalition, available at http://www.digitaldueprocess.org

absence of such reform, more certainty is needed to address these barriers to cloud adoption.

Even if new laws are enacted to address cloud computing, it is important to recognize that the US privacy framework is sectoral, meaning that certain industries may not be regulated under a specific privacy law. Thus, the sectoral approach leaves gaps where protections are uneven. Privacy advocates and industry groups alike have called for more comprehensive protections for consumers.

Consumer Protection Challenges

There are a myriad of consumer privacy concerns in cloud computing services. Participants at the two-day workshop identified a range of concerns that could fit into nine categories.

Consumer Concerns about Data Use

A 2008 Pew Internet & American Life Project report[12] elucidated consumers' biggest concerns about cloud services. Ninety percent of respondents surveyed stated that they would be "very concerned" if cloud providers "sold your files to others." Eighty percent would be very concerned if the service "used your photos and other information in marketing campaigns." Sixty-eight percent would be very concerned if information stored in the cloud were used to tailor ads. Sixty-three percent would be very concerned if the cloud provider kept files after the consumer attempted to delete them.

Law Enforcement Access

Law enforcement access looms large for consumers as a concern as well. Forty-nine percent of those surveyed for the Pew report said they would be very concerned if cloud providers "gave law enforcement agencies your files when asked to do so." Some may say, "If you have nothing to hide, you have nothing to fear." But in the cloud

[12] John Horrigan, *Use of Cloud Computing Applications and Services*, Pew Research Center's Internet & American Life Project, http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx

context, especially in "public clouds," transgressive behavior of one consumer can affect others. For instance, if one user employs a shared (or "public") cloud service to commit a crime, investigators may seize computers or backups that contain the data of the guilty and innocent alike on that shared service. Providers may also be pressured to scan their systems for copyright enforcement or illegal content.

Consumers may not even realize that their data has been moved to the cloud, especially when using new devices such as smartphones. It seems arbitrary for Fourth Amendment protections to hinge upon technical design and service questions that are increasingly complex and not in control of the user.

Lock-in

Other, more subtle challenges exist. For instance, consumers may not understand the lock-in risk until they decide to leave a provider. A consumer might spend many years uploading volumes of information, or otherwise customizing the service. These actions could cause a consumer to be effectively locked to a particular service or provider, threatening competition.

Providers could use proprietary formats or employ subtle technical obstacles to exporting this data in order to capture customers. These could be as simple as requiring consumers wishing to export their data to select each file individually for download. Requiring the consumer to click through page after page of files to accomplish a simple export task could effectively make the service non-portable.

Data Security

Consumers are right to expect that data entrusted to the cloud will be stored securely, meaning that the data will be protected from unauthorized access, be maintained with integrity, and backed up in case of loss. However, in their survey of 31 terms of service contracts for cloud providers, Simon Bradshaw, Christopher Millard, and Ian Walden observed:

> *A natural concern for Cloud computing customers is that data placed into the provider's Cloud be secure against loss, be it loss of integrity or availability (resulting, for example, from corruption or deletion) or loss of confidentiality (due perhaps to a security breach*

> *or an unauthorised disclosure). Our survey found however that most providers not only avoided giving undertakings in respect of data integrity but actually disclaimed liability for it.*[13]

They continue:

> *…In effect, a number of providers of consumer-oriented Cloud services appear to disclaim the specific fitness of their services for the purpose(s) for which many customers will have specifically signed up to use them. Some providers…state that data integrity will only be guaranteed where the customer has paid for additional specific backup services.*

Since many providers will not create legal assurances for data security and integrity, the consumer must simply trust the service provider.

In the cloud, consumer control of data can be diminished depending on the deployment and service model at issue, and consumers may lack effective mechanisms to determine whether security protections comply with established criteria. Insider threats are more severe, since a single corrupt employee of a cloud provider may be able to access many different accounts and obscure logs of such access.

Further, even if security criteria are disclosed, consumers may not understand what they mean or whether they are adequate, making comparisons impossible. Only a small number of cloud computing users may have the clout, technical capability, and resources to thoroughly evaluate a service provider's security protections. These concerns over security, and the diminished ability of consumer to verify security in the cloud, are key challenges for the adoption of cloud computing.

Security breach notification laws attempt to bridge the gap of consumer awareness of security issues by informing individuals when an unauthorized party obtains certain sensitive information. Such laws create a performance-based security standard that can help consumers and regulators understand whether a company's security implementation is reasonable. However, it is unclear how this approach will work in the cloud, because the scope of security breach notification laws and their

---

[13] Simon Bradshaw, Christopher Millard and Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper No. 63/2010, available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

implementation may lead providers to fail to notify users after a breach. For instance, data may be stored in a jurisdiction not subject to security breach notification, or cloud services may be exempted from breach notification.[14] Cloud providers may argue that their services are "data agnostic," meaning that the provider does not know specifically what kind of information is stored in an account. According to this reasoning, the cloud provider would not have to issue breach notifications, because it does not know that it possesses sensitive information. This is a dubious argument. It is certainly foreseeable that users will upload personally identifiable information into cloud services, especially when using backup products that mirror the user's entire hard drive.

Moreover the key issue here is whether the cloud provider knows that there was a breach of security. When breaches occur, the best course of action is to enable users to make their own judgments and take appropriate steps if necessary.

Secondary Uses of User Data

Recall the Pew Internet study finding great concern over marketing uses of data. This is an example of a "secondary use," the employment of user data for purposes not related to the technical operation of the service. Cloud providers may employ secondary uses of consumer data or transactional information without consumers realizing that those uses are taking place or whether those secondary uses have legal implications. For instance, the scanning of email content in Gmail is a secondary use of communications data. Using email message content to target advertising could erode consumers' legal rights by diluting their expectations of privacy in the communications.

Fairness in Terms of Service

Terms of service represent another challenge in the cloud. Courts have given legitimacy to one-sided agreements that reflect no bargaining or even the opportunity to bargain. Bradshaw et al. found that many contracts for cloud services were silent on key terms.[15] Worse yet, providers often reserve the right to change terms at will.[16]

[14] See e.g. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (and 2009 telecommunications regulations).
[15] See fn. 13 supra.

Important terms can be buried in long user agreements. There is a need for consensus around what terms are important to consumers about a cloud service, and for a prominent disclosure of those important terms, in plain language. This is an area that may benefit from standardization,[17] and the model disclosure in Appendix B attempts to present key terms (that are often not disclosed at all) to consumers in a short notice.

Massive Storage and Massive Failure

Of course, terms change radically when a business fails. One benefit of cloud computing—massive storage—has a potential downside: the problem of massive failure. Thought must go into the possibility that cloud providers will fail well in advance of an adverse event, which might be simply bankruptcy or a natural disaster that affects the provider's infrastructure. Obviously systems have to be backed up, but also, there have to be provisions and sufficient time for consumers to export their data when a cloud provider ends operations.

Jurisdiction

Rules of consumer protection and law enforcement access vary from jurisdiction to jurisdiction. This is a particularly challenging problem with respect to cloud services, because the most efficient design is one that allows data to flow from region to region, or exist in several different regions, without regard to local rules or the lack of them.

On the other hand, jurisdiction may offer opportunities for greater privacy or consumer protection. For instance, one Canadian-based cloud services provider now advertises a service that is based only in Canada, thus reducing the risk that user data

---

[16] EPIC, Cloud Computing, available at http://epic.org/privacy/cloudcomputing/

[17] For example in the UK the importance of improving quality of information under terms and conditions has been recognized by the Financial Services Authority that recently introduced the summary box model in delivering information on financial services to consumers, see Financial Services Authority, Banking Conduct Regulation, Jun. 29, 2010, available at http://www.fsa.gov.uk/Pages/consumerinformation/product_news/banking/banking_conduct_regulation/index.shtml

will be obtained by other governments.[18] Risk is reduced in this approach because users are exposed to the legal framework of only one government, in this case, a government with a strong privacy protection framework established in law.

Just as there are benefits in allowing the business models to develop, thrive or decline in economic models, it is also important to allow legislatures to develop new approaches to address consumer protection as new technologies, policies or business practices emerge.

The Role of Transparency

Transparency is a bedrock approach for consumer protection challenges. It obviously will play a role in assuring consumer and business users of the cloud. However, transparency has to be done well in order to work.

Relevant information must be provided, at the relevant time. Key terms that materially affect the legal and technical status of cloud data must be policed. For instance, a "private cloud" in industry parlance represents a service dedicated to a single entity, rather than multiple users. This has obvious legal and technical implications. But imagine the confusion that could be caused by a provider that decided to call its business "PrivateCloud" without provisioning dedicated service. Thus, this and other key terms in cloud computing must be policed and used only where appropriate, in order to ensure a fair marketplace.

To address the challenge of transparency, we propose best practices in cloud services disclosure for business-to-consumer (B2C) cloud services. We hope that these simple statements will help consumers focus on key legal and technical issues, and prevent providers from obfuscating practices. From a provider perspective, this standardized statement can provide competitive advantage—it will enable comparative analysis, and be especially useful for companies innovating in the privacy and security realms, where it is difficult for consumers to compare service offerings.

[18] CentriLogic, CentriLogic Launches First Canadian-Based Distributed Cloud Computing Service, Apr. 7, 2010, http://www.centrilogic.com/announcements/newsitem.php?news=19

Despite all of these challenges, an opportunity exists to manage these risks. These challenges are shared by both average consumers and businesses. It is clear that adoption of cloud services will suffer if uncertainty persists on the issues identified above. Consumer protection in the cloud context clearly is good for both consumers *and* businesses.

Consensus Best Practices for Cloud Computing Services

Participants in the retreat organized by Consumer Federation of America discussed challenges and opportunities for consumers in the cloud computing arena. A consensus developed around the following high-level principles to promote consumer protection, security, and privacy in cloud services. These recommendations go beyond calls for transparency and urge providers to follow baseline practices to foster a climate favorable to consumer and business adoption of cloud services. We hope that businesses that are considering using cloud services will follow these best practices to ensure that their customers' interests in privacy and security are adequately protected.

Law Enforcement Access to Data

A consensus emerged that data stored in the cloud should have the same Fourth Amendment protections as data in possession of an individual. Although providers do not have the power to change the law that applies to cloud services, they can follow certain policies, procedures, and technical design to maximize privacy rights. The group agreed that where service providers are not prohibited by law, they should notify consumers when a law enforcement or civil request has been made for their information.

Legal protections sometimes are justified based upon the employment of technical measures, such as privacy settings. Thus, cloud service providers that make encryption and other privacy-enhancing technologies available to consumers will be at a competitive advantage.[19]

[19] However, recent renewed calls for enhanced mechanisms to facilitate law enforcement access to data held by private networks could affect any competitive advantage gained through such technologies. See

Secondary Use

The group could not come to consensus about the appropriate extent of secondary uses in cloud service models. Some argued that secondary uses were not well understood by consumers, and that such uses inherently conflict with a cloud provider's role as information fiduciary. Consumers may conceive of a cloud service as akin to a storage locker—as a rental company that simply rents space that is physically locked by the consumer. A secondary use business model is one where the rental company breaks the lock and periodically peeks at the contents of the locker. Not only that, the rental company may track and record the consumer's comings and goings, how often they open the unit, etc.

Other retreat participants argued that secondary uses might constitute the basis of the bargain for provision of the service. Consumers may be willing to have content or transactional information scanned for advertisements or for analytics in exchange for discounted or free services. Other participants argued that secondary uses should be prohibited altogether.

The group did achieve a clear consensus requiring transparency for secondary uses. Providers should clearly demarcate uses for data that are necessary for operation of the service, "technical justifications," versus "business justifications," that is, uses of personal information that are related to the business model employed by the provider. For instance, monitoring the amount of use a consumer engages in is operationally necessary to address issues such as forecasting the need for more servers or bandwidth. Conversely, accessing content or transactional information for advertising or other marketing activities is a clear business secondary use that is not necessary for technical operation of the service.

Furthermore, when a provider develops new uses of content and transactional information, it should notify the consumer and use an opt-in consent standard before deploying the new use.

---

e.g., Charlie Savage, *Officials Push to Bolster Law on Wiretapping*, New York Times, Oct. 18, 2010, available at http://www.nytimes.com/2010/10/19/us/19wiretap.html

Portability and Interoperability

A consensus emerged that data portability is a key issue to competition and user freedom. The risk of lock-in is a substantial barrier to adoption of cloud services for consumer, business, and government users. Consumers should be able to easily export the information they supply to and generate in the cloud.

This risk of lock-in reaches its zenith in highly-sticky, popular web services, such as Facebook. Consumers spend years enhancing their profiles and building links to friends in environments that do not support portability, thereby creating imposing switching costs for individuals who wish to change to different services. These sites leverage network effects to become popular, but once they have obtained broad adoption, stickiness and a lack of portability reduces competitors' chances of attracting users.

On the other hand, it is precisely this social graph and related services that constitute the "special sauce" of Facebook and similar companies, at least a part of whose success is attributable to innovation and investment. Some argue that it is unfair for consumers to use a free service and also have the option to take the value from that service at will.

A subset of the group argued that nevertheless, competition would be enhanced by the ability of consumers to export all information related to their profiles. This group argued that while services like Facebook have created compelling platforms for interaction, they are fueled by the currency of consumers' personal information and attention. In the case of Facebook and many of its competitors, users are subjected to advertisements. This points to an exchange in value and bolsters the argument that users of services like Facebook should be able to export their data when they desire. On balance, the interests of consumers and competition would be served by the ability to export this information elsewhere.

Data portability may raise nuanced privacy problems if not implemented carefully. James Grimmelmann, in his article *Saving Facebook*, elucidates risks of unintended privacy harms: if the exported data are moved to a service with different norms or privacy rules, it could result in consumers pulling information about others

into less-protected spaces.[20] If, for instance, a consumer set restrictive sharing preferences in Facebook, should that consumer's friends be able to export the data to another service that is less restrictive?

Interoperability is a related and important issue to portability. Consumers and businesses alike will benefit from the employment of standard data formats that lower switching costs and prevent lock-in. A consensus emerged that providers should not affirmatively interfere with interoperability.

Data Security

Consumer control is a particular challenge in the cloud. While consumers may experience an effective increase in security protections through cloud services, they also may lose the ability to make smart security decisions based on how they—or trusted experts—evaluate the risks of using a particular service. Thus, it is particularly important that cloud providers work to demonstrate operational safeguards and verify trusted security mechanisms in a transparent manner—without jeopardizing the security of the wider community through complete disclosure.

Transparency is so important in this realm that it is our consensus view that cloud providers should make their systems available for analysis by outside security experts. This could take the form of expert audit, which would result in the conferral of an industry-recognized certification. Such certifications (e.g., ISO-27001/2) demonstrate to both active and prospective customers alike that the provider is taking necessary steps to protect personal data.

"Free" Services

Our consensus view holds that "free" services should be subject to the same rules as traditional for-pay services. It is said, "Consumers get what they pay for," but in the case of "free" services, *consumers are paying*. Providers operating "free" services profit through the currency of personal information instead of direct payment.

[20] 94 Iowa Law Review 1137, 2009, available at http://works.bepress.com/james_grimmelmann/20

Creating a level playing field for for-pay and free services will enhance competition. Without parity, "free" services will compete by cutting corners rather than providing quality services; this will actually dilute best practices, causing for-pay services to join free alternatives in a race to the bottom.

Deletion

Our consensus view is that consumers should have the right to delete the data they upload to the cloud. There was some disagreement surrounding the extent to which consumers should have the ability to delete data. It seems intuitive that consumers should be able to delete the data they upload to storage and similar services. However, a consensus did not emerge surrounding data that is generated in the cloud itself. For instance, a consumer may tag someone else's photos, write on the "walls" of social networking sites, and the like. Some thought that such material would not be subject to a deletion option, while others thought that deletion should be more expansive. User deletion is a complex issue and there is still much to resolve. It may be costly and complex, for instance, for providers to delete data in backup systems. Furthermore, the volumes of transactional data generated in the cloud presents policy and technical challenges for deletion.

We are aware that sometimes, consumers state that they wish to delete their cloud data, and later regret the decision, often asking the provider to somehow recover the material. An interesting approach to this problem is found in a Norwegian best practices standard concerning cloud storage of photographs.[21] Under that standard, customer files and metadata are quarantined for a period before being actually deleted. This makes the data unavailable to both the consumer and the cloud provider, for a specified period of time, unless the consumer reactivates the account.

[21] Norwegian Consumer Council, New standard for secure online photo storage, available at http://forbrukerportalen.no/Artikler/2010/standard_for_secure_online_photo_storage

Transparency

Transparency is a critical aspect of consumer protection, but by itself, it may fail to achieve results in line with reasonable consumer expectations. In cloud services as with many other technical products, subtle design decisions can have profound implications for consumers, and consumers often do not perceive these issues until they encounter a problem.

Recall the discussion above concerning portability. At enrollment, consumers probably are not thinking about the idea that someday, they may have to cancel their service and wish to remove data from the cloud. A clear disclosure on this important subject made available when the individual is comparing services, could sensitize the consumer to this concern, and cause some consideration of the importance of portability to that particular user.

We think that clear disclosure of key terms will prepare consumers to think through the implications of adopting cloud services, and make better decisions. We also believe that a model disclosure will enhance competition in this space, as its information-forcing value is likely to cause providers to end marginal practices and to highlight meaningful ways in which services are distinguished from others.

The model disclosure in Appendix A focuses on several key issues:

- What is the cloud service provider's business model? Bradshaw et al. found that the business model was key in influencing the terms on which service is offered.[22] It thus must be completely clear how the cloud service provider intends to monetize its product. It is not clear at all that consumers understand that some providers intend to use data uploaded to the cloud or transactional data for secondary purposes. Consumers may see that web services are advertising-supported, but many may not understand the extent to which data they provide is used to tailor marketing.

[22] See fn. 13 supra.

- What entity actually provides the cloud service? In order to evaluate competitors, the actual service provider's identity is critical information for consumers and business users concerned about possibly providing data to a competitor or to a government with adverse interests.
- Is consumer content or transactional information shared? If so, with whom? Recall that information sharing is a key consumer concern according to the Pew Internet study. Far too many privacy policies cryptically discuss information sharing. Some use the word "partner" to mean third party. Some muddy the waters by making speculative statements about sharing: "We may, from time to time, share information with carefully chosen marketing partners…"
- Is consumer content or transaction data used for purposes not required for the technical operation of the service? A key consumer concern is secondary uses of information unrelated to the technical operation of the service. These uses need to be prominently disclosed in order for the consumer to understand the basis of the bargain.
- Is the provided service a private or public cloud? Whether data are stored on a shared resource or a dedicated one is critical for practical privacy and security concerns.
- What data can the consumer export and in what format? Portability is a key issue, and practically, the formats in which one can export data are important for determining whether a service is compatible with the consumer's existing software.
- Will consumers be notified of security breaches? Security breach notification laws have broad application, but do not always require notice to consumers in the cloud computing context. For instance, some providers are "data agnostic," meaning that they do not claim to know whether a consumer's account contains trigger information for security breach notification laws. Consumers may falsely assume that providers

are required to notify them of breaches; policies surrounding notification should be made clear.

- Where are data stored and what law governs the privacy and security aspects of the cloud provider's services? Generally speaking, consumers are not aware of where a service stores their data or what laws protect (or do not protect) data uploaded to the cloud. A short disclosure of which laws are applicable will guide users in choosing services.
- What procedures are followed when closing accounts? Consumers need to know how services will handle problems such as non-payment and the potential bankruptcy or massive failure of a service provider.
- Who is responsible for consumer and privacy issues and what is their contact information? Including accurate contact information for the individual responsible for consumer privacy and security concerns is extremely helpful for when consumers have questions or when problems arise. This information should include not only company specific resources, but consumer protection and regulatory resources for dealing with complaints when a situation cannot be resolved with the company.

Conclusion

It is our goal that these best practices for business-to-consumer services will reduce uncertainty and promote competition in cloud computing. We believe that consumers, businesses, and governments will benefit from more transparency, and a commitment to the consensus values identified in this document

Appendix A: Best Practices in Disclosure for Business-to-Consumer Services

**Answers to the questions provided are illustrative.*

1. What is the cloud service provider's business model?
    a. "We charge consumers a fee for this service."
    b. "We serve advertising based upon consumers' interests in exchange for the service"
    c. "We analyze consumers' information in order to serve advertising based upon their interests"
2. What entity actually provides the cloud service?
    a. "We provide it directly"
    b. "We provide it directly, and use the following subcontractors…"
    c. "We subcontract all services to…"
3. Is consumer content or transactional data shared? If so, with whom? What choice mechanisms are in place?
    a. "No"
    b. "Yes, we share information with affiliates, and you can opt out by X"
    c. "Yes, we share information with third parties, and you can opt out by X"
4. Is consumer content or transaction data used for purposes not required for the technical operation of the service?
    a. "No"
    b. "Yes, we use content/transaction data to target advertisements"
5. Is the provided service a private or public cloud?
    a. Private cloud: the service is provided for a single entity
    b. Public cloud: many consumers may be using the same service
6. What data can the consumer export and in what format?
    a. The consumer can export all data that the user provides in standard formats, including csv, txt, xls.
    b. The consumer can export data only in proprietary formats
7. Will users be notified of security breaches?
    a. Yes, according to the law of [jurisdiction]
    b. No
8. Will the consumer be promptly notified if there is a law enforcement or civil request for data about the consumer?
    a. Yes, if we are legally able to notify users
    b. No
9. In what jurisdiction are the data stored?
    a. [list one or more countries]
    b. [indicate whether user or service has discretion to select storage location]
10. What jurisdictions' laws govern the privacy and security aspects of the cloud providers' services, and what is the relevant consumer protection authority?

11. What procedures are followed when closing accounts?
    a. We will give consumers 30 days of access before closing their accounts for non-payment
    b. In the event of discontinuance of service, we will give consumers 30 days of access to extract data
12. Who is responsible for consumer and privacy issues and what is their contact information?
    a. Name responsible employee and provide contact information.

Appendix B: Sample Disclosure

Our Business

We provide services to you for a fee.

We own and operate the equipment for this cloud service.

Your Data

We do not share content or transactional data with third parties.

We only use content and transactional data for purposes required for the technical operation of the service.

You can export data uploaded and generated on this service in standard formats, including csv, txt, and xls.

If possible, we will notify you if another party requests data or information about your use of this service.

Our Cloud

Your service level is a private cloud, meaning that we are using a dedicated infrastructure for your services.

Our cloud operates in the following countries: the USA and Canada.

Our cloud services are governed by the laws of the USA and Canada and by the following regulators:

U.S. Federal Trade Commission
Privacy Commissioner of Canada

Security

If we become aware of a security breach, we will inform you of it consistent with the law of California.

In January 2010, our service was certified as compliant with ISO-27001/2 by our auditor.

Account Termination

In the event of a termination of our services, or nonpayment on your account, we will give you notice and 30 days to export data from our cloud.

Contact Us

Our privacy and security contact is:

Joan A. Privacyofficer
1 Embarcadero Center
San Francisco, CA 94001
(415) 555-1212
privacyofficer@cloudprovider.com

Appendix C: Cloud Computing Retreat Participant List

June 20-22, New York City

Svenn Anderson
Policy Advisor
Norwegian Consumer Council

John Breyault
Vice President of Public Policy,
Telecommunications and Fraud
National Consumers League

Justin Brookman
Senior Fellow
Center for Democracy and Technology

Jules Cohen
Director of Online Privacy and Safety
Microsoft

Mike Egan
Director of Government Affairs
Microsoft

David Fagan
Partner
Covington & Burling LLP

Harold Feld
Legal Director
Public Knowledge

Robert Gellman
Privacy Consultant

Colin Gilbert
Director
Civitas Group

Beth Givens
Director
Privacy Rights Clearinghouse

Rick Gordon
Managing Director
Civitas Group

Susan Grant
Director of Consumer Protection
Consumer Federation of America

Chris Hoofnagle
Lecturer
University of California Berkeley Center for Law & Technology[23]

Brian Huseman
Senior Policy Counsel
Intel

Marzena Kisielowska-Lipman
Senior Policy Advocate
Consumer Focus

Cornelia Kutterer
Senior Manager, Regulatory Policy
Microsoft

Falk Luke
Policy Officer, Consumer Rights in the Digital World
Federation of German Consumer Organizations

[23] Affiliation for identification purposes only.

Helen Nissenbaum
Professor, Media, Culture and Communication
New York University

Marco Pierani
Head of Public Affairs
Altroconsumo

Ira Rubinstein
Senior Fellow
Information Law Institute
New York University School of Law

Linda Sherry
Director, National Priorities
Consumer Action

John Simpson
Consumer Advocate
Consumer Watchdog

Katherine Strandburg
Professor of Law
New York University School of Law

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation

Frank Torres
Consumer Affairs Director
Microsoft