UIC John Marshall Journal of Information Technology & Privacy Law

Volume 27
Issue 4 *Journal of Computer & Information Law - Summer 2010*

Article 3

Summer 2010

An Evolutionary Study of Cloud Computing Services Privacy Terms, 27 J. Marshall J. Computer & Info. L. 593 (2010)

Konstantinos K. Stylianou

AN EVOLUTIONARY STUDY OF CLOUD COMPUTING SERVICES PRIVACY TERMS

KONSTANTINOS K. STYLIANOU*

INTRODUCTION

By now we should be used to technology advancing faster than the law can adapt to it. This often means that in the early stages of technological developments there might be some uncertainty as to what norms apply and how should new products and services be treated. Cloud computing, the vagueness of the term notwithstanding, is one of those turning points where new opportunities and new dangers collide, while the law remains still largely absent. This legal gap is partly filled by contractual terms (usually referred to as Terms of Use), which are not always fair, clear or adequate. These weaknesses become more controversial when they relate to sensitive issues like privacy. And precisely because the main idea behind cloud computing is the remote processing and storage of large amounts of information – some of which private- vulnerabilities in the contractual terms of use of cloud computing services attract greater scrutiny.

That said, privacy dangers are often grossly overstated. Moreover, the rapid pace of technological advancements raises fears that technology is becoming increasingly intrusive in our lives. With cloud computing at the gates, the question, then, becomes whether privacy is indeed under greater threat than before. This paper examines the evolution of a number of cloud computing services' terms of use with the aim to discern whether they offer less or more (or equal) privacy safeguards. To better highlight the changes cloud computing has brought about, I focus on those privacy terms that relate to the special modus operandi of cloud services.

To this end this paper proceeds in three parts. Part I identifies the special ways by which cloud computing challenges privacy. These are

* S.J.D. University of Pennsylvania Law School (c.) '13, LL.M. Harvard Law School '10, LL.M. Aristotle University of Thessaloniki '08, LL.B. Aristotle University of Thessaloniki '06.

issues that have been known to pose threats to privacy in the pre-cloud world as well, but are exacerbated in the cloud environment given its nature. Part II discusses a series of privacy terms commonly found in the sampled cloud computing services and follows their evolution by comparing previous versions where available. Part III then goes on to analyze what the changes mean and whether they give reasons to believe that cloud computing will more deeply compromise privacy. The overall conclusion is that cloud computing does result in the collection of more private information, but this mostly happens voluntarily. Industry trends also show an increase in sharing and combining the collected information. But in terms of how companies treat the privacy of their users, all in all we notice a more professional stance and a significant effort to abide by higher standards. Thus, this paper concludes, cloud computing poses a greater threat insofar as more information is being collected and shared, but from a technological perspective cloud companies do not appear to indulge in greater privacy compromises than necessary to deliver their services.

I. CLOUD-SPECIFIC PRIVACY CONCERNS

After sixty years of digital technology and twenty years of digital networking the legal scholarship is inundated with examples that substantiate the very real threat to privacy posed by digital technology.[1] Recently, however, with the dawn of broadband networks and always-on connectivity, the interconnected world experienced a qualitative shift in how people interact with networks. Whereas up until now digital networks served mostly as a communications tool that connected people with each other or with businesses and services, now they have transformed into an extension of the human social life, working environment, and entertainment sphere. As a result, the new ubiquitous networking ecosystem is in certain respects qualitatively different and so are the concerns it raises with regard to privacy.[2]

Although it is hard to delineate the precise transformations in the networks' nature or the exact time the transition happened, a definition of what has come to be called cloud computing is at this point necessary. What most business executives, lawyers and computer technicians probably understand under cloud computing is a scalable network of servers

1. There is probably no better illustration of how technology facilitates privacy violations than the very recent collection of data breaches the Privacy Rights Clearinghouse put together documenting more than 350 millions of stolen records from 2005 till today. See *Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE (Apr. 20, 2005), http://www.privacyrights.org/ar/ChronDataBreaches.htm.

2. Johann Cas, *Privacy in Pervasive Computing Environments – A Contradiction in Terms?*, 24 IEEE TECH. & SOC'Y MAG. 24 (Spring 2005), *available at* http://rfrost.people.si.umich.edu/courses/SI110/paper_support/Cas,%20Privacy%20and%20Ubiquity.pdf.

on which users store data that would traditionally reside on a local computer, and whose processing power they use to run applications and services while their output is transmitted to the user's computer.[3] Typical cloud services include webmail clients (e.g. Yahoo! Mail), software-as-a-service (e.g. Google Docs), and infrastructure services (Amazon EC2). The availability of quasi-unlimited storage, the distributed architecture of storage and processing, and the high-speed always-on connections that carry the necessary traffic recast the focus vis-à-vis privacy in three main respects:

Quantity and Nature of Data: Cloud computing services by definition aggregate large amounts of data either while serving as storage facilities or as part of a processing request. The proliferation of cloud computing services further means that more data –some of which private- will be transferred away from the user's immediate physical control (i.e. the user's personal/work computer) and to the control of a remote third party.[4] Most importantly though, various cloud computing services address different consumer needs and therefore require the collection of different kinds of information.[5] As a result cloud computing services cause more diverse information to be shared with remote third parties. This in turn, raises concerns about whether this volume of data will be abused by the controlling third party or the government.[6]

Fourth Amendment Issues: Another set of issues concerns how cloud computing services relate to the theory and case law around the Fourth Amendment. More specifically it is still debatable whether access to online stored data should be considered a search, whether the uploader has a reasonable expectation of privacy,[7] or whether by communicating data to a remote server the subject is considered to have know-

3. Cloud computing is more of a marketing than a legal term (previously referred to as grid computing). *See* David Chappell, *A Short Introduction to Cloud Platforms: An Enterprise-oriented View*, DAVID CHAPPELL & ASSOCIATES (Aug. 2008), http://www.davidchappell.com/CloudPlatforms—Chappell.pdf. *See also* Brian Hayes, *Cloud Computing*, 51 COMMS. OF THE ICM 9 (2008). Richard Stallman, founder of the GNU project, finds no real value in treating cloud computing as a separate technology, and rather finds it "a marketing hype." *See* Bobbie Johnson, *Cloud Computing Is a Trap, Warns GNU Founder Richard Stallman*, THE GUARDIAN, September 29, 2008, http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman.

4. Ann Cavoukian, PRIVACY IN THE CLOUDS 3 (2008), *available at* www.ipc.on.ca/images/Resources/privacyintheclouds.pdf.

5. Randal Picker, *Online Advertising, Identity and Privacy* 2 (Univ. of Chi. Law & Econ. Working Paper No. 475, 2009).

6. Stephen H. Wildstrom, *Google's Gmail Is Great — But Not for Privacy*, BUS. WK., May 3, 2004, at 30. Privacy leaks may occur even accidentally, due to a technical bug or human error. *See*, *e.g.,* Jason Kincaid, *Google Privacy Blunder Shares Your Docs Without Permission*, TECHCRUNCH, (Mar. 7, 2009), http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/.

7. Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

ingly exposed the information and hence is not entitled to protection.[8] If privacy is indeed an important concern for users and companies, then cloud computing exacerbates the situation, as it not only multiplies the cases where privacy and technology may collide, but it also complicates matters as it blurs the line between actions that used to take place only on one's desktop computer and actions that can now be performed online.[9] It is indeed hard to pinpoint the difference in a user's practice and animus between typing a document on his desktop computer and typing a document on Google Docs. Yet the location of the physical copy of the file (the user's local computer or the remote cloud computer) makes a world of difference. Another issue that remains open is what kind of analogies courts will be willing to uphold in comparing physical and digital spaces.[10] Courts do seem favorable to affording protection to emails[11] and password-protected websites[12] (as would be the case of an online storage service), but we are far from having a comprehensive privacy framework on which businesses and customers could safely rely.

Transfer of Data Between Countries: By its very nature cloud computing is effectuated through a system of distributed and decentralized computer networks that may or may not be confined in a single state. In other words, cloud services may draw the necessary data and processing power from servers that reside in different parts of the world. However, while technological applications may transcend national borders, privacy laws often do not,[13] and so the locus of storage is a very real consideration for companies whose business network extends beyond the borders of one state. The gravest expression of the implications of different levels of privacy protection occurred when the European Union –known for its stringent privacy rules- passed the Data Protection Directive,[14] which allows the transfer of data intended to undergo processing to third countries only if they ensure an adequate level of protection (ar-

8. *Id.* ("What a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protection"). *See also* U.S. v. White, 401 U.S. 745 (1971); California v. Greenwood, 486 U.S. 35 (1988).

9. Bruce R. Wells, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content,* 12 J. CONST. L. 223, 231 et seq. (2009).

10. David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2219 et seq. (2009).

11. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).

12. U.S. v. D' Andrea, 497 F. Supp. 2d 117 (D. Mass, 2007).

13. For an account of how different cultures reflect different privacy concerns and how this translates into different privacy laws *see* Steven Bellman et al., *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20 INFO. SOC'Y 313 (2004).

14. Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 281) 31 (EC).

ticle 25(1)). In the cloud computing context this would mean that data collected by an American company by servers installed in Europe could not be transferred to servers in the United States unless the United States offered a similar level of protection, even if the entire process was automatic and only for the purpose of making the cloud service possible. Since a privacy law overhaul would be too much to ask for, the United States negotiated a "Safe Harbor" agreement with the European Union, according to which American companies could transfer data from Europe as long as they abided by a commonly agreed upon privacy framework set by the United States Department of Commerce and the European Commission.[15] While the US-EU Safe Harbor program provides some assurance when it comes to doing business in Europe, the problem of divergent privacy laws and data transfer between countries remains open both for companies that do not subscribe to the Safe Harbor Program and for companies that do business outside of Europe.

Interoperability and Data Portability: The growing tendency to transfer more and more activities online has not only led to the development of specific-purpose applications but also to online platforms, which serve as a hub for users to create their own applications or store content (e.g. Google AppEngine, Salesforce). While we are not quite there yet, it is likely that in the near future some (or maybe the majority) of these platforms and applications will allow interoperability, so that users can transfer content seamlessly from one service to another.[16] This may come as a very welcome development from the viewpoint of innovation and consumer welfare,[17] but it raises certain privacy concerns, because the technical interoperability of two services does not necessarily guarantee similar privacy safeguards. Therefore, the transfer of data from one service to another might result in some privacy loss. One could reasonably argue that informed consent to the privacy policy of the service where the data is being transferred can serve as a satisfactory solution, however, it is also reasonable to expect that users will simply assume a comparable level of protection between the two similar services and will thus omit reading the new privacy policy. To complicate things even further, it may not always be the end user who requests the transfer of data. Such is the case of a user that shares personal data with a company (or other entity such as a hospital) and the company subsequently

15. William J. Longand & Marc Pang Quek, *Personal Data Privacy Protection in the Age of Globalization: The US-EU safe Harbor Compromise*, 9 J. EUR. PUB. POL'Y 325 (2002).

16. Marco Iansiti, *Principles that Matter: Sustaining Software Innovation from the Client to the Web* 10-14 (Harvard Bus. Sch. Working Paper No. 09-142, 2009).

17. Interoperability and openness enhance the conditions of innovation output because they maximize the value of the platform upon which applications are developed by allowing more users to connect and share data. *See* MARCO IANSITI & ROY LEVIEN, THE KEYSTONE ADVANTAGE 161-164 (2004).

chooses to outsource part of their operations to a third party cloud company. It then rests with the outsourcing company to ensure that the commissioned company offers an equivalent level of protection to which its users have consented.

II. TRACING THE EVOLUTION OF CLOUD COMPUTING SERVICES' PRIVACY TERMS

As cloud computing services become more popular, the stakes of offering robust privacy protections become higher.[18] At the same time, the amount of information available to companies increases steadily and forms a valuable source of consumer habits, such that companies are enticed to increase their ad revenues or expand their business.[19] In drafting the contractual privacy terms, companies are called to strike a balance between protecting the privacy of their customers and indulging in the temptation to monetize the data available to them. In this part, I explore the evolution of major cloud services providers' privacy terms to highlight the tendencies in the fields that are the most vulnerable to the peculiarities of the cloud environment as explained previously in Part I: how much data is collected, where is it stored, how long is it retained, how is it used, who has access to it, and under what conditions of security does all of this happen. The discussion will revolve around the following typical examples that cover the spectrum of the most common cloud services:

- IBM LotusLive (online collaboration)
- Amazon Elastic Compute Cloud (EC2) (infrastructure)
- Apple MobileMe (online synchronization tool)
- Gmail (email client)
- Mozy (remote storage service)
- Microsoft Windows Azure (cloud operating system)
- Salesforce Force.com (cloud platform for business applications)

The previous versions of the privacy policies were drawn by the Internet Archive (archive.org) and EFF's TOSBack project (tosback.org). For some of these services the user's privacy status is regulated either only by the company's general privacy terms (e.g. Mozy) or by the general privacy terms complemented by an additional agreement for the

18. A recent Microsoft survey found that 90% of Americans are using some form of cloud computing, but at the same time "more than 90 percent of [the people] are concerned about the security, access and privacy of [their own data in the cloud]." See MICROSOFT, CLOUD COMPUTING FLASH POLL – FACT SHEET (2009), http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc.

19. Michael A. Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1486-1489 (2000).

specific service.[20] In such cases, all the binding legal documents were reviewed (*see* Appendix).

Quantity and Nature of Collected Data: Cloud services collect two types of data: information that the service automatically collects as part of its operation or as part of its advertising policy, and information that the user voluntarily shares with the service as part of using it. The general impression is that the amount and quality of data cloud services collect automatically has increased, but not disproportionally compared to other websites that use cookies and web beacons (single pixel gifs that assist in the deployment of cookies and the collection of information) to track the user's activity on the website as well as to collect information about the user's location, computer type, referring site and other non-identifiable information.[21] This is not to understate the dangers stemming from the growing number of tracking cookies, but rather that this is not a cloud-specific phenomenon. Like most websites, cloud services make clear that they install cookies, but they do not disclose their number or their exact function. Some companies, like IBM, provide a few additional details concerning the expanded scope of collected information stating that they collect "information that pertains to [the user] indirectly through other sources, such as list vendors."[22] Unlike its previous privacy policies, IBM also notes that it may also collect and share information with third parties in case the user signs up for *co-branded* offerings sponsored both by IBM and the third party.[23]

With regard to the second type of collected information, naturally the volume and diversity of the information users choose to share with cloud services is vastly greater compared to the pre-cloud era. Mozy can replicate a user's entire hard disk on its servers, Apple's MobileMe stores "in the cloud" a user's contacts, email and calendar events, and Salesforce customers can host their entire business' inventory and clientele. Some of the sampled companies have also started offering online technical support, forums or live help. These options, however, do not relate directly to the cloud service itself and users are free to disclose as much information they want.

---

20. Amazon's EC2 service, for example, is offered under the "Amazon Web Services Customer Agreement" which incorporates by reference Amazon's general privacy notice.

21. A recent study commissioned by THE WALL STREET JOURNAL showed that the number of tracking cookies websites planted in the users' computers has grown significantly, and that tracking technology has become more sophisticated. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html?mod=what_they_know (last visited Nov. 8, 2010).

22. *IBM Online Privacy Statement: Cookies, Collection of Personal Information*, IBM (Jan. 28, 2010), http://www.ibm.com/privacy/details/us/en/#section_1.

23. *IBM Online Privacy Statement: Marketing*, IBM (Jan. 28, 2010), http://www.ibm.com/privacy/details/us/en/#section_1.

Use of Data: Some of the collected data's uses are obvious and relatively uncontested (e.g. fulfill a request, personalize the user's experience on the website). Others are more vague, but still sound innocuous; for example, in 2007, Apple added to its Customer Privacy Policy that it can use the collected information for "data analysis, and research to improve Apple's products," a term that still stands.[24] Google Gmail's automated scanning technology was highly criticized when introduced back in 2004, but by now the polemic against Google's intrusiveness has significantly abated. Interestingly, Google changed the wording in its Privacy Policy from "[w]e serve highly relevant ads . . . using our unique content targeting technology"[25] in 2004 to "[t]he Gmail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Gmail[,]" in 2009[26] signifying an effort to reassure users that its technology is not invading their privacy. Later in 2009 Google instituted the Ads Preferences Manager, an aggregate ad-managing tool for all of Google's services. The relevant Gmail part provides yet further details for the users' information: "Google scans the text of Gmail messages in order to filter spam and detect viruses. The Gmail filtering system also scans for keywords in users' emails which are then used to match and serve ads. The whole process is automated and involves no humans matching ads to Gmail content."[27]

However, as the value of users' online presence increases for advertisers, online companies are enticed to use the information they collect more broadly. Amazon, for example, has added in its latest Privacy Notice that cookie-related data can be used to provide "personalized advertisements on *other* websites (e.g. Amazon associates with content served by Amazon.com. . .)."[28] According to its new Privacy Notice, Amazon also helps third party advertisers by allowing them to use data collected by Amazon to personalize advertisements that Amazon then delivers to the user on their behalf.[29]

---

24. *Privacy Policy: Collection and Use of Personal Information*, APPLE, http://www.apple.com/privacy/ (last updated June 21, 2010).

25. *Gmail Privacy Policy (2004)*, GOOGLE, http://web.archive.org/web/20040610074335/gmail.google.com/gmail/help/privacy.html (last visited Nov. 8, 2010).

26. *Google Gmail Privacy Policy: Uses (2009)*, GOOGLE, http://www.tosback.org/diff.php?vid=1087 (last visited Nov. 8, 2010).

27. *Google Advertising and Privacy*: *What Information Does Google Use to Serve Ads on Gmail?* (2010), GOOGLE, http://www.google.com/intl/en/privacy_ads.html (last visited Nov. 8, 2010).

28. *Amazon.com Privacy Notice: What About Cookies?*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496#cookies (last updated Oct. 1, 2008).

29. *Amazon.com Privacy Notice: What About Third-Party Advertisers and Links to Other Websites?*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496#third_party (last updated Oct. 1, 2008).

It is also worth noting that companies increasingly *share* and *combine* the data they collect from their affiliated businesses and/or websites directly or indirectly.[30] Microsoft's[31] Online Privacy Statement is the clearest example of how this works. Microsoft states that it collects information by placing a persistent cookie on the user's computer and that it may "associate this information with [the user's] subsequent visit, purchase or other activity on participating advertisers' websites in order to determine the effectiveness of the advertisements."[32] Having said that, Microsoft also makes clear that "[w]hen [it] display[s] personalized targeted ads, [it] take[s] a number of steps designed to protect [the user's] privacy. For example, [it] store[s] page views, clicks and search terms used for ad personalization targeting separately from [the user's] contact information or other data that directly identifies [him]."[33] IBM has also significantly expanded the practice of sharing by adding in its latest Online Privacy Statement the following term:

> We may also use or share your information to protect the rights or property of IBM, our business partners, suppliers, clients, or others when we have reasonable grounds to believe that such rights or property have been or could be affected. In addition, we reserve the right to disclose your personal information . . . when we believe that disclosure is necessary to protect our rights, or the rights of others. . .[34]

The wording of this provision takes an alarmingly broad view of what IBM can do with users' information and leaves a lot of margin for interpretation of what kind of rights or entities IBM might seek to protect.

---

30. The IBM Online Privacy Statement states that "[t]he information we collect, either directly or indirectly, may be combined to help us improved its overall accuracy. . .," at Collection of Personal Information. *IBM Online Privacy Statement: Cookies, Collection of Personal Information*, IBM (Jan. 28, 2010), http://www.ibm.com/privacy/details/us/en/#section_1. Amazon states that it shares the information it collects with third-parties for the purposes described in its Privacy Notice, but the relevant part is unclear about which data precisely is being shared. *Amazon.com Privacy Notice: Does Amazon Share the Information it Receives?*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496#share (last updated Oct. 1, 2008).

31. Microsoft is a computer software and equipment company. Microsoft Azure is an operating system that allows the user to run software on remote Microsoft servers.

32. *Microsoft Online Privacy Statement: Display of Advertising (Opt-Out)*, MICROSOFT, http://privacy.microsoft.com/en-us/fullnotice.mspx (last updated Aug. 2010).

33. *Id*.

34. *IBM Online Privacy Statement: Protect the Rights and Property of IBM and Others*, IBM, http://www.ibm.com/privacy/details/us/en/#section_1 (last updated Jan. 28, 2010). Other companies already had similar but considerably more restricted terms. For example Salesforce's equivalent provision states: "Salesforce.com reserves the right to disclose personally identifiable information of the Company's Customers or Visitors if required by law or if the Company reasonably believes that disclosure is necessary to protect the Company's rights. . .." *Privacy Statement: Sharing of Information Collected*, SALESFORCE (Sept. 18, 2010), http://www.salesforce.com/company/updated_privacy.jsp.

Data Retention Policy: Most companies acknowledge that it is important to users to be able to exercise full control over the data they voluntarily share with a service. One aspect of this control is the ability to permanently remove on demand their data from the service. With respect to this option the protection offered by cloud services has generally improved. For example, when Salesforce[35] started its operation back in 1999, and for many years, its privacy statements provided that if a customer wanted to discontinue the service and have his data returned, he should contact Salesforce by email.[36] There was no specific timeframe by which Salesforce was bound to abide. On the contrary, its current Master Subscription Agreement clearly states that upon request the company will delete all data after thirty days.[37] Gmail's previous Privacy Policies also lacked a timeframe providing only that "[r]esidual copies of email may remain on our systems, even after you have deleted them from your mailbox or after the termination of your account."[38] Google later changed its Gmail Privacy Policy to: "Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems,"[39] but this provision was removed in the last version. Mozy's Privacy Policy has consistently allowed users to remove their personal data from its databases throughout its operation from 2005 to today.[40]

Data Storage Location: Because different national laws accord different levels of protection to personal and private information, it is important that users know where their data is stored. Some of the cloud services that do business in different parts of the world have selected to provide information as to where their users' data reside. In detail, companies inform about and ask users to consent to the transfer of their data from and to the United States, most likely in view of the Safe Harbor requirements, to which all of the sampled companies participate.

---

35. Salesforce is a cloud computing company that provides business software –most notably customer relationship management tools- on an online platform.

36. *See, e.g.*, *Privacy Statement, Correcting & Updating Your Information (2004)*, Salesforce, http://web.archive.org/web/20040406201932/salesforce.com/us/statements.jsp?file=privacy&src=web (last visited Nov. 8, 2010).

37. *Master Subscription Agreement (2009), § 12.5*, SALESFORCE, http://www.salesforce.com/company/msa.jsp#term (last visited Nov. 8, 2010).

38. *Gmail Privacy Policy: What Types of Personal Information Do We Collect and How Do We Use It (2004)*, GOOGLE, http://web.archive.org/web/20040610074335/gmail.google.com/gmail/help/privacy.html (last visited Nov. 8, 2010).

39. *Google Gmail Privacy Policy: Your Choices (2009)*, GOOGLE, http://www.tosback.org/diff.php?vid=1087 (last visited Nov. 8, 2010).

40. *Decho Corporation Privacy Policy: User Information Decho Collects*, MOZY (May 14, 2009), http://mozy.com/privacy. *See also Decho Corporation Privacy Policy: User Information Decho Collects (2005),* http://web.archive.org/web/20060217041245/www.mozy.com/mozy/privacy (last visited Nov. 8, 2010).

It is not always clear, however, what level of protection applies to users' data when they circulate across the globe. Out of the sampled services, only IBM states that "even in countries whose laws provide for less protection for your information, IBM will still handle your information in the manner described here."[41] While this is a generous statement, it does not answer the question of what happens in case a state where IBM does business in requires a higher level of protection than that described in the Privacy Statement.

Data Safety, Security and Integrity: One frequently advertised advantage of cloud computing is that users store and process their data on highly reliable servers backed by the expertise and experience of IT behemoths. Mozy proudly states that it partners with EMC for the storage of data, one of the worldwide leaders in hosting. It also uses encryption technologies both in transmitting and in storing users' data, one of the few companies to clearly state its security policy.[42] Salesforce also provides detailed information regarding its security policy, but there is no mention of whether the stored data are encrypted (as opposed to the exchange of data, which are encrypted by using SSL).[43] IBM has made its Privacy Statement slightly more explanatory with respect to how it protects users' data. The previous version read "We implement appropriate measures and processes, such as using encryption when transmitting certain sensitive information, to help us to keep your information secure and to maintain its quality,"[44] whereas the updated version is more enhanced and contains more details:

> IBM implements reasonable physical, administrative and technical safeguards to help us protect your personal information from unauthorized access, use and disclosure. For example, we encrypt certain sensitive personal information such as credit card information when we transmit such information over the Internet. We also require that our suppliers protect such information from unauthorized access, use and

41. *IBM Online Privacy Statement, Sharing of Personal Information and International Transfers*, IBM (Jan 28, 2010), http://www.ibm.com/privacy/details/us/en/#section_1.

42. *Mozy Privacy Commitment: Protecting Your Information*, MOZY, http://mozy.com/privacy/commitment (last visited Nov. 8, 2010).

43. *Privacy Statement: Sharing of Information Collected*, SALESFORCE (Sept. 18, 2010), http://www.salesforce.com/company/updated_privacy.jsp. See also *Master Subscription Agreement § 8.3: Protection of Your Data*, SALESFORCE, http://www.salesforce.com/company/msa.jsp?fromSearch=true#confidentiality (last updated Jan. 31, 2009) where it reads:

> We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 7.5 (Compelled Disclosure) or as expressly permitted in writing by You, or (c) access Your Data except to provide the Services or prevent or address service or technical problems, or at Your request in connection with customer support matters.

44. *IBM Privacy Practices on the Web: Information Security and Quality,* IBM, http://www.ibm.com/privacy/details/us/en/previous.html (last visited Nov. 20, 2010).

disclosure.[45]

Amazon is surprisingly candid about its potential inefficiency in protecting data: "We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly . . . you bear sole responsibility for adequate security protection and backup of Your Content and Applications."[46]

Worse even, all of the sampled services consistently repudiate any liability for loss of data and advise users to back up their content. They also declare that it is in their sole discretion to discontinue the service. The future fate of the users' data is not always clear. Only Mozy has a relevant provision stating that in case of termination of the service it "will use commercially reasonable efforts to make [the user's] Data available for [him] to download for a period of three (3) days. Decho has no obligation to provide [the user] with a copy of [his] Data and may remove and discard any Data."[47] Apple goes as far as to include a term in the MobileMe Terms of Service, according to which:

> Apple reserves the right at all times to determine whether Content is appropriate and in compliance with these TOS [sic], and may prescreen, move, refuse, modify and/or remove Content at any time, without prior notice and at its sole discretion, if such Content is found to be in violation of these TOS [sic] or is otherwise objectionable.[48]

III. DISCUSSION

Maybe the most easily noticeable trend that cloud computing has helped spur is the incredible amount and diversity of information users store online. Web 2.0 may have made the Internet more interactive, but it is cloud computing that signifies the transition to ubiquitous always-on networking which has the potentials to substitute part of the desktop computer. As users continue to share more and more information, it is only natural that cloud services will have a much larger database to capitalize upon. However, this should not be construed as cloud services are becoming more pervasive (with the exception of tracking cookies, but this applies to all websites, not just cloud services). The vast majority of data they collect are put in their hands voluntarily by their users. The reasons why users feel comfortable sharing so much information with third

45. *IBM Online Privacy Statement:* Information Security and *Accuracy*, IBM (Jan. 28, 2010), http://www.ibm.com/privacy/details/us/en/#section_4.

46. *Amazon Web Services Customer Agreement*, § 7.2, AMAZON, http://aws.amazon.com/agreement/ (last updated Oct. 21, 2010).

47. *Mozy Terms and Conditions: Term and Termination*, MOZY, http://mozy.com/terms (last visited Nov. 8, 2010).

48. *MobileMe Terms of Service: Removal of Content,* APPLE, http://www.apple.com/legal/mobileme/en/terms.html (last update Jan. 14, 2010).

parties vary.[49] Users may care more about the advantages of new technologies than the disadvantages of some unproven privacy risks,[50] or they may recognize that their information is not always worthy of enhanced protection. As Jeffrey Reimant has put it "a threat to privacy is only worrisome insofar as privacy is valuable or protects other things that are valuable. No doubt privacy is valuable to people who have mischief to hide, but that is not enough to make it generally worth protecting."[51]

Whatever the case –whether privacy matters to consumers or not- there is really no way to attest that cloud services do indeed treat users' data with the discreetness they proclaim. A few, like Mozy and Salesforce explicitly state that their employees do not read or review customer data,[52] but the temptation of employing technical mechanisms (as opposed to humans) to "review" the stored information with the aim to monetize them, thus bypassing the strict wording of the privacy statements, is big.[53] This temptation becomes even more worrisome when it is the reason why companies choose not to apply security and integrity measures so that they can access their users' data and profit from them. For example, if the information transmitted to Gmail and stored on its servers was encrypted, Google's targeted advertising system could not have been possible, because Google could not scan the content of the emails for key words.[54] Cloud services therefore almost always choose to store data in unencrypted format.

---

49. Even traditional privacy threats like government surveillance may be tolerated by users under certain circumstances; if for example surveillance takes place to deter a greater security threat. *See* Tamara Dinev et al., *Internet Privacy Concerns and Beliefs about Government Surveillance – An Empirical Investigation*, 17 J. STRATEGIC INFO SYS. 214 (2008).

50. Social networking sites illustrate this tradeoff in the most exemplary way. While many users have expresses deep concerns about privacy protection in such sites, we have witnessed an explosive growth in the information they post online and the activities –some of them very intimate- they undertake in the frames of digital social networks. *See* MIZUKO ITO ET AL., LIVING AND LEARNING WITH NEW MEDIA: SUMMARY OF FINDINGS FROM THE DIGITAL YOUTH PROJECT 13-34 (2008). *See also* Kevin J. Delaney, *Will Users Care if Gmail Invades Privacy?*, WALL ST. J., Apr 6, 2004, at B1.

51. Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future,* 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 29 (1996).

52. *Decho Corporation Privacy Policy: How Decho Uses Information, Personal Data,* MOZY (May 14, 2009), http://mozy.com/privacy; *Privacy Statement, Customer Data,* SALESFORCE, (Sept. 18, 2010), http://www.salesforce.com/company/updated_privacy.jsp.

53. Paul T. Jaeger et al., *Cloud Computing and Information Policy: Computing in a Policy Cloud?*, 5 J. INFO. TECH. & POL. 269, 276 (2008).

54. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 395.

The biggest threat for unprotected data, however, does not come from inside the cloud companies, but from malicious third parties. Like anything else online, unprotected cloud storage and processing is vulnerable to unauthorized interception, deletion or modification.[55] It is thus no wonder that the uncertainty of how data will be handled once stored, and the fears for potential intrusion, are among the primary reasons why users are reluctant to adopt cloud computing.[56] It is striking that more sophisticated security measures have not been adopted or advertised. One explanation might be that lay consumers, unlike businesses, are largely ignorant both about potential threats and about available remedies, and so companies may lack the incentive to add more security features.[57] To put it differently, lack of market demand creates limited interest from cloud services to come up with enhanced security, especially in view of the additional cost of implementation that it incurs.

As of 2001, government surveillance has also become a major concern when it comes to storing data online in unencrypted format.[58] Despite the heightened value of information they carry, cloud services unfortunately still seem to perform no better than any other web service, at least as far as their contractual terms are concerned. The standard policy of the sampled services is the generalist approach that they do not share personal information unless mandated by law. In effect, the combination of the sensitive nature of information that cloud services usually attract, the lack of adequate security from cloud services, and the intensification of governmental intrusiveness, stands as an impediment to the spread of cloud services.[59]

Notably, when considering cloud computing as an option for the bus-

---

55. Marian Radu &Hilda Larina Ragragio, *The Cloud or the Mist?*, VIRUS BULLETIN CONFERENCE, 238-39 (Sept. 2009), http://www.microsoft.com/downloads/en/details.aspx?FamilyID=76D45B93-467D-414A-B558-D22DF61ABC6A&displaylang=en.

56. *See Cloudy With a Chance of Rain*, THE ECONOMIST, March 5, 2010, at 6, *available at* http://www.economist.com/node/15640793?story_id=15640793. *Amazon Web Services: Overview of Security Processes, Amazon Elastic Compute Cloud (EC2) Security, Instance Isolation,* AMAZON WEB SERVICES, (Sept. 5, 2008), http://aws.amazon.com/articles/1697 (containing detailed information about how information is handled.) One useful detail to know regarding privacy is that "[c]ustomer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically wipes every block of storage used by the customer, and guarantees that one customer's data is never exposed to another."

57. Christopher Soghoian*, supra*, note 55, at 392-95.

58. *See* Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111 (2001). *See contra* Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

59. *Unisys Poll Shows Security Concerns as Leading Cause of User Hesitancy in Adopting Cloud Computing*, INFO. TECH. NEWSWEEKLY, at 64 (Sept. 29, 2009).

iness sector the situation is aggravated.[60] On the one end of the spectrum businesses need to assess whether cloud computing services are ready to support operations in a much larger scale than those of lay consumers. On the other end, and most importantly, businesses must ensure that they have the right to migrate to the cloud when they administer sensitive information, as is the case with hospitals and financial houses.[61] It is indeed doubtful that hospital patients would feel comfortable with the idea of their medical records being stored "somewhere in the cloud." The reluctance for transferring data to the cloud is justified given the qualitative peculiarities of cloud computing. While in essence both cloud services and "traditional" web services store data online, the former make a better target for attacks and surveillance. The reason is that, because of their specialized role and size, they cannot benefit from the attention scarcity effect that characterizes most of the Internet.[62] In other words, because cloud computing services collect large amounts of data, an attack to such services will be more lucrative and economical than several attacks to a variety of separate services. Their premium position comes with greater responsibilities, which they have yet to assume.

Businesses may also be more sensitive than individuals to a couple of other open issues that cloud services have not yet adequately addressed. The first issue relates to the availability of the cloud service. The sampled services present a mixed picture. On the one hand they repudiate any liability for loss of data and they declare that they can stop the service at any time at their sole discretion and even without a warning. On the other hand they are usually very reassuring of the continuous availability of the service. For example, Amazon and Microsoft commit to more than 99.9 percent availability.[63] But at the end of the day, it is reasonable for businesses to be hesitant to entrust their data

60. Paul T. Jaeger et al., *supra*, note 54.

61. For example when Lakehead University decided to start using Gmail's servers as a cheaper alternative to an in-house email system, professors expressed their opposition and claimed that this deal broke "terms of their collective agreement that guarantees members the right to private communications." *See* Simon Avery, *Patriot Act Haunts Google Mail*, THE GLOBE AND MAIL (March 24, 2008), *available at* http://www.theglobeandmail.com/news/technology/article675014.ece.

62. Herbert Simon has famously stated "a wealth of information creates a poverty of attention." *See,* Herbert Simon, *Designing Organizations for an Information-rich World, in* COMPUTERS, COMMUNICATIONS, AND THE PUBLIC INTEREST 37, 40 (Martin Greenberger ed. 1971). *See also* Eszter Hargittai, *Open Portals or Closed Gates? Channeling Content on the World Wide Web*, 27 POETICS 233 (2000), *available at* http://www.webuse.org/pdf/HargittaiPortals2000.pdf.

63. *See Amazon Elastic Compute Cloud*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2/ (last visited Nov. 20, 2010); *Windows Azure Storage Service Level Agreement,* MICROSOFT DOWNLOAD CENTER (Nov. 12, 2010), http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d32702dd-a85c-464d-b54d-422a23939871&displaylang=en.

and processing needs to an entity that assumes no responsibility for whatever can go wrong with storage.

The second issue concerns the location of data storage. As explained before, an inherent characteristic of cloud computing is its distributed operational model, and the technological trends show that information will increasingly be treated as a tradable clustered commodity, whose constituent bits may be dispersed throughout the world.[64] While some firms state that user data may be stored in whichever country the company does business, they offer no way for the user to track down the location of his data or control their flow. The widespread adherence to the EU-US Safe Harbor Agreement[65] somehow ameliorates the problem, but this solution is limited both in scope and in space.[66]

On the bright side, cloud customers may not know the exact location of their data, but at least cloud services are taking positive steps towards ensuring that users remain in control of their data and their online profile. For example, contrary to common fears that the physical alienation of the data from their proprietor would result in loss of ownership over them,[67] all of the sampled services make it perfectly clear that they do not own customer data, rather that their ownership status remains intact.[68] At the same time cloud services increasingly allow users to access the information the service retains about them and even modify it. To counter-balance the more pervasive advertising techniques, cloud services have additionally started offering opt-out features, whereby users can select not to allow the service to share their data with third-parties when they seek to serve targeted advertisements to them.[69]

All these steps, which show greater respect for users' concerns regarding their privacy, are commendable and add up to the list of initiatives taken to better address privacy holes in the services' terms. It

64. *See Clouds Under the Hammer*, THE ECONOMIST, (Mar. 11, 2010), http://www.economist.com/node/15663898?story_id=15663898.

65. All of the sampled services participate in the Safe Harbor, although some joined with a considerable lag since they commenced their operation. In order of join date, Microsoft joined in 2001, IBM and Salesforce in 2002, Amazon in 2003, Apple in 2004, Google in 2005 and Mozy (Decho Corporation) in 2007. *Safe Harbor List,* EXPORT.gov, https://safeharbor.export.gov/list.aspx (last visited Nov. 20, 2010).

66. For a short review of the Safe Harbor limitations *see* James T. Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles,* 9 CURRENTS: INT'L TRADE L.J. 80, 83-84 (2000).

67. *See, e.g.,* Kieron O'Hara & Nigel Shadbolt, *Privacy on the Data Web*, 53 COMMS. OF THE ACM 39 (2010).

68. The peak of this ownership frenzy occurred when a change in Facebook's Terms of Use was misinterpreted to mean that Facebook owned in perpetuity user content, even after deletion. *See* Caroline McCathy, *Facebook: Relax, We won't Sell Your Photos*, CNET (Feb. 16, 2009 2:24 PM), http://news.cnet.com/8301-13577_3-10165190-36.html.

69. *See, e.g.*, Amazon's Network Advertising Initiative Opt-out and Google's Ads Preferences Manager.

seems in general though that the cloud environment is suffering from a circularity problem whereby cloud companies do enhance their services but only bit-by-bit as there is relatively low demand because consumers are still unconvinced of the security the cloud offers. In that respect cloud services are slow to adopt radical (and often expensive) measures, like transferring and storing data in encrypted format, which could possibly increase reliability and attract more users and especially business customers. On the other hand, when it comes to user friendliness, a lot of progress has been noticed. Cloud services are increasingly more transparent and clear about their privacy terms and seem to respect users' needs. There is, however, always room for progress, and though we are surely to expect the continuation of the conflict between the law and the protection level of cloud services, this ongoing clash is not to be interpreted that cloud services are not trustworthy or even dangerous.

CONCLUSION

In his classic work "The Transparent Society" David Brin writes: "No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay."[70] If one is inclined to see technology through such pessimistic lenses, then what cloud computing brings upon us can only reinforce the belief that a surveillance era has come to stay.

However, a more neutral examination of the true implications of emerging cloud computing services suggests two things: a) that people are *willing* to share more information, and b) that cloud services respond relatively well to consumer and legislative pressures in providing increased privacy protection along with the new empowering tools. Most of the companies have significantly expanded their privacy statements to help consumers understand how they treat their data, they have put some effort toward offering harmonized international protection, and they adhere to self-regulatory programs.

Some legal gaps certainly still exist and many of them will become the crux of fierce disputes. But we need to recognize the potentials of the new technological wave and come up with a legal framework that facilitates it, rather than stifles it. How are cloud services supposed to offer a seamless experience to the user if they are not allowed to plant any kind of cookies on the user's computer without his consent, as the new EU privacy directive mandates?[71] It is measures like these that fail to grasp the modus operandi of the digital environment and that we need to steer

70. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 8-9 (2008).

71. Directive 2009/136/EC, art. 5(3), of the European Parliament and of the Council of 25 November 2009, 2009 O.J. (L 337) 20.

away from. Fortunately, cloud services seem to adapt quickly and their increased capabilities and functionality will not disappear in overly strict privacy terms and terms of use.

APPENDIX: LIST OF SAMPLED LEGAL DOCUMENTS

IBM LotusLive (online collaboration)

- Online Privacy Statement (January 28, 2010), http://www.ibm.com/privacy/details/us/en/
- Privacy Practices on the Web (May 1, 2009), http://www.ibm.com/privacy/details/us/en/previous.html

Amazon Elastic Compute Cloud (EC2) (infrastructure)

- Web Services Customer Agreement (October 21, 2010), http://aws.amazon.com/agreement/
- Privacy Notice (October 1, 2008), http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496

Apple MobileMe (online synchronization tool)

- Apple Privacy Policy (June 21, 2010), http://www.apple.com/privacy/
- MobileMe Terms of Service (Jan 14, 2010), http://www.apple.com/legal/mobileme/en/terms.html

Gmail (email client)

- Google Advertising and Privacy (2010), http://www.google.com/intl/en/privacy_ads.html
- Privacy Policy (February 9, 2010), http://www.tosback.org/diff.php?vid=1087
- Privacy Policy (April 8, 2004), http://web.archive.org/web/20040610074335/gmail.google.com/gmail/help/privacy.html

Mozy (remote storage service)

- Privacy Commitment (2010), http://mozy.com/privacy/commitment
- Decho Corporation Privacy Policy (May 14, 2009), http://mozy.com/privacy
- Berkeley Data Systems Privacy Policy (September 15, 2005), http://web.archive.org/web/20060217041245/www.mozy.com/mozy/privacy

Microsoft Windows Azure (cloud operating system)

- Online Privacy Statement (August 2010), http://privacy.microsoft.com/en-us/fullnotice.mspx
- Microsoft Windows Azure Storage Service Agreement (2010), http://download.microsoft.com/download/6/9/6/6966ACAE-9942-47

D0-89B3-09935A6408B9/Windows%20Azure%20Storage%20SLA-English.doc

- Microsoft Windows Azure Compute Service Level Agreement (2010), http://download.microsoft.com/download/0/E/E/0EE244BF-22CA-4180-ACF0-F2F40CAEE3D6/Windows%20Azure%20Compute%20SLA-English.doc

Salesforce (cloud platform for business applications)

- Privacy Statement (September 18, 2010), http://www.salesforce.com/company/updated_privacy.jsp
- Master Subscription Agreement (January 31, 2009), http://www.salesforce.com/company/msa.jsp
- Privacy Statement (2004), http://web.archive.org/web/20040406201932/salesforce.com/us/statements.jsp?file=privacy&src=web