Protecting user privacy in the Cloud: an analysis of terms of service

Konstantinos Stylianou [1] , Jamila Venturini [2] & Nicolo Zingales [3]

Cite as Stylianou K., Venturini J., & Zingales N., "Protecting user privacy in the Cloud: an analysis of terms of service", in European Journal of Law and Technology, Vol 6, No 3, 2015.

ABSTRACT

We present the results of a study that collected, compared and analyzed the terms and conditions of a number of cloud services vis-a-vis privacy and data protection. First, we assembled a list of factors that comprehensively capture cloud companies' treatment of user data with regard to privacy and data protection; then, we assessed how various cloud services of different types protect their users in the collection, retention, and use of their data, as well as in the disclosure to law enforcement authorities. This commentary provides comparative and aggregate analysis of the results.

Keywords: Privacy; Data protection; Terms of service; Cloud computing; Trust; Cloud; Terms of use

1. INTRODUCTION

For anyone following the news, the intersection of privacy and the policies of online services is becoming an increasingly common theme. The terms of service (ToS), as they are usually called, define to a large extent the rights and obligations of users and online services, including those that affect privacy. With the proliferation of cloud services, an increasing amount of data is moving away from the direct control of users and into the hands of private companies. This creates great opportunities and efficiencies both for consumers and for innovative business models, but inevitably also generates significant risks and liabilities.

To harness the potential of this economy, it is important to preserve trust in the use of cloud solutions. This can be greatly facilitated by a better understanding of how cloud services treat customer data vis-a-vis privacy, and more specifically with regard to the collection, use, retention and sharing of those data. Likewise, it is important that "netizens" appreciate the conditions under which cloud services disclose customer data to law enforcement. To that end, the study at hand illustrates the results of the application of privacy-related human rights standards to a list of cloud services, in particular by analyzing their terms of service. The analysis conducted offers insights in industry standards, and good practices and bad practices or omissions by cloud providers.

The study undertaken here is part of a bigger project that was coordinated and funded by the Center for Technology and Society of FGV Law School in Rio de Janeiro, Brazil, and aims to assess the compliance of online services' ToS with basic human rights such as privacy, freedom of expression and due process (Terms of Service and Human Rights Project).

2. FRAMING THE QUESTION AND SETTING THE OBJECTIVE

Cloud services providers are becoming increasingly conscious of the value of protecting citizens against possible privacy abuses, both by private entities and law enforcement agencies. This is illustrated by the constant re-evaluation of the privacy practices and policies of cloud services as they roll out new features and functionalities, and the recent re-definition of their guidelines for cooperation with law enforcement.

Indeed, one of the consequences of the Snowden revelations is the increased level of awareness by Internet users about the little constraints that such agencies face in accessing user data, and the growing recognition of the need to reform the existing procedures in order to incorporate better safeguards against illegitimate or disproportionate interference. But while the need for an overhaul of the current intelligence apparatus was recognized publicly by President Obama in January 2014, [4] the results obtained so far provide limited relief against the angst of unrestricted governmental access to data that motivated campaigners in Congress, [5] and privacy advocates worldwide.

As others have noted, [6] there are two main features calling for a reconceptualization of the relationship between law enforcement: first, service providers and users in the Web 2.0 era lie in the non-rivalrous nature of data stored in the cloud, which makes it impossible for

users to detect any act of breaking into their "digital self"; second, the so called "third party doctrine" [7] enables the US government to compel service providers to grant access to customer data with a mere subpoena (that is, without prior judicial oversight). Due to the exposure of these negative externalities in programs such as PRISM and MUSCULAR, where Internet platforms' backdoors were instrumental for the acquisition of user data by intelligence agencies, users have become more sophisticated in their demand for privacy and data protection, and the market has showed signs of moving to respond to those demands. For example, Apple attracted some criticism by law enforcement agencies when it launched a new encryption policy under its new mobile operating system, iOS 8, indicating that the company will not have access to customer passcode - thus making it impossible for them to respond to government requests for data that is encrypted through that private passcode. [8] Days after this release, Google followed suit with a similar announcement regarding the default encryption of communications in its mobile operating system. [9]

One of the latest manifestation of this trend came on February 16th, 2015, when Microsoft officially adopted the first international cloud privacy standard (certified ISO 27018), which goes beyond its established encryption for data stored in the cloud [10] and promises a number of important features such as: enhanced security protection, including best efforts in the industry and strict confidentiality obligations for anyone processing those data; transparency over the return, transfer and deletion of personal information, including regarding its location and the identity of third party processors; notification about government access to data; and last but not least, no use of data for advertising purposes. [11]

In addition to the protection vis a vis governmental abuses, multiple aspects of consumer privacy, such as the policies adopted by a particular service for data collection, data retention and data use, represent particularly important determinants of consumer demand in the market for cloud services. Ideally, in a competitive market, these elements should form integral part of the supply: if adequately informed, users concerned about disproportionate governmental access to data will migrate towards those "diligent" services. That way, even conceding that law enforcement agencies may force service providers to install backdoors or giving otherwise easy access to data, users will be able to secure a minimum but strong level of privacy protection due to the limited data (or rights over those data) that these companies have at their disposal in the first place.

Yet, what we see is that this dynamic is not fully functioning, as many cloud providers still provide a suboptimal level of protection. This might be indicative of two underlying problems. First, the inability of consumers to understand, or even read, the terms of service of the companies they use. Second, the superior bargaining power of service providers, who as repeat players and providers of essential services are in the position to impose restrictive conditions through standardized contracts that users cannot negotiate. In other words, the combination of significant market power together with a persistent asymmetry of information generates a market failure enabling such companies to force consumers to agree to virtually any kind of contractual arrangements. [12]

Motivated by this situation, the study at hand constitutes an attempt to bridge the information gap by drawing attention to the contractual practices of various cloud services in relation to privacy and data protection. [13]

3. METHODOLOGY

The methodology employed in this study derives from the methodology chosen for the broader Terms of Services and Human Rights Project, mentioned in the Introduction. [14] As a first step, a number of cloud services was identified to match the scope and purpose of this study: the selected services represented three different types of cloud services, and within each type we picked the most popular services based on their Alexa rank. For consistency, only cloud services based in the United States were analyzed, and only the English version of their policies was reviewed.

Secondly, a list of evaluation criteria was compiled on the basis of 18 privacy-related factors. These factors correspond to the most common privacy-related provisions found in the ToS of the sampled services.

Third, an assessment of the ToS of the selected companies was performed against the above mentioned factors list to see which platforms engage in which practices. Those practices that advance user privacy were characterized as "positive" (e.g. platform encrypts data), whereas those that limit user privacy were characterized as "negative" (e.g. platform allows third parties to track users on site). While it should be acknowledged that other competing considerations come into play besides privacy, and many of the "negative" practices might be necessary in order to serve other legitimate interests, the purpose of this study was to focus on the privacy-related protection of ToS. To that end, it identified minimum principles and best practices and simply proceeded to calculate the extent to which those were followed, not considering for instance the impact of those on the ability of firms to innovate or profitably market their products or services.

It is also important to mention that for purposes of this study, "ToS" refers to various types of enforceable contractual agreements between users and companies, including Terms of Use, Terms and Conditions, User Agreement, Privacy Policies, Cookies Policies etc. In doing so, the analysis did not account for internal company rules or other non-binding practices that companies may follow to ensure better protection of users' privacy. This approach was based on the idea that ToS constitute a specific, binding and enforceable commitment to users, while technological or other informal practices can be changed at any time.

Two main challenges were faced in implementing this methodology:

(1) the need to define the standards by which ToS are to be evaluated. While the reviewed providers are all subject to US jurisdiction, the scope and means of privacy protection vary significantly around the globe. When devising the list of factors and to avoid heterogeneity, we attempted to find common ground. To do so, we sought guidance in how privacy is dealt with in various international legal instruments on human rights. These included the International Convention on Civil and Political Rights, the OECD and APEC Privacy

Principles, the Council of Europe Guide on Human Rights for Internet Users and related documents, and relevant opinions of the Article 29 Working Party.

(2) the need to adopt a common definition of cloud services, while at the same time recognizing the different types of services and the potentially different assessment required for each group. According to the National Institute for Standards and Technology, a cloud service is based on "a model for enabling ubiquitous, 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"). [15] For the purposes of this study, the services were subdivided into three groups according to their main activity: (i) storage; (ii) collaboration and (iii) IaaS/PaaS. While the first two groups are mainly addressed to plain users, the services of the third group are targeted primarily to corporate users and are offered in exchange for a fee. The hypothesis that guided this subdivision is that the more similar the services are, the more their practices regarding users' privacy and data protection would coincide.

4. ANALYSIS

This section provides the results of the analysis of the ToS of 12 cloud services, based on a specific list of factors on privacy and data protection (TABLE 1). Those services are 4shared [16], Dropbox [17], Mega [18], Rapidshare [19], Google Drive [20] (with Google Docs etc), Github [21], One Drive [22], Kolab Now [23], Azure [24], Cloudant [25], EC2 [26], Salesforce [27].

TABLE 1: Privacy and data protection, by company

	Storage				Collaboration				PaaS/IaaS			
	4Shared	Dropbox	Mega	RapidShare	Google Drive	Github	One Drive	Kolab	Azure	Cloudant	EC2	Salesforce
Platform does not collect more data than necessary for its operation	○	○	○		○	●	○		○	○	○	○
User is allowed to view, copy,	●		●	●	○/●		●					●

download, or modify all of his or her personal information											
Users allowed to permanently have all of their data deleted within reasonable time upon request	●		○			●	●			○		●
Platform does not store user data for longer than necessary for the operation of the platform or as required by law	○	●	○		○		○	○/●	○	○		●
Platform does not scan or collect data from non-public user content (e.g for ads, prevent malware, spam etc)				●	○		○					
Platform does not track users in other		○			○		○	●		○	○	

websites												
Platform does not allow third parties to collect user data/metadata or track its users	○	○					○		○	○	○	○
Platform does not aggregate or combine data across own or affiliated services					○		○			○		○
Platform does not aggregate or combine data across devices												○
Platform does not share user data with third parties for commercial reasons				●		●	○	●		●	○	○
Platform does not share user data with third parties for processing or to complete an operation of the platform		○		●	○	●	○	●	○	○	○	○

Platform does not share user data with third parties for other reasons (e.g. proposed mergers, protection of assets & staff, etc)		○	○	○	○	●	○	●		○	○	○
Platform does not ask for license on user data that goes beyond the main purpose of the platform			●		○		○			●		●
Platform encrypts or allows encrypted transmission of data			●		●	●	○/●	●		○/●	●	
Platform encrypts stored data			●			○/●			●			
Platform takes additional security measures to protect user data (e.g. protocol on staff access to		●			●		●			●		

user data)											
Platform does not give data to law enforcement for judicial purposes unless there is a legitimate warrant, judicial order or subpoena	●	○	○	○	○	○	○	●	●	○	○
Platform explicitly states it will analyze and/or challenge law enforcement requests		●	○	○	○	○	○	○	●		

Table 1 presents 18 factors on users' privacy and data protection and 12 companies divided in three groups. The symbols represent how the services' policies fulfill that particular factor. The factors are written in a way that expresses a positive or desirable practice. Table 2 then shows the balance between positive, negative and ambiguous/neutral clauses in each service. These percentages were calculated on the basis the total of factors effectively analyzed for each platform, thus giving higher numbers for platforms where the ToS did not offer an answer to each question of our inquiry.

TABLE 2: Distribution of relevant factors in companies' ToS

Service	Positive clauses	Negative clauses	Ambiguous / neutral clauses	Total number of factors analyzed
4shared	50.00%	50.00%	0.00%	6
Dropbox	33.33%	66.67%	0.00%	9
Mega	30.00%	60.00%	10.00%	10
Rapidshare	57.14%	42.86%	0.00%	7
Google Drive	15.38%	76.92%	7.69%	13
GitHub	66.66%	22.22%	11.11%	9

One Drive	18.75%	68.75%	12.50%	16
Kolab Now	75.00%	12.50%	12.50%	8
Azure	42.86%	57.14%	0.00%	7
Cloudant	23.07%	69.23%	7.69%	13
EC2	14.28%	85.71%	0.00%	7
Salesforce	33.33%	66.66%	0.00%	12

4.1 GENERAL REMARKS

A quick look at Table 1 shows that, of all the companies offering sufficient information to make a determination on this matter, a large majority collects more data than necessary for their operation (9 out of 12), tracking users in other websites (5 out of 6) and allowing third party tracking (7 out of 7). Additionally, half of the companies appear to retain data for a excessive period of time, and most services state they share users' data for commercial reasons, processing and/or other reasons. While some of these reasons could be justified, sharing users' data with unidentified third parties runs against the core principle of privacy: the right to have control over their information. For instance Dropbox's terms note that the user gives them permission to access, store and scan user data and that "this permission extends to trusted third parties we work with."

Even more troublesome is the fact that 8 out of the 12 services analyzed do not commit to sharing users' data for law enforcement only upon legitimate judicial order, warrant or subpoena. Quite the contrary: they have in place privacy policies containing vague and potentially problematic terminology: Google for example shares personal information if it has "a good faith belief" that this is necessary "to meet any applicable law, regulation, legal process or enforceable governmental request." This means that the data collected and stored by companies may be disclosed to government agencies outside due process guarantees foreseen by the legal system for decisions that may impact adversely the rights of an individual. However, the fact that two services, 4shared and Microsoft's Azure, commit to disclosing information only when there is a legitimate judicial order, warrant or subpoena, signals that there is room in the market for the adoption of this more "responsible" business practice.

Table 2 also shows some recurring patterns. For example it is noticeable that IaaS/PaaS services scored the worst results (despite their remunerated nature), while the top results come from services classified as collaborative (Kolab Now and Github).

4.2 GROUP 1: STORAGE

This group brings together four storage services. [28] Storage services are those whose primary function is to provide storage and file sharing capabilities. Most of them have both a free and a paid subscription option.

Data collection

One of the key parameters used in this study was the amount of information companies state they collect in the frames of their operation. The assumption was that not all collected information is necessary for the provision of the service. Information collected for statistical analysis or commercial purposes, for example, was deemed not essential. When the relevant policies were not clear about the limits of information collection, they were also considered excessive. As a result, the analysis showed that three out of four services collect more information than necessary for their operation, whereas one (Rapidshare) doesn't give enough relevant information. An example of such policies comes from Mega:

We may also collect information about visits to our website to measure the number of visitors to different parts of the website, to assess user access patterns and otherwise to operate the website.

The silence of the ToS analyzed leaves us in a state of uncertainty as to whether scanning private user content is indeed a common practice in this category of companies. However, it is telling that Rapidshare is the only provider that affirmatively states it will not:

RapidShare does not open or examine the data of its users and the data is neither catalogued by RapidShare, nor is the content listed anywhere. […] We do not open or analyse your stored data.

Relating to data collection, another factor was whether the service tracks its users on other websites. Where technologies can be used for tracking as well as other purposes, such as cookies, it was considered that they track users only when explicitly stated in their policies. As we can see in Table 1, only Dropbox explicitly states it tracks users on other websites and in particular "the web page [the user] visited before coming to [Dropbox] sites."

When it comes to allowing third parties to collect users information or track them on the reviewed services' websites, Mega's and Rapidshare's ToS are silent, whereas Dropbox's and 4shared's ToS are affirmative, providing also specific examples. 4shared for instance allows "Social Media Features," "Widgets" and "interactive mini-programs" to be hosted on its site and collect user data.

Tracking users in other websites is commonly used for serving personalized advertisements. The fact that three out of four storage services do not mention anything in that regard might be revealing of two alternative scenarios: first, these companies have not invested on this type of practice, arguably to preserve maximum trust of their users. Alternatively, and this would be problematic, tracking occurs without any disclosure of the practice to consumers. More research is needed to verify which hypothesis is closer to reality.

Data sharing

A second key parameter in the evaluation concerns the data shared with third parties. Results here are mixed, depending on what is seen as a legitimate ground for sharing. For instance, none of the services mentions sharing user data for commercial reasons (although services in other categories do, e.g., OneDrive, EC2 and Salesforce), and only Rapidshare affirmatively says it won't:

This arrangement [:ToS agreement] prohibits the disclosure of your data by RapidShare itself or third parties. RapidShare may only deviate from this requirement if mandatory regulatory or judicial orders demand this.

Companies may also share data with third parties for reasons that go beyond monetizing. Dropbox's policies state that it will share data with third parties for processing purposes, while Rapidshare explicitly says it won't, and both Mega and 4shared say nothing about it. Three of them specifically mention other reasons, including to protect their assets of in case of a merger.

A generic clause on sharing "for other reasons", such as to protect companies' assets, can be problematic since users are unable to determine the exact conditions under which their data will be disclosed. This also relates to how services give data to law enforcement for judicial purposes: of all the storage cloud services, 4Shared is alone in specifying that data will be disclosed for law enforcement or judicial purposes only upon showing of a *legitimate* warrant, judicial order or subpoena.

Data Protection vis a vis third parties

Only the ToS of one provider (Mega) explicitly commit to the encryption of data, both when stored and when in transit for communications between different users. [29] However, a good example from a security perspective is provided also by Dropbox, which commits in its ToS to special security measures, such as testing for vulnerabilities and alerts when new devices are linked to user accounts.

4.3 GROUP 2: COLLABORATION

The second group includes platforms that offer collaborative functions, sometimes on top of any file sharing and storage capabilities. From the four platforms under consideration, three offer both free and paid services and one just paid services. In this group are the main storage and file sharing services of two integrated companies: Google (with Google Drive) and Microsoft (with One Drive).

The first issue that calls for attention in this group is the substantial difference in the number of relevant factors treated under their policies. Both Google and Microsoft seem to have more comprehensive policies that deal with most of the issues addressed in this analysis. While Google Drive has information on 13 out 18 factors and Microsoft on 16, the other two services - GitHub and Kolab Now - had only 9 and 8 respectively. However, detailed policies do not necessarily reflect better practices regarding users' privacy and personal data

protection. On the contrary: around 77% of Google Drive's and 69% of One Drive's privacy clauses can be considered negative, while GitHub had 67% and Kolab Now 75% of positive clauses (see Table 2).

Data collection

When it comes to data collection and retention, Google and Microsoft appear to collect more data than necessary for the operation of the platforms. The good practice in this respect is offered by GitHub, the only provider to refrain from collecting more data than necessary for its operation. All it requires is the following:

When you register for GitHub we ask for information such as your name, email address, billing address, or payment information. Members who sign up for the free account are not required to enter any payment details.

On another important aspect of data collection, scanning users' private content, negative results came from Google Drive and One Drive. Google's policies clearly affirm that scanning is performed also for commercial purposes:

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

One Drive, in contrast, states it will not scan to target advertising; however, it also warns users that it may deploy automatic scanning of users' content to identify abuses [30] :

We also deploy automated technologies to detect child pornography or abusive behavior that might harm the system, our customers, or others. When investigating these matters, Microsoft or its agents will review Content in order to resolve the issue. [...] We do not use what you say in email, chat, video calls or voice mail, to target advertising to you. We do not use your documents, photos or other personal files to target advertising to you.

Negative results came out also from the analysis of tracking: only one provider affirmatively commits not to track users on other websites. As we have shown in Table 1, most providers are ambivalent about it.

According to Kolab Now policies:

Cookies are only used in so far as they are required for the technical working of the system, and we never use them to track you on third party sites.

Data sharing

One big difference on how users' data is treated by this group of services is related to sharing data with third parties. While Google's and Microsoft's ToS affirmatively state that they will share for commercial purposes, processing or other reasons like mergers & acquisitions or to protect companies assets, in the other two cases there is a specific

commitment to the contrary. However, only one of these two (Kolab Now) explicitly commits to disclosing users' data to law enforcement for judicial purposes only if there is a legitimate warrant, judicial order or subpoena, while the others don't specify the requirements for this type of disclosure.

Data protection vis a vis third parties

Finally, going back to the issue of encryption discussed at the outset: all of the services analyzed in this group commit to encrypting or allowing encryption of data transmitted. Half of the providers also commit in their policies to take additional security measures. Google Drive's policies states:

We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems. We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

4.4 GROUP 3: IAAS/PAAS

The third group comprises cloud services commonly classified as Infrastructure as a Service (IaaS) and Platform as a Services (PaaS). These have different business models than most of the other providers analyzed, as they are offered in exchange for a fee and mainly directed to corporate or other types of organizations (as opposed to individual users).

Data collection

In analyzing the policies of these providers, some common patterns emerge. First, all their ToS are clear about collecting what was considered, for purposes of this study, to be more than necessary for the operation of the service. This seems to suggest that maximal data collection constitutes integral part of the business model of these companies even if they rely on another mechanism (the payment of a fee) to monetize their services. Similar results can be found with respect to tracking, as all providers allow third parties to track or collect data from their users. Cloudant, for instance, states:

We have also engaged with certain third parties to manage some of our advertising on other sites. These third parties may use cookies and Web beacons to collect information (such as your IP address) about your activities on IBM's and others' Web sites to provide you targeted IBM advertisements based upon your interests.

Lastly, as noted previously data retention policies in this group of services followed a similar trend to the other types of services in that only one (Salesforce) committed to not storing data for more than necessary for the operation of the platform or as required by law, while Cloudant and Azure have vague clauses that potentially open the door for a disproportionate retention. By way of example, Cloudant's ToS state:

We will retain and use your registration information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Data use

It is perhaps surprising that all of the analyzed providers explicitly affirm that data with third parties for processing purposes. This is striking because in the other two groups, at least some of the services affirmatively commit to not sharing users' data in those circumstances.

On the other hand, a positive finding is represented by the fact that half of the providers refrain from asking a license on users' content that goes beyond the purpose of the platform. Salesforce policies, for instance, state:

You grant Us and Our Affiliates a worldwide, limited term license to host, copy, transmit and display Your Data, and any Non-Salesforce.com Applications and program code created by or for You using a Service, as necessary for Us to provide the Services in accordance with this Agreement.

Examples of how licenses can be unnecessarily broad is to make the license perpetual, irrevocable, or to ask a license for adaptation beyond the uses necessary for the operation of the services users sign up for. While the two remaining providers in this group offer no information on this matter, these findings might reflect a special care taken by the IaaS/PaaS services when treating corporate information, on consideration of the valuable intellectual property rights, trade secrets or other sensitive information that may be found in their customers' data.

Data protection vis a vis third parties

Perhaps the above mentioned motivation explains also the best practice provided by Microsoft Azure, the only operator which affirmatively commits to encrypt stored data as well as to disclose data to law enforcement only upon legitimate judicial order, warrant or subpoena. In this light, it is interesting to see the contrast between the protection offered by Microsoft's Azure and One Drive, which is not targeted to corporate customers- and displays a notably lower degree of protection. However, the question looms large as to why this good practice is not followed by the other providers in this category.

5. DISCUSSION

There are many ways to read the results of the previous analysis. In this section, some reflections are offered on the extent to which privacy protection is enshrined in the ToS of these major cloud providers.

Terms that appeal to user concerns are more likely to be addressed in ToS: It is interesting to notice that companies choose to address more terms and conditions that have generated controversy or are a common concern among users, as opposed to terms that, despite their importance, have not generated much discussion. For example, issues like user rights to

access, delete or get a copy of their data or the digital and physical security of user data are not clearly addressed, whereas some information on the type of collected data, data retention, data sharing and law enforcement are almost always present in ToS. Considering that government surveillance and sharing of user data with third parties has been constantly in the news and involved in scandals, it is perhaps expected that companies want to reassure users that they have adequate policies in place regarding those issues. This does not mean that user interest is the only factor that sets companies' priorities when shaping their ToS (among others court decisions and the evolution of relevant legal, industry or community standards have a role), but that it is a relevant consideration.

Companies are complacent about law enforcement requests: While most companies discuss how they deal with judicial and law enforcement requests for data disclosure, their policies as described in the ToS are not satisfactory. First, although companies rightly say that they will share data when required by a warrant, court order or subpoena, they often open up the scope to other general "legal processes," a term without specific legal content and therefore potentially too broad. Further, only a handful of companies explicitly state that they will attempt to challenge judicial and law enforcement requests when they think they can be excessive or illegitimate. This is important because such requests are often too broad and complying with them, although legally acceptable, creates an unnecessary risk for user privacy. To be fair, some companies, like Google, while they fail to commit specifically with terms like "legitimate" and "challenge,", they state in their transparency reports that they attempt to narrow the scope of requests. However, it should be noted that transparency reports or other auxiliary documents do not create a binding obligation, and therefore are not sufficient to guarantee user privacy rights.

Companies do not commit to adequate physical and digital security of user data: Considering the line of business cloud services are in, it is surprising that the majority of the companies at issue does not mention encryption policies in their ToS. Although some mention encryption of the data transmitted with SSL, few make the extra commitment of encrypting the data stored on their servers or of providing additional security measures, for example establishing the conditions under which the company's personnel has access to user data. While it is clear that encryption is an additional cost to companies, proper privacy practices should offer a relevant commitment at least as an opt-in choice. Much like law enforcement requests, even though companies may in reality employ detailed security measures, the fact that such a commitment is not included in the binding ToS allows them to deviate at any time, without warning and without liability, thusly offering a low level of assurance.

Many ToS are silent on important issues that affect user privacy: As one can notice from Table 1, companies frequently don't provide enough information on issues that are key to the treatment of user data. To some extent this is understandable because companies may wish to strike the right balance between concise and user-friendly ToS on the one hand, and adequate user protection on the other, considering that overloading the ToS with clauses could have the effect of alienating users from reading and understanding ToS. However, from a privacy perspective, the interest of committing to a high level of transparency and protection trumps that of achieving user-friendliness, which can be achieved by other means

(such as explanatory videos, user-friendly settings panel, and the adoption of standardized icons).

Smaller companies seem to be more respectful of user privacy: An overview of our analysis shows that smaller companies, such as Rapidshare, Github and Kolab Now scored higher than services of larger companies such as Amazon's EC2, Google Drive, Dropbox or Microsoft's OneDrive (even within the same category). This can be attributable to various factors and requires further research. One hypothesis is that smaller companies don't see the same value in capitalizing on user data as bigger companies do or are unable to do so. Another reason might be that smaller companies try to differentiate themselves from competition by offering users better privacy options (e.g. KolabNow markets itself thusly: "Want to ensure that your data is stored only in a single legislation, with highest barriers to data disclosure? Kolab Now is that service"). Moreover, smaller companies may as a matter of ethics, culture or mission, consider privacy and important consideration, which might make them more willing to comply with good privacy policies.

6. CONCLUSION

The purpose of this paper was to study the privacy terms and conditions cloud services ask users to agree to, and determine whether they offer sufficient protections. The study yielded a wide range of results, identifying both good practices and problematic situations. Overall, it is clear that the power asymmetry between users and companies allows companies to maintain with a certain degree of abusive practices, despite the growing sensibility of users to the infringement of their privacy. For this reason, more systematic attention should be given to terms of service to appreciate the scale of the problem of contractual imbalance, which this paper has merely pointed to. Greater awareness and control are particularly important considering the vast amount of data (often of sensitive nature) that cloud services store and process.

---

[1] Lecturer, University of Leeds Law School. E-mail: k.stylianou@leeds.ac.uk

[2] Research Associate, Center for Technology and Society, FGV Law School. E-mail: jamila.venturini@fgv.br

[3] Assistant Professor, Tilburg University Law School. E-mail: n.zingales@tilburguniversity.edu

[4] White House, Office of the Press Secretary, "Presidential Policy Directive" of 17 January 2014. Available, http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities; Office of the Director of National Intelligence , "Intelligence community's implementation of Section 4 of Presidential Policy Directive/PPD-228" (2015). Available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

[5] D. Roberts and D. Rushe, "Proposed changes to US data collection fall short of NSA reformers' goals". *The Guardian* (3 February, 2015). Available at

http://www.theguardian.com/us-news/2015/feb/03/proposed-changes-us-data-collection-nsa-reformers

[6] C. Soghoian, "Caught in The Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era, 359 *Journal on Telecommunication & High Technology Law*". (2010) 379, 384

[7] See United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[8] S. Frizell, "The FBI and NSA Hate Apple's Plan to Keep Your iPhone Data Secret". *Time* (27 September 2014). Available athttp://time.com/3437222/iphone-data-encryption/

[9] "Google to Boost Android Encryption, Joining Apple". *Security Week* (18 September, 2014). Available at http://www.securityweek.com/google-boost-anroid-encryption-joining-apple

[10] C. Duckett, "Microsoft confirms encryption across services". *Zdnet* (5 December, 2013). Available at http://www.zdnet.com/article/microsoft-confirms-encryption-across-cloud-services/

[11] B. Smith, "Microsoft adopts first international cloud privacy standard". *Microsoft Blog* (16 February, 2015). http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/

[12] C. Smith, "7500 Online Shoppers Accidentally Sold Their Soul to Gamestation". *Huffington Post* (17 June, 2010). Available athttp://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html

[13] See also D. Stitilis, & I. Malinauskaite, "Compliance with basic data protection principles in cloud computing: the aspect of contractual relations with end-users". *European Journal of Law and Technology*, Vol 5, No. 1., 2014; K. Stylianou, "An Evolutionary Study of Cloud Services Privacy Terms",*John Marshall Journal of Computer & Information Law, Vol. 27, No. 4, 2010*

[14] Human Rights and Online Terms of Service: Report of Findings (Direitos Humanos na Internet e Termos de Uso: Relatório] (forthcoming, FGV Press 2016).

[15] P. Mell & T. Grance. "The NIST Definition of Cloud Computing". Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce. Gaithersburg, MD 20899-8930: National Institute of Standards and Technology (September 2011). Retrieved January 28, 2014, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[16] The analyzed version of the Terms of Service was from April 6th, 2012. Both the Privacy Policy and the DMCA Policy didn't show the date of their last update.

[17] The analyzed version of the Terms of Service was from January 22nd, 2015 and the Privacy Policy from February 13th, 2015. Both the Acceptable Use Policy and the Government Data Request Principles didn't have information on their last update.

[18] The analyzed version of the Terms of Service was from January 15th, 2015.

[19] RapidShare ended its services in March, 2015. The analyzed version of the Terms of Use and Privacy Policy didn't have information on their last modification date.

[20] The analyzed version of the Terms of Service was from April 14th, 2014 and of the Privacy Policy from December 19th, 2014.

[21] The analyzed Terms of Service had no information on its last modification as well as the Privacy Policy.

[22] The analyzed Terms of Service was from December 12th, 2014.

[23] The analyzed version of the Terms of Service was from July 25th, 2013 and of the Privacy Policy from June 1st, 2014.

[24] The analyzed version of the Privacy Statement was from October 2014.

[25] The analyzed version of the Terms of Service didn't have information on its last modification and the Privacy Policy was from November 1 st, 2014.

[26] The analyzed version of the Terms of Service was from December 23rd, 2011 and the Privacy Policy didn't have information on its last modification.

[27] The documents analyzed were the Master Subscription Agreement, from September 1st, 2014 and the Privacy Statement, which had no information on its last modification.

[28] Mega is the successor to the popular Megaupload service that opened in 2005 and operated through 2012.

[29] While Mega states it encrypts stored data and data in transit (through User Controlled Encryption) it doesn't clarify whether user personal information are stored in encrypted format as well or if this applies only to user data.

[30] For full disclosure, it should be clarified that although scanning private content may provide substantial benefits for consumers (for example, to detect phishing or malware), this practice was considered privacy-intrusive when imposed by default (i.e., without a specific request in this sense).