Confidentiality and Data Sovereignty in the Cloud

ABSTRACT

To the extent that most of the content and software application are only accessible online, users have no longer control over the manner in which they can access their data and the extent to which third parties can exploit it. The main issue with Cloud from a data protection perspective is control on users' data.

1. INTRODUCTION

Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. The relationship between data protection and ICT developments changes all the time. This has been demonstrated by the challenges of Cloud Computing to data protection, particularly in the management of cross-border data transfers.

Businesses must balance the flexibility and potential cost savings of cloud computing with the risks inherent in storing data off-site, beyond the company's direct control, and possibly even in a foreign country with different laws. Cloud Computing has become a multibillion dollar business globally, it's clear that organisations are finding ways to protect their data in the cloud.

Although Cloud Computing constitutes a great opportunity for small start-ups to compete in the market for online services without the need to make massive initial investments, exporting all their infrastructure and data into the Cloud is decreasing the capacity of users to control the manner in which their resources are being held. Given that everything can be stored, processed, or executed on any computer system regardless of its whereabouts, most of the means of production are increasingly owned or at least *de facto* controlled by large companies.

The trend is clear. Resources are moving away from end-users, towards centralized systems that possess huge processing power and storage capacities. Users' devices are devolving from personal computers to laptops, smart phones or integrated devices whose main function is to access particular sections of the Cloud through browsers or mostly dumb applications. While front-end processing is perhaps becoming slightly more common in the form of in-browser application, data storage is heavily biased towards centralized back-ends. The implications are many: users are giving away their content under a false ideal of community; they are giving away their privacy for the sake of a more personalized service; they are

giving away their rights in the name of comfort and accessibility; but, most importantly, they are giving away their freedoms and, very frequently, they do not even realize it.

By analysing the way the Internet has developed over time, it will draw attention to the fact that the Internet has been and is evolving into an increasingly centralized architecture that might strongly impair the rights of end-users and endanger the privacy and confidentiality of information stored into the Cloud.

These problems are exacerbated by the international character of the Cloud, which extends over multiple jurisdictions but does not account for national boundaries. Regulating the Cloud has turned out to be an extremely challenging task, which has not yet been properly addressed by the law. With this paper, we do not purport to come up with a solution, but merely to propose a series of recommendations on how to address these challenges by public and private means.

2. THE EMERGENCE OF CLOUD COMPUTING

DEFINITION OF CLOUD COMPUTING

Given its recent and very fast adoption in everyday language, the actual definition and scope of Cloud Computing are still under debate. In part, this stems from the fact that Cloud Computing does not actually provide much in terms of new technology, but rather an alteration of the use of older technology to serve new types of business structures. The underlying idea of Cloud Computing dates back to the 60's with the concept of 'utility computing' - the dynamic provision of computing resources according to the client's needs. As for the term 'Cloud Computing', telecommunication operators already employed term 'cloud' in the early 90's as a means to demarcate the boundaries of responsibilities between users and service providers.

The problem is, however, that policy is inherently malleable. In practice, there is no privacy policy, uptime assurance or data protection mechanism that can eliminate the added operational risk created by shifting to a third party infrastructure. At best, the risk can be minimized by not storing sensitive data and mitigated by not relying on one single cloud platform.

3. LEGAL ISSUES OF CLOUD COMPUTING

It takes only very basic examples to show the danger of over-centralization in the sphere of the Internet. In addition to the most common examples, such as Google and Facebook, there are a very large number of actors whose operations are crucial in the everyday life of many Internet users. The more the level of dependency increases, the more the effects of not having control over the content or infrastructure become apparent, although some of the implications might remain very subtle.

3.1 CENTRALIZED CONTROL

Today, no matter how much one tries to keep it secret, there exist many mechanisms or devices that collect personal data and communicate it to third parties without the consent of the data subject. Most often, however, it is actually the user who willingly communicates information to a variety of interested parties.

Security risks, privacy concerns, lack of interoperability and user's lock-in are only few of the problems that might derive from the fact that users do no longer have control over their own resources. Indeed, as many users no longer control nor understand their infrastructure, they are increasingly controlled by those who do know how to control the infrastructure - and by those who own it.

The problem arises when the information given to separate (and apparently independent) services is actually aggregated together by one single entity (either because it is the common provider of said services, or because it has acquired the data from third parties). Even though information had been voluntarily provided by users, aggregated data might provide further information about users, which they did not necessarily want to disclose.

Technically, this is already a possibility, and, as a matter of fact, this is already part of reality. Increased demand for clear privacy settings in software and understandable privacy policies appears to be slowly improving this gap in awareness.

Profiling is necessary for Google to know what users want, so as to eventually offer them the most personalized results and the best kind of advertisements. The greater the user-base, the most accurate the profiling can be, and the higher the profits that can be extracted from a system of customized advertisement dependent upon the interests of each individual user. In this case, the fact that the end-users do not pay for the service means that they themselves are the product being sold, or rather, statistics about them are. There is no reason to assume malice here, but there is reason to draw attention to privacy concerns.

Hence, although the majority of Google's services are offered for free, users pay - willingly or not - with their own data, which is only later turned into profit by Google AdSense or other forms of advertisement. When users search for something on the web, Google can learn about their interests; when users read their emails on Gmail, Google can learn more about their personal or professional life; when users check out a location on Google Maps, Google can learn where each user has been or wants to go. The greater the scope of the Cloud, the greater is the amount of data that can be gathered together and the more valuable is the information that can be obtained with the processing and correlation of such data.

While this is likely to help Google increase its profit, the collection and processing of user data into a common integrated framework can also benefit the users when it comes to increasing the quality of the service. Many users are therefore not merely agreeing, but even eager to share their personal data and information with Google in order to obtain a more customized and integrated service. Google Calendar is more valuable because it can be integrated with Gmail for e-mail reminders and notifications and with Orkut and Google+ for discovering new events and remembering the birthdays of some friends. As the value of a service increases not only with the number of users connected to that service but also with its degree of integration with other services, the wider is the portfolio of services offered by Google, the most users will be attracted to these services.

3.2 PRIVACY & CONFIDENTIALITY

There is an inherent security risk in the use of the Internet to transfer sensible information and personal data. As a general rule, information wants to be shared, and most of the value that can be extracted from it emerges from the usage and communication thereof. Given the global scope and international character of the Cloud, these risks have considerably increased with the deployment of Cloud Computing. Every bit of information that has been published into the Cloud becomes accessible from anywhere and at anytime, yet, once it has been exported into the Cloud, users lose the possibility to control their data, which can no longer be accessed, edited or retrieved without the consent of the Cloud provider.

Likewise, even though users are made to access the services by password, unless there is file system level encryption of the data with a key held only by the user - which is impractical in most cases - the operator of the service or anybody else who gains physical access to the servers can peer into the stored data.

3.2.1 PRIVACY RISKS / CHALLENGES

Cloud services do not present unique issues in data protection, but they do add to the complexity of existing issues, especially in relation to cross-border data transfers. For instance, the cloud provider may decide, for technical network efficiency reasons, to transfer data from one data centre to another, and these data centres may be located in different countries, or under the control of different jurisdictions. Furthermore, another risk regarding data sovereignty is the sharing of resources in the 'public cloud'.

To date, few jurisdictions have attempted to draft regulations expressly designed to regulate the provision of 'cloud' services. This probably reflects both the broad range of services that fall within the concept of 'cloud', as well as the flexibility of scope within existing regulatory concepts.

Overall, increased interoperability of laws and regimes is important to reduce the likelihood of friction over cross-border data flows for cloud services. Security concerns are born from a series of data residency / privacy and industry-specific regulations that describe how data must be treated.

<u>Data Residency / Privacy Laws</u>

- Data residency / privacy legislation in specific countries or governmental associations such as the European Union (EU) prescribes that sensitive or private information may not leave the physical boundaries of the country (residency) and that information should not be exposed to unauthorised parties (privacy).
    - Example of legislation includes:
        - ✓ The United Kingdom Data Protection Law (Data Protection Act 1998)
        - ✓ The Swiss Federal Act on Data Protection
        - ✓ The Canadian Personal Information Protection and Electronic Documents Act
    - The EU Data Protection Directive is also an important piece of data privacy legislation that regulates how data on EU citizens needs to be secured and protected.
    - The Data Protection Office acceded to the Council of Europe's Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) on 17 June 2016 at Strasbourg, France. The convention is the first and only international legally binding instrument dealing explicitly with data protection and had 48 signatories including 47 Council of Europe Member states as well as Uruguay until Mauritius became the 49th State Party. The treaty entered into force on 1 October 2016 in Mauritius.
    - Mauritius is positioned as one of the leading democracies in Africa and the accession to Convention 108 is also an expression of the will of my office to show its unflinching commitment to democratic principles including data protection.

- As part of Vision 2030 Blueprint which stipulates that "data protection legislations need to be compliant with international best practices", the Data Protection Office has adopted the position to partly meet this target with the ratification of Convention 108. Additionally, with the Amendment Bill to the Data Protection Act (2004) submitted to our parent Ministry, this office will be fully compliant with Vision 2030 Blueprint as this new bill will also align our existing Data Protection Laws with the new 2016 EU Directive.

Industry-specific compliance requirements

- Industry-specific compliance requirements covering a specific industry, type of business or government agency prescribe that the appropriate treatment and security of private or sensitive information needs to be taken.

Third Party Obligations

- Agreements among business partners that outline how a party such as a contractor or vendor will handle and treat private or sensitive data belonging to another organisation.
- Such agreements often hold the external party accountable for securing the data in the same fashion as the owner of the data, including adherence to all residency, privacy and compliance requirements**.**

In view of all the residency and compliance requirements that companies face, it's a challenge to strike a balance between safeguarding data and attaining maximum benefit from cloud services.

It's simply not an option to place clear text data in the cloud, as this would violate the data protection principles in a variety of ways.

- The cloud provider may process or store data on servers (either primary or in backup locations).
- Employees of the cloud provider have access to the data as they perform routine processes and maintenance, such as data backups or server upgrades, and these employees are frequently located in other regions.
- This incidental access though necessary under the cloud provider's service level agreement (SLA), still violates strict policies or regulations covering who is authorised to view or handle the data.
- Cloud providers rarely accept full accountability in their SLAs for the security of their customers' data, leaving the customers with full liability in the event of a breach.

The issues discussed above largely stem from data being "in the clear."

Anyone who can access the data, whether they are authorized to do so or not, can clearly see the meaning and values of the data. The way to resolve this problem is to “obfuscate” the data – that is, make it unreadable or meaningless so that if the data is breached, it’s unusable by the intruder. **[Making use of ENCRYPTION]**

The issue of consent

- According to our Data Protection Act (DPA), consent can only be given by data subjects. Therefore, companies acting as data controllers usually do not have the "lawful authority to disclose the data" which they process for e.g. commercial purposes.
- Organisations can normally only disclose data upon prior presentation of a judicial authorisation / warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required.
- Data controllers cannot lawfully provide access or disclose the data to foreign law enforcement authorities that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view.
- It is imperative that data transfers have a specific and legitimate legal basis in the law of the requested Party (e.g. judicial authorisation / warrant), that the principles of necessity and proportionality are respected and that no large-scale access to personal data is permitted. An additional protocol to an international Convention that would appear to provide for access to data stored on computers abroad by applying the law (or the definitions of consent) of the searching party would be in violation of the Data Protection Act.

3.3 TRANSNATIONALITY

The international character of the Cloud introduces an additional layer of complexity to an already complex problem. Information stored in the Cloud can be subject to a variety of different laws according to the location where it is stored, processed or transmitted. In order to provide a service to end-users, Cloud providers might avail themselves of the services of different Cloud providers located in different jurisdictions. In addition, regardless of whether or not the service is being partially outsourced, data is frequently transferred from one data centre to another in order to be processed across multiple jurisdictions. This is generally done on the basis of technical constraints and on the grounds of network efficiency, but also depending on legal or economic factors (e.g. taxation, hardware cost or price of electricity). As a result, it is often difficult to determine in advance and with certainty the actual location of information stored in the Cloud: a file being served from Luxembourg at one moment could be served from the Philippines at the next. Each jurisdiction may have pros and cons in terms of legal environment.

The huge amount of data stored outside of national boundaries has become a critical issue that is directly related to the problem of effective jurisdiction - i.e. the question of government control over domestic data. While government control can be exerted over information stored within the national jurisdiction of a country, it can be extremely difficult to practically enforce after the data has been exported into the Cloud. The reason is that it is almost impossible to provide a definition of what constitute 'domestic data'. Data, as such, does not have any nationality but merely inherits the law of the territory in which it is located.

A crucial problem that emerges from the international character of the Cloud is the issue of forum-shopping. Different servers and data-centres located around the world can be used to take advantage of certain laws and/or to circumvent others. Unless it has been contractually precluded to do so, a Cloud provider with data-centres in more than one jurisdiction could theoretically move information from one jurisdiction to another in order to benefit from the most favourable laws. This can be used, for instance, as a means for any service provider to bypass domestic regulations on data protection.

In a context designed not to take into account national boundaries and where everything can travel from one place to the other in a completely transparent manner, the real challenge is to determine who can exert control over what. Moreover, given that data can transfer from one Cloud to another and from one jurisdiction to the other, different laws might apply to the same bits of information at different moments in time.

4. RECOMMENDATIONS

4.1 PRIVATE MEASURES AND LEGISLATIVE LIMITATIONS

Yet, the law does not seem able to follow the pace at which Cloud Computing is evolving. Eben Moglen points out that Cloud Computing can never truly be regulated, as any regulation of the Cloud will be pre-empted by a change in the way the Cloud is defined, or in which jurisdiction it operates. 'The cloud means that we can't even point in the direction of the server anymore' he states, adding that:

'You can make a rule about logs or data flow or preservation or control or access or disclosure but your laws are human laws and they occupy particular territory and the server is in the cloud and that means the server is always one step ahead of any rule you make.'

The legal framework is unable to deal with the flexible and dynamic character of the Cloud. The length of the legislative process cannot compete with the speed at which private actors can identify and rapidly implement technical or contractual mechanisms to avoid the constraints formerly introduced by the law.

4.2 INTERMEDIARY LIABILITY AND RESPONSIBILITIES

SLAs (Service Level Agreements) traditionally contain wide disclaimers of liability that serve to protect the service vendor. The dynamic character of the Cloud is such that any service provider could decide at any given time to out-source part of its infrastructure and operations to third-party providers, without ultimately informing the other parties to the contract. Although the operation is generally not visible to end-users, it might nonetheless affect the quality and reliability of the service as a whole. In order to preclude any responsibility in the eventuality of failure, most of the services provided to end-users are offered under specific SLAs that stipulate that the service provider cannot be held responsible or liable for the activities performed by third-party contractors. While these can be justified for business reasons, they should stand out as a warning for end users to avoid these services even though they do not currently realize the dangers they entail.

Users are thus left without direct recourse against the other actors involved in the actual provision of the service, which are not necessarily informed of the terms and conditions of the end-user agreement.

4.3 PRIVACY ENHANCING TECHNOLOGIES AND DATA PROTECTION

SLAs could be developed to better reflect the privacy and confidentiality concerns of users and smaller vendors. Yet, SLAs and privacy policies are useless in the face of events which are irrevocable, such as the exposure of private data.

A strong step towards data protection and user security could be made if service vendors were to start offering privacy-by-design by default. In the meantime, user education and public awareness projects could go a long way towards increasing security on the user end.

The problem is that the risk of private data being illegitimately accessed or stolen cannot be resolved exclusively at the service end. Asides from the implementation of stronger security mechanisms, it would be ineffective to protect users' data by providing encryption at level of the service, since the key would ultimately be stored in the same place as the lock. The risks derived from losing control over the infrastructure can be mitigated in different ways. One way consists of using Cloud-level server virtualization but insisting on the use of on-disk encryption with remote key management, or other privacy enhancing methods. Another way to mitigate those risks is to abstract storage and computational capacity in such a way that data can be hosted securely on a remote host with specific access keys that are only available to one user (so that processing can be done arbitrarily at any given time by only that user). Essentially, this amounts to formalizing the Cloud not as a service to dumb client devices but as extensions of smart client devices. These clients can in turn become dynamic servers, controllers of their own data. Various arguments have been made about the complexity of strong encryption and privacy technologies and how average users have little interest or ability to apply them. However, this claim has been taken at face value with remarkably little scrutiny. Conversely, smaller networks catering to more local communities could distribute the risk and limit the scope of potential damage.

4.4 OBLIGATIONS OF DATA CONTROLLERS UNDER DPA

Under the Data Protection Act 2004, data controllers (i.e. the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing personal data) have responsibilities and obligations related to the processing they undertake.

- The data controller is thus required to implement organisational measures to protect personal data against unauthorised disclosure or access.
- The data controller should ensure that the data is necessary for an investigation and is disclosed on a need to know basis.

- For transfer of personal data abroad, the data controller is also required to seek the written authorisation of the Data Protection Commissioner.
- Retention period depends on the purpose of the processing of the personal data as per section 28 of DPA. The duration which has to be determined by you must be reasonably justified.
- Section 27 of DPA explains the shared legal responsibilities between a data controller and a data processor (the cloud provider). Hence, the data controller must ensure that any selected cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organisation.
- Encryption is recommended for the transit of data from your company to the cloud provider.
- The country where the cloud provider is operating should have data protection principles in force or otherwise abide by contractual data protection standards.

You will need to have a contract with the cloud provider that covers the following points amongst others:

- Continuity of service, backups and integrity,
- Certification such as ISO 27001 compliant (which is not mandatory, but essential),
- Auditing of the cloud provider by third party,
- Appropriate access rights are provided to officers of your company for creation, amendment and deletion of data with audit trails,
- Termination of contract,
    - Ensure that all personal data are returned to you and no copies are kept at the cloud provider.

4.5 PEERS-TO-PEER ALTERNATIVES, INTEROPERABILITY AND NETWORK NEUTRALITY

The emergence of P2P alternatives to centralized services has encouraged some of the dominant players to introduce new barriers to entry. If consumer lock-in is no longer sufficient to eliminate competition, the solution is to attack the infrastructure of the Internet, by acquiring priority access to the network. That way, it becomes impossible for others to compete on equal grounds, because regardless of the quality of the service, it will always be slower, and therefore less valuable. In order to preserve competition in the market, net neutrality should therefore be respected. This can be achieved either by regulating the extent to which private parties can operate ex-ante (e.g. by introducing an obligation of non-discrimination), or by regulating the market ex-post with the tools that are already available under competition law.

5. CONCLUSION

Cloud computing is a new model of computing fuelled by the shift of control from end-users towards increasingly centralized services providers. There are many consequences to the deployment of cloud computing: some intended, others unintentional; some good, and others bad. Many are already noticeable and measurable, while others can only be foreseen by analysing the trends that have been set. The advantages offered by Cloud computing are clear: infrastructure providers can benefit from strong economies of scale, whereas Internet service providers can benefit from enhanced flexibility and scalability of costs. From the perspective of end-users, the main advantages are the possibility to access data from anywhere and at any time - regardless of the device they are connected from - and the ability of avail themselves of the computing power and storage capacity of the cloud. Further, it allows clients to outsource the obligation of maintaining complicated infrastructure and having to maintain up-to-date technical knowledge, while externalizing the cost of purchasing and running the infrastructure.

This does not, however, come without costs. Exporting data to the cloud means that users can no longer exercise any kind of control over the use and the exploitation of data. Data stored in various data centres can be processed without the knowledge of users, to be further redistributed to third parties without their consent. If everything has been stored in the cloud, cloud providers can ultimately determine everything that users can or cannot do. As most Internet users are no longer in charge of their own data and are no longer capable of managing their own infrastructures of production, storage, and distribution, the control is all in the hand of few corporate entrepreneurs.

After the industrial revolution governments were urged to exercise their authority for the creation of labour and consumer protection laws, and are today faced with a similar situation as regards to the digital revolution. The claim that governmental intervention has become necessary in order to promote civil liberties and to protect fundamental rights on the Internet is not unfounded. At this point in time, however, the power dynamic is not yet so set in stone that structural changes cannot remedy the problems providers and users are faced with. P2P technologies and protocols, open standards with good interoperability mechanisms, strong encryption made widely available to users, better service level agreements and policies amongst cloud providers, greater awareness of privacy and data protection issues amongst users are amongst the methods which can be employed to reduce the risks inherent in Cloud Computing, and return the Internet back to its distributed origins, lest it rain.

Data protection law requires that data security is safeguarded when processing personal data. Confidentiality, availability and integrity of data must be ensured by means of appropriate organisational and technical measures.

These also include the protection of systems and data from the risks of unauthorised or arbitrary destruction, arbitrary loss, technical faults, forgery, theft and unlawful use, as well as from unauthorised modification, copying, access or other unauthorised processing. Ultimately, the data controller remains legally responsible for the observance of data security, even if he processes data on a third party's (cloud provider) appliances.

Thank You.