# Cloud computing requires a new approach to privacy and security

A single 'responsible party' has to be identified to protect data at all times, regardless of where and by whom data is processed in the cloud.

By **Wim Nauwelaerts** and **Pauline Le Bousse**.

Last July it was reported that a hacker had broken into the email account of an employee of social networking site Twitter, giving the hacker indirect access to Twitter's documents through Google Apps. Twitter uses Google Apps for a range of web-based services such as email, word processing and spreadsheets, and to store its company data "in the cloud". As a result of the breach, the hacker was able to expose Twitter's business information as well as personal data relating to the company's employees (and even their family members). Luckily for Twitter and its employees, apparently the hacker just wanted to make the point that no one's data are safe on the Internet, which is why he sent some of the hacked data to a couple of technology news blogs. The Twitter case is yet another illustration of the growing concern about data privacy and security in the context of what is now often referred to as "cloud computing".

## So what is cloud computing?

Many attempts have been made to define "cloud computing", but the definition of Ontario's Information and Privacy Commissioner Dr Ann Cavoukian probably captures the essence of the phenomenon. Cavoukian describes cloud computing as "a fundamental shift in how data are managed and processed. Rather than running software on a desktop computer or server, Internet users are now able to use the 'cloud' – a networked collection of servers, storage systems, and devices – to combine software, data, and computing power scattered in multiple locations across the network." Put simply, cloud computing refers to a remote computing model which obviates the need to install software and hardware or store data on one's own computer or devices. Or, as Oracle founder CEO Larry Ellison recently noted, cloud computing is "nothing more than a faddish term for the established concept of computers linked by networks".

There are different cloud computing models in use today. Through cloud computing, software can be offered as an online service (software as a service, or "SaaS"). In that case, a software provider licenses an application to users for use as a service on demand. The application typically runs on the provider's cloud infrastructure (for example networks and servers), providing for a complete cloud computing experience. In the case of platform as a service (PaaS), the user relies on the provider's cloud infrastructure as the main or sole solution to run its own applications. Another form of cloud computing is infrastructure as a service (IaaS), where the user combines the cloud provider's infrastructure with its own or other computing infrastructure to deploy its applications.

## The pros

Cloud computing arguably offers several advantages from the viewpoint of users as well as service providers. For users, cloud computing can offer an affordable alternative to conventional computing models that require significant investments in IT resources and infrastructure. In addition to cost savings in terms of IT infrastructure, the software applications available through the cloud are often free or cheaper than comparable desktop products. Moreover, users can access cloud computing services from almost any location or device and in the event of hardware failure, users' data remain available in the cloud. By providing their services through the cloud, providers can easily monitor their services and keep them up to date. Since users do not receive any hard copies, it is also easier for cloud providers to protect their technology against piracy and reverse engineering. If a user violates the provider's terms of use, access to the service can be denied and the user's account can be terminated in a heartbeat. Last but not least, many providers of "free" cloud computing services (such as webmail) seize the opportunity to monetise users' information by including (targeted) ad- vertisements in their offerings.

## The cons – from an EU privacy perspective

The ubiquitous and dynamic nature of cloud computing services – with data being stored and processed remotely in the cloud – makes those services particularly vulnerable from a data protection and privacy perspective. Data security and privacy threats exist due to the fact that information (including personal data) is stored and processed remotely, usually without users knowing where the data actually reside. The data breach involving Twitter is only one example of individuals' privacy being compromised as result of cloud computing services, and it can be expected that more of these breaches will occur as cloud computing services become more popular.

The real problem is that existing laws and regulations are not always suitable for dealing with the specific data protection and privacy issues raised by cloud computing. In Europe, for instance, users' data privacy will be protected by the EU Data Protection Directive (95/46/EC), which has been transposed into the national laws of all EU member states. However, the EU Data Protection Directive was written at a time when the Internet was still in its infancy. Therefore, applying the traditional data protection and privacy principles to cloud computing services is a challenge, to say the least. What follows are some of the difficulties that users, cloud providers and authorities may encounter when applying existing data protection and privacy rules to data in the cloud:

1. EU data protection rules only apply to the "processing of personal data". Although this concept is typically given a broad scope of application, in the context of cloud computing it may not always be straightforward to determine whether or not a particular cloud provider is actually processing personal data (for example, in the case of infrastructure as a service). There has also been considerable debate about whether or not collecting IP addresses (for example by a cloud provider) constitutes processing of personal data.
2. Another issue relates to the fact that in many cases it has become more difficult to locate personal data in the cloud, especially if replicas of users' data are kept in several places. EU data protection rules apply to personal data that are being processed in the EU, so for the application of these rules it is crucial to establish where the data processing takes place. Sometimes the cloud provider's terms of use or privacy policy will shed light on this question, for example by stipulating that users' data will not leave the EU. However, if a cloud computing service involves a multitude of providers, determining which cloud provider is subject to EU data protection rules for what data processing can prove to be a Herculean task.
3. Even if it is possible to identify which cloud provider is subject to EU data protection rules, this does not necessarily mean that the cloud provider is responsible for the processing of personal data under EU data protection rules. In the EU, the data controller, that is the person who determines both the purposes and the means of the data processing, will be responsible for complying with EU data protection rules. In many cases, a cloud provider will only process personal data on the instructions of the user, who will be considered the data controller. However, in the case of platform as a service, a user typically does not have any control over the means used to process the data. Consequently, data protection authorities could take the position that both the user and cloud provider are data controllers liable under data protection law. In addition, a cloud provider may fall within the ambit of EU data protection rules if the provider analyses users' personal data for purposes of behavioural advertising.
4. EU data protection law restricts transfers of personal data to non-EU countries. If the country of destination is not recognised as offering an adequate level of data protection, the parties involved in the transfer will usually be required to put in place a contractual framework to ensure that the data remain protected. In practice, cloud providers will often move users' personal data from one jurisdiction to another or transfer the data to other cloud providers outside the EU. From an EU data protection perspective, this cross-border data flow may become problematic if the cloud providers involved have not carefully considered on which legal basis the data will be transferred outside the EU.

## The need for an alternative approach to DP/security

It is clear that the particular nature of data processing in the cloud, the multiplicity of stakeholders involved as well as the difficulty of locating data in the cloud can impose considerable hurdles when it comes to applying traditional EU data protection principles. Therefore, regulators, data protection authorities as well as cloud providers should perhaps consider alternative ways to tackle data protection and privacy issues in connection with cloud computing services. Such an alternative approach could, for example, focus on:

a) **Cloud providers** should consider building – where appropriate – privacy, security and confidentiality-enhancing features into the product – and service design of their cloud infrastructure, applications and software. For example, cloud providers may want to adopt encryption technologies that apply by default, reducing the risk of privacy exposure in case of a data breach. They could also implement data minimisation applications to ensure that personal data are only stored or otherwise processed if necessary, and that databases are regularly purged or anonymised.

Contrary to what the name indicates, privacy by design does not stop at the design stage. Privacy impact assessments should be conducted by independent privacy experts throughout the cloud infrastructure's lifecycle to ensure that privacy enhancing features are updated and adjusted when needed. The privacy and security by design concept is already envisaged to some extent in the current EU data protection framework and has been endorsed by most data protection authorities in the EU. Last year, the UK Information Commissioner's Office, for instance, issued a comprehensive set of recommendations for better data protection through the implementation of privacy by design. In line with the views adopted at the EU level, the UK Information Commissioner's Office recommends that both privacy and security risks should be integrated in a common risk assessment approach.

b) **Users** are likely to raise privacy concerns if they are no longer in control of what happens to their personal data in the cloud. It is therefore essential for cloud providers to adopt a user-centric approach to users' identity and data management. Users should be given the opportunity to provide – or refuse – their informed consent to the processing of their personal data whenever cloud computing services require such processing. In the case of cloud computing services that involve different stages of data processing, this may imply a continuous dialogue between users and cloud providers to ensure that proper consent is in place at all times.

Cloud providers should also use secure identity management systems to avoid the hacking of users' accounts (which apparently happened in the Twitter case). However, with the multiplication of users' devices and cloud computing services, and the increase in security measures for each service (including, for example, biometrics), it may become impractical for users to maintain multiple security credentials and accounts. Cloud providers should therefore consider user-friendly alternatives to effective identity management, such as single sign on, especially when cloud computing services involve more than one provider.

c) **The current EU data protection principles on data transfers** outside Europe are based on a (rebuttable) presumption that jurisdictions outside the EU do not always protect personal data sufficiently.

As this jurisdictional approach is difficult to apply to cloud computing services, the question arises whether there is an alternative, more suitable method for dealing with cross-border data flows in the cloud.

Canadian privacy law has opted for an organisation-to-organisation solution for data transfers that is not based on the concept of adequate data protection in the country of destination. Under Canadian law, each organisation is responsible for personal data in its possession or custody and remains accountable for data sent to third parties for further processing. The organisation is required to use contractual or other means to ensure that the third party processor provides protection comparable to the level of protection the personal data would receive if they had not been transferred.

Applying this approach to cloud computing, it may not be inconceivable to have a single "responsible organisation" accountable for making sure that personal data in the cloud are protected at all times. This "responsible organisation" could, for instance, be the (first) cloud provider with whom a user enters into a service agreement. The responsible cloud provider would subsequently have to verify that third party processors (for example other cloud providers) have effective security measures, policies and processes in place to ensure that the data are properly safeguarded.

## The way forward: regulation or self-regulation?

It looks unlikely that in the short term European regulators will amend existing data protection rules to address the privacy and security issues posed by cloud computing. It seems more plausible that in the near future data protection authorities in Europe will publish (non-binding) guidelines on how to deal with these issues. Such guidance may be provided at national or EU level (for instance via the Article 29 Working Party, which is made up of representatives from the EU member states' data protection authorities, the European Data Protection Supervisor and the European Commission).

In the meantime, a group of cloud providers has joined forces through a self-regulatory initiative that has so far resulted in the publication of the group's Open Cloud Manifesto (see www.opencloudmanifesto.org). The Manifesto intends to start a dialogue between the cloud computing industry and cloud users by introducing a set of principles designed to ensure that the cloud remains open and that the cloud's challenges (including data privacy and security) are addressed through open collaboration and the appropriate use of standards.

Whether self-regulatory efforts will suffice to make sure that personal data are protected in the cloud remains to be seen.

AUTHOR

Wim Nauwelaerts and Pauline Le Bousse are attorneys in the Brussels and Paris offices, respectively, of the Privacy Practice Group of Hogan & Hartson LLP.
Email: wnauwelaerts@hhlaw.com and plebousse@hhlaw.com
Website www.hhlaw.com