iS
CHANNEL

Privacy Issues with Cloud Applications

Vikas Ranganathan
Candidate for MSc Analysis, Design and Management of Information Systems
Information Systems and Innovation Group
Department of Management
London School of Economics and Political Science

KEYWORDS

Privacy
Cloud Computing
SaaS
Legal
Technology Law

ABSTRACT

This privacy review analyses the relevant laws, technological problems and literature on Software as a Service (SaaS). The advent of web applications within powerful web browsers has meant the consumer-oriented segment of the IT industry is evolving away from the server environment to an open field client environment. The article will debate the legal implications of the cloud on the privacy of the user and whether it is possible that technology will have to provide some of the solutions that the legal law cannot provide. At the end, the article concludes whether cloud computing is expected to deliver the benefits that it states it will provide in accordance with adequate regulation, security and privacy features required for its user.

Introduction

"The growth of personal computers and the Internet has made computing a mainstream activity" (Rappa 2004: 40). Cloud computing is developing as the new de facto method of providing a service for software development. Much hype is being placed upon cloud computing, such as "the battle for the clouds between these companies is going to reshape the ICT market structure as PC distribution did in the 80" (Etro 2009: 8). This notion was unthinkable a decade ago and has only become viable through the development of high-speed Internet connections and mobile access. Although cloud computing has many forms, we will be focusing on Software as a Service (SaaS). Popular web applications such as Gmail, Facebook, Twitter, Flickr and more are all SaaS applications. SaaS means "end users can access the service 'anytime, anywhere', share data and collaborate more easily, and keep their data stored safely in the infrastructure" (Armbrust et al. 2009: 4). This abstracts all the complexity, providing common users an alternative to a native running application on their personal systems.

Benkler (2006) assumes that the physical capital (computers, telecommunications infrastructures) required for the production of information goods is abundant and broadly distributed in society, thus enabling individuals to interact in an almost costless way. The popularity of SaaS is because the web browser has become more powerful during the last few years. Web applications have become more popular because "for most applications, the entire user interface resides inside a single window in a web browser" (Hayes 2008: 10). Moving from the early days of just providing information and data, they can now offer interactive applications with the same functionality as their desktop counterpart. However, the problem with these 'web applications' is that the web browser was never built to run desktop style applications. Developers use a method called 'Ajax' to provide this functionality, but this is actually a browser hack that was used previously for a completely different purpose. This means that there were no guidelines, protocols or regulations set for this functionality. Therefore the applications have multiple patch work systems working together to provide the end solution.

Introna argues that it is for the "good of society as a whole that privacy is preserved, even at the expense of legitimate social control" (Introna 1997: 273). Horrigan (2008) agreed with this notion and found that users were very concerned with their data, with over 90% of them very concerned if their provider sold their data to others and 80% of them very concerned if the organisation used their photos or other data in marketing campaigns. Further to this, "a recent report by TRUSTe, an organization that provides a seal to identify trustworthy online organizations, found that most (71%) online users are aware that third parties may collect information about them for advertising purposes, but that 57% were not comfortable with advertisers using such information to serve ads to them" (Horrigan 2008).

Corresponding Author
Email Address: v.ranganathan@lse.ac.uk (V. Ranganathan)

Legislation

"Even when no laws or obligations block the ability of a user to disclose information to a cloud provider, disclosure may still not be free of consequences" (Gellman 2009: 11). Balancing the security of the public with the privacy right of an individual has always been a struggle especially since law usually lags behind technological innovation. In the case of cloud computing and its services this is proved true as many of the original laws view databases as simple storage spaces where 'content' is owned by the data controller. In the modern world, this does not solve the problems of the controller being the user itself or address the problems of the shifting nature of data ownership models and relationships between data controllers and processors.

When using cloud services, a legal contract is created between the user and the service provider on the rules of usage, service expectations and more in the form of Terms of Service (TOS), Privacy Policies and Service Level Agreements (SLA), which benefits both parties. However, the conclusion of the research into privacy policies by Carnegie Mellon University is that "reading online privacy policies would take an average of 10 minutes per policy and would cost $365 billion in lost leisure and productivity time" (McDonald and Cranor 2008: 1). The main cause of this is that privacy policies are generally written in a 'lawyer' style language that is difficult for the public to understand. "Those risks may be magnified when the cloud provider has reserved the right to change its terms and policies at will" (Gellman 2009: 6). An example would be when Facebook changed their terms of use without public consultation or notification in February 2009, causing a public outrage and distrust in the community. According to a report from Forrester Research in March 2008, "Most cloud vendors today do not provide availability assurances. Service-level agreements are mostly nonexistent" (Staten 2008: 9). The SLAs that do exist generally only cater to the uptime of the service, not whether the service met the expectations of its customers. The language and loss of clarity about these issues unfortunately devolves the debate around cloud computing and its applications into a simple balancing act between the various different parties involved.

The government is required to obtain a warrant in order to enter ones home and search or seize their assets. The Fourth Amendment to the US Constitution is part of the Bill of Rights and guards against unreasonable searches and seizures. It provides protection against Government intrusion upon the privacy of individuals and is historically property-based. The Supreme Court has failed to address the Fourth Amendment's application to email and cloud services and "once a user discloses information to the provider, the user relinquishes any Fourth Amendment protection in the information by virtue of losing the right to exclude" (Kerr 2004: 28). The statement therefore states that according to law the government does not violate the privacy of a user by requesting a third party (e.g. Internet Service Provider) to provide access to their private information.

There have been multiple cases involving email misuse including Warshak v. United States where the Department of Justice (DOJ) "illegally ordered defendant Stephen Warshak's email provider to prospectively preserve copies of his future emails, which the government later obtained using a subpoena and a non-probable cause court order" (Electronic Frontier Foundation 2008). The government has found numerous ways to accomplish this misuse of their powers due to the out of date or inadequate laws that were enacted in the past.

The USA Patriot Act increases the ability of law enforcement agencies to search telephone, e-mail communications and other records. This eases restrictions on foreign intelligence gathering within the United States. One of the controversial invocations of the act was the use of National Security Letters (NSL) to retrieve data on residents and visitors of US citizens who are not suspected of any criminal investigation without the knowledge of the individual. "Those who receive an order to disclose information under these authorities are highly limited in their ability to reveal that they received the order" (Gellman 2009: 14). Therefore they were unable to challenge the case in court or inform their users in any form.

CBCNews (1996) discusses Lakehead University in Canada outsourcing its email to Google, causing concern by students and staff. This is due to their emails being stored in the United States and the contents would be vulnerable to the US Patriot Act. This case study raises the issue if non-US data should be allowed to be processed within the US. However considering most of the cloud service providers are all US based, it is hard to come to a conclusion.

Compared to the US, as discussed by the EUR-Lex (1995) the EU Data Protection Directive was enacted to regulate the processing of personal data within the EU. The lack of similar protection in the US caused major problems, since it deemed the export of personal data of EU citizens to third countries that do not provide 'adequate' privacy protection illegal. Therefore the US-EU Safe Harbor agreement was reached in 2000 as a streamlined process for US companies to export data from the EU. However, "the Safe Harbor Framework has been the subject of ongoing criticism, including two previous reviews

(2002 and 2004). Those reviews expressed serious concerns about the effectiveness of the Safe Harbor as a "privacy protection mechanism" (Connolly 2008: 4). The agreement failed to specify what the third countries are able to do with the data. Therefore once the data is moved outside of the EU, it is again under the weakened laws of the US.

Flow of data is a geopolitical issue and each country has different regulations and laws. Therefore individuals can be unsure of their privacy rights "as one has no good way of knowing where ones data is, how it is protected, or what other data and processing are going on in the same infrastructure. In fact, the provider probably does not know, and neither does the auditor" (Rash 2009). Due to the Safe Harbor complications, it is now accepted that if a third party as a data processor obliges its contractual agreements with the data controller, it is the national jurisdiction of the data controller that applies.

Technology

The legal issues discussed, prove that an absence of strong legal protections will continue to cause disruptions in the development of advanced cloud services. Until governments and third parties are limited in their methods of gaining access to data through abusing weaker measures, individuals will not take advantage of the benefits that are offered by cloud services. Therefore, it is possible that technology will have to provide some of the solutions that the legal law cannot provide.

"Encryption is one of the most powerful weapons in the security war, because it makes data useless when it falls into the wrong hands" (Stoller 2010: 37). Therefore data encryption is often considered as a solution to system vulnerabilities. "The RSA cryptosystem, named after its inventors Rivest, Shamir and Adleman, is the most widely known and widely used public-key cryptosystem in the world today" (Hinek 2007: 1). However, even the most secure of encryptions are susceptible to attack, and "of particular importance, RSA is one of the public-key cryptosystems used in the Transport Layer Security (TLS) protocol and its predecessor, the Secure Sockets Layer (SSL) protocol, which are used to provide secure communications on the Internet" (Hinek 2007: 1).

Researchers at the University of Michigan "found they could foil the security system by varying the voltage supply to the holder of the 'private key', which would be the consumer's device in the case of copy protection and the retailer or bank in the case of Internet communication" (University of Michigan 2010). While gaining access to the power supply is unlikely at a large organisation, it showcases vulnerabilities in these encryption systems, even those that are considered to be perfect.

Even when publicly used security protocols are available, not all cloud services ensure they are used. Accessing data without these security features in public areas such as coffee shops, universities and more leaves the user open to vulnerabilities. Google (2010) states that Google Mail only switched to the HTTPS protocol in January 2010 after the suspected Chinese attacks on Google Servers. Other cloud services such as Facebook, although have valid HTTPS certificates, do not use them and do not provide HTTPS encryption service to their users.

As previously stated, web applications are a combination of patchwork systems. One of these patchwork systems is to 'identify' each individual. Since the Internet was not build for authentication, developers have created a number of digital authentication systems, each with its own strengths and weaknesses. "Online identity theft, fraud, and privacy concerns are on the rise, stemming from increasingly sophisticated practices such as 'phishing'" (Cameron 2006: 1). User authentication is a much more complex issue as shown by the problems users face when using these ad hoc systems such as the requirement to authenticate themselves multiple times with a number of services, lost passwords or disclosing extra data than actually required by the service.

Facebook - a social networking website - provides an integration authentication system called 'Facebook Connect'. This is used by thousands of developers to access a user's profile under consent. The Facebook API even provides methods to request 'Extended Permissions' from the user to read their inbox messages. These extended permissions for the illiterate user can be misunderstood as they may have no idea what permissions they have provided. They could accidently grant access permissions to phishing websites (web forgery), causing major privacy breaches. These applications can be used to harvest a user's data and possibly even for identity theft without any knowledge by the user.

The EU has already requested tighter privacy measures on social networks in their 'Article 29' on Data Protection, which was adopted in June of last year. A review of the guidelines in Article 29, states that social networks must have the highest security settings by default "in order to reduce the risk of unlawful processing by third parties. Restricted access profiles should not be discoverable by internal search engines, including the facility to search by parameters such as age or location" (European Commission 2009: 7). It continues to state that users should be informed of the "usage of the data for direct marketing purposes" and "possible sharing of the data

with specified categories of third parties" (European Commission 2009: 7). These clear guidelines should insure tighter privacy features of social networks within the EU.

As previously discussed in the Legal section, using the US Patriot Act, NSL's gain access to millions of records of user activity. While a user's online identity is restricted to the Internet, but the government can crawl through millions of records in order to find incriminating details and reveal their true identity. The problem is that most of these NSL have not provided any real proof of preventing any crimes and they seem to lower the privacy of individuals, not increase their security. There are methods available to protect oneself from being identified within these records and it is argued that the individuals, who have intent to cause harm, would employ such tactics to ensure they do not get caught, removing the benefits of the NSLs. Using these methods, crypto professionals can avoid traces, protect them and render such data retention mandates useless and expensive.

One of the methods used is Virtual Private Networks (VPN), this allows the user to only make a single connection to the VPN server and then all further data is encrypted through the VPN Server. Therefore the only communication recorded is between the user and the VPN, bypassing any detection. Similarly proxy servers are available to hide users history, but unless the user knows the provider of the proxy server, the user risks data collection and may be subject to traffic analysis. Other services including software such as Tor, JAP and I2P rerouting the user's traffic through multiple proxies, so it becomes impossible to trace the user's location and initial connection.

Conclusion

There are a number of legal and technological challenges that are present for cloud applications. The organisation that runs these services must understand that they must provide adequate and detailed information to users. The recent Facebook privacy problems showcases that even large organisation can have a poor understanding of user's privacy rights and proves that large organisation cannot regulate and competing between themselves. On the same notion, Erdogmus (2009) discusses the 'dream of platform independency'. These large organisations without governance could use cloud computing as a method to ensure that their propriety standards prevail. Therefore, privacy policy makers must understand the problems and solutions provided by technology to provide truly secure options and identify gaps to fill in current laws and technology.
Cameron (2005), Microsoft's Chief Identify Architect, during a lecture at the London School of Economics (LSE) discussed his paper on 'identity metasystem', which is similar to the concept of users in the offline world carrying a number of identity cards and having complete control of which card they would like to provide. "It lets users select from among a portfolio of their digital identities and use them at Internet services of their choice where they are accepted" (Cameron 2006: 1). If a website requires a user to prove their age is over 21, the user can request one of their digital identities to provide a yes/no reply only, not the user's actual date of birth. This describes the notion of 'minimal disclosure'. This system is already being implemented by 'Open ID', but has yet to be widely accepted and is still unsecure to phishing attacks and other exploits. Once security protocols improve, however, it will hopefully become a standard for other systems to build upon.

Organisation such as Twitter and Facebook must be more responsible when providing developers access to their users' data. Twitter has already made improvements by using an open protocol called 'OAuth'. This system allows for the client and the server to exchange access tokens, therefore no username or password must be given. Although OAuth is limited in its functionality, it proves the importance of controlling access specifications for users when connecting to multiple amounts of third party applications.

Informing users of where, why and how long their data will be kept will be an important step in reassurance. This could include the ability to opt out of service optimisation (therefore their personal data is stored in a single jurisdiction) or improve their own privacy policy wording so all their users can understand. It can be argued that 'informed consent' in the real world is nearly impossible to achieve. It's important that users not only trust that their data will be private, but also that there data is secure. In the event of data loss, damage or theft, these services must have protocols in place to deal with such situation and not place the responsibility on users who are unlikely to have this knowledge.

"It is for the ultimate good of society as a whole that privacy is preserved, even at the expense of legitimate social control" (Introna 1997: 273). User trust is the most important part of any application usage. Therefore, involving the user at the deepest privacy changes becomes an important part of any service. Due to the EU Data Protection Directive, users must be notified of changes to their privacy policy, but US law does not require such action. If a privacy policy is updated without any notification, but is present on their website, it is deemed acceptable in the US. The US must take steps to protect its own citizens by providing guidelines and regulations to organ-

isations on privacy law. As discussed in Electronic Frontier Foundation (2010), it is reassuring to witness that in March, major organisations including Microsoft, Google, EFF, AT&T and more created a new campaign called 'Digital Due Process' requesting several major changes to existing law.

Only when US Law is updated and cloud service providers improve their encryption and identity technology, they will be able to provide truly secure options to their users. Until then, it's debatable if regulation is ready to protect users and if they can rely on the cloud for all their data needs without knowing the implications that are placed upon every action they perform.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I. and Zaharia M. (2009) Above the Clouds: A Berkeley View of Cloud Computing. *Communications of the ACM*. 53 (4) pp. 50-58.

Benkler, Y. (2006) *The Wealth of Networks*. New Haven: Yale University Press.

Cameron, K. (2005) The Laws of Identity. A Microsoft White Paper. http://msdn.microsoft.com/en-us/library/ms996456.aspx (accessed 5 August 2010).

Cameron, K. (2006) Microsoft's Vision for an Identity Metasystem. A Microsoft White Paper. http://msdn.microsoft.com/en-us/library/ms996422.aspx (accessed 5 August 2010).

CBCNews. 2006, December 11. Lakehead University, you've got Gmail. http://www.cbc.ca/canada/ottawa/story/2006/12/11/google.html (accessed 3 April 2010).

Connolly, C. (2008) The US Safe Harbor - Fact or Fiction? *Galexia*. http://www.galexia.com/public/research/articles/research_articles-pa08.html (accessed 5 August 2010).

Electronic Frontier Foundation. 2008, June 10. Warshak v. United States. http://www.eff.org/cases/warshak-v-united-sta (accessed 5 April 2010).

Electronic Frontier Foundation. 2010, March 30. EFF Joins With Internet Companies and Advocacy Groups to Reform Privacy Law. http://www.eff.org/press/archives/2010/03/30 (accessed 6 April 2010).

Etro, F. (2009) The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe. *Review of Business and Economics*. 54 (2) pp.179–208.

EUR-Lex. 1995, November 23. Directive 95/46/EC. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (accessed 7 April 2010).

European Commission. 2009, June 12. Art.29 Data Protection Working Party. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (accessed 8 April 2010).

Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (accessed 5 August 2010).

Google. 2010, January 12. Default https access for Gmail. http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html (accessed 8 April 2010).

Hayes, B. (2008). Cloud computing. *Communication of ACM*. 51(7) pp.9–11.

Hinek, J. (2007). *On the Security of Some Variants of RSA*. Ph.D. thesis, University of Waterloo, Canada.

Horrigan, J. B. 2008, September 12. Pew Internet. http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx?r=1 (accessed 3 April 2010).

Introna, L. D. (1997) Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy*. 28 (3) pp. 259-275.

Kerr, O. S. (2004) The Fourth Amendment New Technologies: Constitutional Myths and the Case for Caution. *Michigan Law Review*. (forthcoming).

McDonald, A. and Cranor, L. F. (2008) The Cost of Reading Privacy Policies. 36th Telecommunications Policy Research Conference, September 26-28, 2008, Arlington, VA. Carnegie Mellon University.

Rappa, M. A. (2004) The utility business model and the future of computing services. *IBM Systems Journal*. 43(1) pp. 32-42.

Rash, W. (2009) Is cloud computing secure? Prove it. *eWEEK*. http://www.eweek.com/c/a/Cloud-Computing/Is-Cloud-Computing-Secure-Prove-It-849274/ (accessed 1 April 2010).

Staten, J. (2008) Is Cloud Computing Ready For The Enterprise? Forrester.

Stoller, J. (2010) Encryption – The last line of defence. *CMA Management*. June/July pp. 37-38.

University of Michigan. 2010, March 3. Researchers find weakness in common digital security system. http://www.ns.umich.edu/htdocs/releases/story.php?id=7551 (accessed 1 April 2010).