Date: 18/07/2022

Name: Jack Sydenham StudentID: s3841816

**Professional Computing Practice**

**Assessment 1, Milestone 1: Written Report**

**Report on**

**One of the Biggest Ethical Dilemmas Involving Cloud Computing**

Table of Contents

1. **Introduction** - **3** -
2. **Background Analysis**- **3** -
   1. Known Relevant Facts- **3** -
   2. Identifying Stakeholders- **3** -
   3. Obligations of Stakeholders- **3** -
   4. Identifying Ethical Values and Social Impacts- **3** -
3. **Legal Resource in Australia** - **3** -
   1. Identifying Those Legally Responsible for the Negative Consequences- **3** -
   2. Identifying Who is Responsible for Ensuring No Harm Comes to Those Who Use This Technology - **3** -
   3. Reviewing Which (if any) Specific Laws Deal With The Issue- **3** -
4. **Proposed Solutions** - **3** -
5. **Case Study** - **3** -
6. **Conclusion** - **3** -
7. **Bibliography** - **3** -
8. **Appendix** - **3** -

# Introduction

The topic of cloud computing is one that has been discussed with utmost admiration over recent years, with it’s extensive list of benefits being commonly acknowledged by it’s wide range of stakeholders including computer scientists and business owners alike. Though when considering the negative sides of cloud computing, it’s likely that said stakeholders think primarily of the risks that come with investing in such technology, often de-emphasizing the ethical concerns related to the technology. In truth, while there have been acknowledgements of the issues of ethics within the field of cloud computing, this rapidly growing computer system resource has seen hardly any ethical analysis by those with the proper expertise required to analyze it in such a way. While laws in place related to technological ethicality are ever changing, we are at a time now where the boundaries of ethics within the field of cloud computing is struggling to keep up to the rapidly growing industry.

This paper will review current ethical issues known within the field, and propose a potential solution for said issues. Section 2 will address the current situation, outlining stakeholders of the technology and they’re obligations related to adhering to ethical norms within the field. This section will also identify existing ethical values shared by stakeholders, along with the social impacts that cloud computing currently has on the broader IT industries and people involved in these industries. Section 3 will identify the current laws and regulations relating to the field of cloud computing in Australia and review whether or not the current laws appropriately address the ethical issues states in section 2 of the paper. Section 4 will outline two possible solutions that may help in addressing the underlying issue and what positive affects they would have on the field. Finally, section 5 will cover a hypothetical scenario based on real world cloud computing environments, wherein the solutions discussed in section 5 may be applied to help victims of said ethical dilemmas.

# Background Analysis

## 2.1 Known Relevant Facts

Firstly, it is important to understand the meaning of ethics, as this paper will base it’s solution off such a meaning. While there is no formulaic right answer to what is ethically correct in any given scenario, most modern views on ethical rules imply that as Kant’s views suggest, ethics are created through rules that are followed, where the ethicality of a scenario or action is judged based solely on which ethical norms – if any – have been violated (Hill 2006). A study of the collection of data within the cloud computing field was completed by Herschel and Miori to consider the ethics from the view of various ethical perspectives, where from the perspective of Kant’s ethical measure, the collection and use of data in the field of cloud computing contrasts strongly with that of Kant’s views on ethics (Herschel and Miori 2017). They analyzed a total absence of consent from providers, accompanied by dishonest behavior as many providers aim to benefit from the lack of laws in place, all at the cost of the privacy and trust of stakeholders. These issues of lacking trust and privacy have proven to be the largest of ethical issues within the industry. Firdhous (2012) speaks on the interconnection between service providers in the cloud computing field to accommodate for the rapidly increasing amount of users. This allows data to move around and be overly mobile within the cloud, to the point of providers losing track of all the places in which specified data is located. The data in this sense has been described as promiscuous, easily subject to misuse by providers.

## Identifying Stakeholders

There are many types of stakeholders in cloud computing, though understanding their differences is imperative to understanding where the current system falls short ethically.

As (GFG 2021) writes:

Cloud Service Providers (CSP) are a group or organization that provides the cloud service used by Cloud Consumers. As stated in section 2.1, there are many different CSPs and naturally, many sorts of CSPs. IaaS Providers deliver digital access to physical infrastructure such as servers, networks and storage that exist in person. SaaS Providers deliver more business focused technologies rooted in fields of Human Resource Management (HRM) and Customer Relationship Management (CRM). PaaS Providers are tuned more towards software development services, providing things like operating systems and application stack.

Cloud Consumers are end users who utilize the services delivered by CSPs. These consumers may use Service Level Agreements (SLAs) which specify a performance requirement which is to be met by the cloud provider. These SLAs include other things like security measures, quality of service expectations, and resolutions for performance dips. CSPs may also include a set of boundaries, limitations, or obligations within the SLA which the consumer must agree to adhere to.

These are the main stakeholders which will be referenced in this paper, though there are also:

Cloud Carriers, which mediate the cloud computing process, providing connectivity of cloud services, allowing access to necessary cloud networks by CSPs and consumers through the internet.

Cloud Brokers, which are independent organizations which manages statistical behavior of cloud services (for example, managing performance and delivery) to provide its own service as a combination of multiple services. This allows them to create more opportunistic services which provide only the necessary services for an optimal price.

Cloud Auditors, which are independent entities which deliver assessments of cloud services, monitoring things like performance and security. This is done to assess whether the promised service has been implemented correctly or not.

## Obligations of Stakeholders

As Cloud Computing has proven to be such a rapidly growing industry over the past few years, laws and ethical obligations have not been as well established in the field of cloud computing as they have been in other fields of IT. It is especially hard however to regulate an environment like that of a cloud computing service, as no matter the laws which are put in place, the effectiveness of a cloud computing system relies almost entirely on the trust made between the CSP and their consumer(s), as the consumer must concede part of their control over the data which they wish to pass through the cloud service. So then, a user who does not trust a CSP is far less likely to feel comfortable giving their data away and will be reluctant to work with the CSP at all. It is this concept of trust which is the leading factor in promoting good ethical behavior within the field of cloud computing and it is the stakeholders’ obligation to build this trust and bring about a safe environment for cloud service operations. As stated in section 2.2, there are tools like SLAs in place to assist with ensuring trust between the CSP and the consumer is built and an ethical common ground is established, though often limitations and/or obligations of data usage are put in place by the CSP, so as long as the consumer agrees, the CSP has a great deal of freedom with regards to what they can or cannot do with the user’s data. To further this, as stated in section 2.1, many CSPs attempt to benefit from the current laws in place, or rather the lack thereof further reducing the general trust within the field so although it is the stakeholders obligation to regulate the effectiveness of the system through building trust, there will always be bad actors and there must be ethical rules in place to account for such behavior.

## Identifying Ethical Values and Social Impacts

So then, what should these said ethical rules aim to achieve; what ethical values should be prioritized in this field and how does abiding by these values affect society? There are two forms of ethical values which are most commonly referred to today. The first being the aforementioned perspective of Kant, also referred to as deontological ethics, which as stated, describes an ethical society which is governed by a wide set of rules, operating smoothly on the basis of each individual in that society abiding by said rules. Alternatively we Utilitarianism, which focusses on, as Jeremy Bentham puts it, achieving the most broad range of satisfaction; the greatest good among the greatest amount of people (Crimmins 2019). In this, things that aren’t generally considered ethically right are allowed, provided they lead towards widely desired outcomes. So which ethical theory then, applies to cloud computing most effectively? Truly, there is no right answer, as the social impacts of both sides have negatives to accompany their positives. As mentioned in section 2.3 there will always be bad actors who aim to bend the law in their favour, which is brought to light by the theory of Deontological Ethics, focusing on a law abiding environment. As for the application of Utilitarianism, since this industry is so new and rapidly growing, it poses the extremely difficult task of analyzing all potential situations and uses of data for creating a set of limitations on which the theory will be based on.

# Legal Resource in Australia

## 3.1 Identifying those legally responsible for negative consequences

With this industry growing so rapidly as previously stated, there is no totally effective legal framework in operation to clearly lay out the obligations/limitations of stakeholders and impose lawful policies in an environment like that of a cloud computing network (Kshetri 2013). This means issues of lost data may legally be blamed entirely on the consumer, despite the CSP being the one storing the data for. For the case of cloud consumers within Australia, multiple laws pertaining to the responsibility of data protection, including the *Freedom of Information Act 1982* and the *Privacy Act 1988*, stating that it is the consumer’s responsibility to ensure contractual measures such as SLAs are establishedbetween consumer and their CSPs to prevent a breach of Australian Privacy Principles.

## Identifying Who is Responsible for Ensuring No Harm Comes to Those Who Use This Technology

As mentioned, this field is kept safe primarily by the trust developed by both the cloud consumer and cloud provider alike. While the consumer must ensure that they create a contractual agreement which keeps their data out of harm’s way, it is ultimately the CSP which is handling the data, and so it is on them to cooperate with the consumer and ensure the safety of the data. However, as mentioned in section 3.1, in Australia the responsibility of ensuring that the CSP will safely treat both the consumer and their data lies with the consumer themselves, despite their potential lack of control over the usage of the data and the concern of a CSP not cooperating with the consumer is something which the consumer must consider before agreeing to hand over their data.

## Reviewing which (if any) specific laws deal with the issue

As stated previously, there are laws surrounding the topic of cloud computing, though they are not focused on ethical dilemmas directly. We must then look towards the ethical laws in place to regulate the cloud. There may be sufficient ethical laws in place to counteract some of the bad actors in the industry, however as (Bartolini 2018) discusses, in practice, laws of certain jurisdictions may not align with each other. Therefore, since cloud computing has such ease of access and potential to spread internationally, current legal terms of ethics sill surely not be able to effectively regulate cloud environments if they are not contained within provinces which have aligned laws.

# Proposed Solutions

As evident from the information provided prior to this section, it is clear that there are two ways to go about solving this dilemma of unregulated/untrustworthy environments in cloud; regulation through legal jurisdiction or standardized implementation of more responsible operations within a cloud environment. The following subsections will outline these individually.

## Solution 1: Regulation through legal juristiction

The current attitude towards legislation in the realm of computing is to address problems when they become real, rather than attempting to totally predict the problems new technologies will create (Whitehouse 2016). In the field of cloud computing however, such problems are currently occurring, as has been discussed. So then, to address these problems in a legislative way which merges seamlessly between nations, a global standard of legislative rules surrounding cloud computing should be introduced. At this point, no such regime has been put in place to regulate the industry on a global scale (Baylis 2006, p637). Naturally, it would seem that such an implementation would be near impossible, since the likelihood that all states partaking in the regime would agree on all necessary regulatory practices is extremely low. In truth, Legislative regimes within the cloud computing industry would be more likely to hinder the potential success of the technology, with laws surrounding the matter consequentially inhibiting the cloud’s development (Nelson 2009, p75) and more importantly the construction of trust based relationships between consumers and their CSP.

## Solution 2: standardized implementation of more responsible operations within a cloud environment

Unlike solution 1, this method intends to do quite the opposite, where effective regulation is undermined for the sake of stakeholder-based trust development. While it may be said that as (European Data Protection Supervisor 2015) states, things like audits, contractual obligations and specified boundaries may lead to a robust trust between provider and consumer, it could just as easily be argued that since trust is an undefinable requirement which is needed for the basis of cloud systems, eliminating the overruling government of cloud and data protection by de-emphasizing these required legal documents and focusing rather on the responsibility of business’ and other consumers’ to build trust would prove to be more utilitarian and reward responsible consumer and provider behavior in the long term.

# Case Study

So then, let us imagine a realistic hypothetical case where the given solution would improve the situation described. Let us imagine that there is a high school, ‘Balwyn High’ which is looking to move their student data from their on-site hard drive storage to a cloud environment. They reach out to ‘Kloud Tech’, a cloud service provider to discuss their plans and begin to lay out the plans for implementation. The primary goal of Balwyn High is to ensure their data which is moving to the cloud will be kept safe by Kloud Tech, however the leading ethical issue is now arising; how can Balwyn High safely assume that their data will be looked after. For the sake of the study, let us imagine that Kloud Tech do indeed intend on misusing Balwyn High’s data once they have control over it; they may wish to steal money using the students’ attached school fee payment details. For Balwyn High to ensure they can trust Kloud Tech, they will want to establish some SLAs which bound Kloud Tech to certain limitations which suit the needs of Balwyn High’s data, though Kloud Tech may have obligations or limitations which restrict Balwyn High to an extent, giving Kloud Tech the freedom to handle the data in ways which Balwyn High may not be happy about. Furthermore, with the help of the current laws surrounding cloud computing in Australia, if Kloud Tech were to misuse or even lose Balwyn High’s data, it would be the school who is held responsible and the CSP could face little to no repercussions for their ill behavior.

So then, as discussed in section 4.3, if laws pertaining to responsibility and documentation were de-emphasized, then it would be much more important for trust to be built between the CSP and consumer, as they can’t simply set limitations and deceive the consumer using the law. In turn, CSPs would be inclined to make more of an effort to build the necessary trust with their consumer and form closer relationships with them in the long term. This way, consumers also have much more of a say over what happens to their data, rather than settling for the potentially long list of obligations and limitations set by the CSP.

For our circumstance, Balwyn High would then be able to lay out their exact needs of Kloud Tech, and with a more trust-based environment being formed, ensure their data is handled according to their needs, without needing to consider all the specific limitations set by Kloud Tech in the hopes of being able to misuse the given data without Balwyn High noticing.

# Conclusion

Issues related to data ownership, cloud legislation, and trust within a cloud environment were discussed and it was found that the rapidly growing industry of cloud computing is one that presents itself as being difficult to regulate ethically. At this point, the topic of ethical issues pertaining to cloud consumers and service providers is one that is only lightly discussed, despite its growing (though already high) level of importance. In closing, it can be said that the multi-stakeholder field that is cloud computing can only operate effectively and in line with ethical expectations if all stakeholders involved commit equally to building the necessary trust between each other, for a strong, truthful relationship between a consumer and their CSP is imperative to their success in cloud computing both ethically and logistically.

# Bibliography

Australia: Act No. 119 of 1988, Privacy Act 1988 [Section 3.1, Page 5]

Australia: Act No. 3 of 1982, Freedom of Information Act 1982 [Section 3.1, Page 5]

Baylis, J., Smith S., (2001) ‘The Globalization of World Politics’ (Oxford). [Section 4.2, Page 6]

**Bartolini, C., Santos, C., & Ullrich, C. (2018). Property and the Cloud. Computer Law & Security Review, 34(2), 358–390. [Section 3.3, Page 6]**

**Crimmins, J. E. (2019). Jeremy Bentham. In E. N. Zalta (Ed.), Stanford Encyclopedia of Philosophy. [Section 2.4, Page 5]**

European Data Protection Supervisor. (2015, September 11). Towards a New Digital Ethics. [Section 4.3, Page 6]

**Firdhous, M., Ghazali, O., & Hassan, S. (2012). Trust Management in Cloud Computing: A Critical Review. International Journal on Advances in ICT for Emerging Regions (ICTer), 4(2), 24. [Section 2.1, Page 3]**

Sharma, M. (2021) ‘Cloud Stakeholders as per NIST’. GeeksforGeeks. [Section 2.2, Page 4]

**Herschel, R., & Miori, V. M. (2017). Ethics & Big Data. Technology in Society, 49, 31–36. [Section 2.1, Page 3]**

Hill, T. E., Jr. (2006). Kantian Normative Ethics. In D. Copp (Ed.), The Oxford Handbook of Ethical Theory (pp. 480–514). New York: Oxford University Press. [Section 2.1, Page 3]

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. [Section 3.1, Page 5]

Nelson, M. (2009) ‘The Cloud, The Crowd and Public Policy’. Issues in Science and Technology. [Section 4.2, Page 6]

Whitehouse, D., Duquenoy, P., Kimppa, K. K., Burmeister, O. K., Gotterbarn, D., Kreps, D., & Patrignani, N. (2016). Twenty-Five Years of ICT and Society: Codes of Ethics and Cloud Computing. ACM SIGCAS Computers and Society, 45(3), 18–24. [Section 4.2, Page 6]

# Appendix

Link to google drive containing references:

<https://drive.google.com/drive/folders/1RtepTuGycqe4N28zG1k3uyaIjUTGWzz8?usp=sharing>

Essay word count (from ‘Introduction’ to ‘Conclusion’ [not including headings/subheadings]): 2765