Ethics and Cloud Computing

Brid Murphy and Marta Rocchi

Abstract While the benefits of cloud computing are widely acknowledged, it raises a range of ethical concerns. The extant cloud computing literature reports specific ethical perspectives on focussed topics in this domain, but does not explicitly refer to a specific ethical conception or reference point. This chapter provides an overview of ethics and ethical theories, which can be used to analyse the use of cloud technology and the complex multi-stakeholder structure of the industry. It is critical that cloud providers and users recognise that they effectively shape the morality of the cloud computing context through their interactions with other providers and users, and with the platform itself. Both stakeholder sets must be accountable for the possibilities offered by the technology. While pertinent regulation is continuously evolving, it is unlikely to advance at a

B. Murphy (✉)

DCU Business School, Irish Institute of Digital Business, Dublin City University,
Dublin, Ireland

e-mail: brid.murphy@dcu.ie

M. Rocchi

DCU Business School, Irish Institute of Digital Business, Dublin City University,
Dublin, Ireland

e-mail: marta.rocchi@dcu.ie

© The Author(s) 2021

T. Lynn et al. (eds.), *Data Privacy and Trust in Cloud Computing*,
Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-030-54660-1_6

similar rapid pace to that of innovation in the cloud computing industry. It is therefore essential that ethics is carefully considered to orient cloud computing towards the good of society.

Keywords Ethics • Cloud computing • Ethical analysis • Ethics of technology • Data ownership • Data privacy • Green computing • Organisational ethics • Personal ethics

6.1 INTRODUCTION

The many benefits and risks associated with the adoption of cloud computing technology have been widely reported by computer scientists. However, the same cannot be said in relation to ethical issues associated with the adoption of this technology: while voices caution that cloud technologies may traverse the boundaries of what is morally desirable for individuals, business, and society, few academics with ethics expertise have actually analysed the ethical issues associated with cloud computing. Contributions on ethical concerns connected with this new technology have been published mainly in computer science journals and have been discussed at conferences with a similar audience—sometimes privileging the explanation of technical aspects over the depth of the ethical analysis.

In light of this, the chapter aims to review selected ethical issues related to cloud computing, arising from the nature and use of the technology and the way in which the industry is structured, making reference to the existing literature on the topic. Section 6.2 provides an overview on ethics and some prominent ethical theories. It establishes the significance of ethical analysis when applied to a particular domain, such as cloud computing. The section concludes by questioning the depth of ethical analysis conducted in relation to cloud computing. It also details how the remainder of the chapter is organized, in accordance with recurring themes in existing literature; however, these do not take into explicit consideration particular schools of ethics when describing ethical issues associated with cloud computing, as the literature to date has failed to do so. Section 6.3 categorizes existing literature specifically related to cloud computing in accordance with three different and interrelated perspectives: it critically reviews ethical perspectives related to data, it then examines the ethical perspectives pertinent to providers of cloud computing services, and it also explores ethical issues related to the final users of cloud computing

services. Each of these sub-sections presents literature within the context of ethical analysis as outlined in Sect. 6.2; it should however be noted that due to the limitations previously outlined on the depth of ethical analysis, the section is sometimes presented as a critical collection of existing contribution on the theme. The Conclusions section hosts final reflections and outlines avenues for further research; ultimately, it suggests that ethical analysis pertinent to cloud computing needs to be more ethically grounded, if it seeks to contribute authoritatively to wider ethical debates regarding the ethics of new technologies.

6.2 AN OVERVIEW OF ETHICS AND ETHICAL THEORIES FOR ANALYSIS OF CLOUD COMPUTING

Before reviewing existing literature about the ethics of cloud computing, it is important to understand what ethics is, and who the main thinkers that nourished the debate in this branch of philosophy are. Throughout history, many thinkers devoted attention to human actions and asked fundamental questions about their meaning and purpose, reaching very different—and even contrasting—conclusions. For example, Aristotle regarded ethics as a discipline to study the way human beings live and act in order to achieve a life worth living. Aristotle’s inquiry was not only theoretical, but also eminently practical: he focused his attention to studying the habitual dispositions that human beings can develop when working towards the realization of their good, which he called virtues (Aristotle 2000). He is considered one of the fathers of Virtue Ethics, one of the most prominent ethical theories. Other thinkers studied questions similar to those of Aristotle, but arrived at different conclusions. The seminal work of Jeremy Bentham and John Stuart Mill, as well as Immanuel Kant, considered to be the fathers of Utilitarianism and Deontological Ethics, respectively, is also very significant. For Bentham, the guiding principle for human actions was the principle of utility, which he first formulated as the achievement of the greatest good for the greatest number of people (Crimmins 2019). Utilitarianism established itself as one of the most pervasive normative ethical theories and considers as “right” that which achieves the satisfaction of the highest number of people possible. Its main focus is on the consequences of human actions, up to the point of considering undesirable actions as “right” if they can in turn achieve desirable outcomes. Despite recognized shortcomings, Utilitarianism inspired many

theoretical constructs, particularly in economics and law, thereby influencing economic and societal life. The proponent of the third highlighted approach, Kant, formulated categorical imperatives for every human being to obey, whatever the circumstances and whatever the outcome of the actions following these imperatives. This perspective, more widely known as Deontological Ethics, focused more on rules that need to be respected than on the outcome of actions (Hill 2006). Kant's approach has been highly influential in relation to applied and professional ethics. The challenge pertaining to this approach relates to the identification of both the rules to be followed and who is in charge of setting them.

According to the philosopher Julia Annas (Annas 1993), the main difference between the abovementioned approaches to ethics is that ancient ethical theories (i.e. Aristotelian Virtue Ethics) tend to be centred on the agent, considering the life of the acting person as a narrative unity with a *telos*, a purpose. This agent-centred perspective also characterizes the work of the later Neo-Aristotelian philosophers (such as Anscombe or MacIntyre). On the other hand, more modern ethical theories (i.e. Utilitarianism and Deontological Ethics) are centred on particular actions, and tend to perceive morality as 'punitive or corrective' (Annas 1993, p. 4).

This chronological and thematic overview of the three most prominent approaches to ethics provides a foundation for ethical analysis of cloud computing. However, in reviewing existing contributions which claim to devote their attention to ethical issues related to cloud computing, it appears that these existing contributions: (i) do not explicitly align to a particular school of ethics; (ii) do not offer an explicit or exhaustive account of what ethics is, i.e. do not select a particular definition or approach to ethics; and (iii) do not disclose conceptions of what is "good" or what is "right," which should be the starting point for an analysis which seeks to determine the boundary of what is acceptable (or not) within a professional or business domain.

As a consequence, the structure of the chapter does not reflect the differences between the abovementioned approaches to ethics. The next section, Sect. 6.3, appraises recurring topics in the literature that generally deal with ethical issues related to cloud computing: Section 6.3.1 examines recurring ethical issues linked to the collection, storage and usage of data, Sect. 6.3.2 analyses the perspective of providers of cloud computer services, while Sect. 6.3.3 explores issues related to one of the key stakeholders in the cloud computing industry—the final users of cloud computing services.

6.3 ETHICS AND CLOUD COMPUTING

The previous section introduced ethics and some guiding principles for conducting an ethical analysis according to three prominent ethical approaches. This section reviews existing literature describing ethical concerns related to cloud computing. De Bruin and Floridi (2017) refer to the environment, governments, investors, private and business cloud users, and individuals and corporations interacting with private and business users, as key stakeholders of the cloud computing industry. The literature examined in this section addresses the ethical issues faced by the cloud computing industry when dealing with this complex multi-stakeholder context. The three areas reviewed concern data and the perspective of both providers and users.

6.3.1 *The Ethics of Data in Cloud Computing*

If Aristotle, Bentham or Kant were alive today, they would probably study the manner in which human beings deal with the vast amounts of data currently collected, stored and managed via the cloud. Each would likely promote a different perspective in relation to the best way of dealing with data ethics. Herschel and Miori conducted such an exercise and effectively analysed the ethics pertaining to data according to selected perspectives, including Virtue Ethics, Deontological Ethics and Utilitarianism (Herschel and Miori 2017). They highlight how, from a Kantian perspective, the lack of consent for the collection and use of data would be a clear violation of autonomy, and contrary to Kant's understanding of human beings always as ends in themselves, never as means. They also argue that, from a Utilitarian perspective, the analysis of the ethics of data would be very difficult to perform. They assert that it would be particularly difficult to calculate in a unitary way all the pros and cons of the use of data, and of the ultimate beneficiaries of data usage. In relation to the perspective of Virtue Ethics, this task does not seem to be any easier, given that a Virtue Ethics-based ethical analysis would need to consider how a virtuous person could make the best possible use of data while becoming the best version of themselves.

It would seem that the task of a comprehensive ethical analysis using prominent ethical approaches is particularly difficult, to the point that "data ethics" is now constituting itself as a new branch of applied ethics (Floridi and Taddeo 2016), which is developing its own language and

tools, highly correlated with the ethics of algorithms (Mittelstadt et al. 2016). The analysis conducted in this growing—but still very young—field can be applied, *mutatis mutandis*, to the ethics of data in cloud computing. However, the contributions examined in this section make use of a more legalistic framework, strongly influenced by abundant studies in relation to data ownership, and data safety and privacy. As a result, this section offers an overview of these areas related to the ethics of data in cloud computing, which, in the future, will need to incorporate more explicit ethical considerations.

6.3.1.1 Data Ownership

When an individual or a business uses a cloud computing-based platform, it may be asked “who owns the data”? Can this data be considered as private property, or does the mere fact of using a cloud computing platform mean that this data automatically may belong to another party?

The majority of individual and corporate consumers outsource data storage to cloud services, whereby users can use the flexibility and scalability of the cloud without purchasing standalone software or hardware. These are owned and maintained by various service providers whose overall remit is to store and share the data of a multitude of users. However, these service providers do not provide a uniform service. Further, cloud computing services typically traverse national borders, operating in a global context. This global and international cloud computing environment presents difficulties for regulating in such a context. In practice, national laws and regulations may not always align seamlessly into the international domain. As a result, it is becoming apparent that current legal provisions, which are largely pertinent to national jurisdictions, may not appropriately regulate for the cloud (Bartolini et al. 2018). As a consequence, the relevance of ethics is increasingly debated in relation to a potentially essential role regarding the ‘outsourced’ and international exchange of data in the cloud.

Indeed, the ownership of data and the respect of the right of this particular kind of property is essentially linked with the respect of the fundamental dignity of the human person. The European Data Protection Supervisor (EDPS), an independent institution of the European Union, clearly affirms that human dignity is at the heart of digital ethics: ‘the dignity of the human person is not only a fundamental right in itself but also is a foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data’ (European Data Protection

Supervisor 2015, p. 12). This authority specifically refers to cloud computing as one of the technologies that needs to carefully address the protection of data stored in cloud based systems, especially in an age when people are requested to upload their data from many and different instances in order to access even services related to basic needs. The EDPS also states that human dignity and ethics can be protected only in so far as the following four pillars are established: current regulation should be future-oriented; accountability of those in charge of checking compliance with internal policies and general regulation should be enhanced by codes of conduct, corporate rules and audits; the computer engineering system should be respectful of human dignity, structurally taking into account issues related to privacy; final users need to be empowered (Sect. 6.3.3 will address this last point more in-depth).

It is intended that these pillars should be applied to cloud computing, especially because issues pertaining to data ownership in the cloud environment may not be clearcut (Al-Khouri 2012; Grimes et al. 2009). Indeed, ownership of data is dependent on the nature of the data owned and where and/or how it was created. Some data is created by the user before uploading to the cloud while other data may be created on the cloud platform (e.g. statistical data). The service provider's terms of services can vary and may grant ownership of such data to the provider or to the public domain i.e. the mere uploading of content to the cloud may erode the user's ownership entitlements to the data (Al-Khouri 2012).

In addition, the arrangement and structuring of data on the cloud may be dominated by the service provider rather than the user and this manipulation of the data, e.g. generating and running algorithms while optimising data or generating statistical analysis, can have implications in relation to ownership. Ultimately, it is difficult to determine who actually owns this optimized data as any data on a cloud platform is likely to have complicated ownership (Cavoukian 2008).

6.3.1.2 *Data Security and Privacy*

Data security in the context of cloud computing refers to securing data from unauthorised access and is largely a technical issue which providers must implement and maintain (Zissis and Lekkas 2012). Firdhous et al. (2012) discuss the importance of the security issue in specific relation to cloud computing. The complex interconnection of multiple services by a series of different providers for ever increasing numbers of users generates a myriad of issues in relation to the security of users' data. In reality, the

strength of the cloud correlates with the security strength, or otherwise, of its weakest actor and a breach or an unauthorised access may effectively impact all users (Ali et al. 2015).

Data security may be regarded as an ethical issue because of the responsibility of those in charge of data collection, storage and usage towards the multi-stakeholder environment involved in the cloud environment. The concept of responsibility has a strong ethical connotation when it needs to go beyond what is prescribed by existing laws, leaving to the willingness of individuals and companies the duty to respect the rights of the owners of the data. Each of the abovementioned ethical theories would agree with the suggestion that data security concurs to the good of data security concurs to the good of society (when data is not related to illegal or unethical issues). This is evidenced more widely in the context of regulation, where various legislative provisions pertaining to data issues in the complex cloud environment have been readily introduced. This highlights that it is relatively more straightforward in some instances to identify a shared legal minimum requirement with regard to data security.

Ethical issues related to data security, when data is not collected, stored and managed by the same entity, are particularly significant. Within the overall cloud context, data security is effectively outsourced to service providers. Security measures adopted are dependent on the delivery models e.g. for SaaS models (i.e. Software-as-a-Service), users depend entirely on service providers to prevent multiple users viewing each other's data, while in PaaS models (i.e. Platform-as-a-Service), providers may assign some security elements to those charged with building applications on top of the platform (Subashini and Kavitha 2011). Reed et al. (2011) highlight six areas of focus in relation to the lifecycle data in the cloud, 'Create', 'Store', 'Use', 'Share', 'Archive' and 'Destroy' and assert that data security measures must be implemented at all stages. The importance of security measures in relation to 'data remanence', the 'residual physical representation of the data after it has been deleted' is also detailed (Kumar et al. 2018, p. 693).

In addition, consumers expect providers to facilitate key data properties: 'integrity', 'confidentiality', and 'availability' (Izang et al. 2017; Kumar et al. 2018; Sun et al. 2014; Tanenbaum and van Steen 2016; Zissis and Lekkas 2012). Integrity of data assumes a confidence that the data has not been manipulated or deleted by unauthorised actors; confidentiality assumes data has not been revealed to unauthorised parties and availability assumes the data is intact and that users can use or recover it as

needed. The maintenance of these three properties requires service providers to carefully monitor access and authorisation in respect of all cloud components and may also require linkages to or some supervisory element of third party mechanisms, along with some ongoing verification of the integrity of the data (Bowers et al. 2009; Schiffman et al. 2010). Effective management of all three properties can help to increase overall trust in the system (see below Sect. 6.3.2.1).

The integrity, confidentiality and availability of data is also an essential component of the perception of data security from the point of the users of cloud computing services; this perception is what is characterized as data privacy.

Early concerns regarding privacy issues linked to storing and sharing content online have been somewhat sidelined as the usability and convenience of such systems have proved very attractive in the marketplace (Constantine 2012). However, notwithstanding the wider debate in relation to the moral justification of a right to privacy, the privacy debate in the context of technological innovations is topical (Constantine 2012; Nissenbaum 2009, 2011; Timmermans et al. 2010; van den Hoven 2008). *Privacy* is ‘the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively’ (Sun et al. 2014, p. 6). In many societies, legislation and regulation require compliance such that personally identifiable information is appropriately managed (e.g. European Commission 2018; US Government 1986). In turn, *data privacy* is concerned with the proper handling of data and issues such as consent, notice and compliance with legislation and regulations are dominant (The Centre for Information Policy Leadership 2018). Service providers are thereby challenged with operating services which afford privacy, comply with legal requirements and also balance usability (Stark and Tierney 2014).

In relation to the cloud specifically, Whitworth and de Moor (2003) highlighted conflicts between data privacy and usability at an earlier point. While many of these have subsequently been addressed (Pearson et al. 2009), Stark and Tierney (2014) contend that data in the cloud is ‘still too mobile, too “promiscuous” and too often subject to inappropriate use or abuse’ (Stark and Tierney 2014, p. 6). They acknowledge that in today’s technological society, user autonomy and empowerment must be maximized, but argue that the “safety” of data should not be compromised and highlight mechanisms such as encryption which are widely used to foster privacy within information flows. They also assert that providers must

work to ensure data is “live” only when the user is “live” on the network: they stress that the “liveness” of data online, linked to the ‘input of the live user, ties decisions about stored online data to an individual’ (2014, p. 6). Stark and Tierney (2014) also detail cases where service providers track user information and use this for their own benefit and that of third parties, without the explicit permission or knowledge of users, highlighting that service providers may readily access user data and may also release such data to external agencies.

However, recent governmental policy decisions incorporate focus on such matters e.g. the UK Government’s Data Ethics Framework ‘sets out clear principles for how data should be used...It will help [organisations] maximise the value of data whilst also setting the highest standards for transparency and accountability when building or buying new data technology’ (The Centre for Information Policy Leadership 2018, p. 19). This framework for data ethics is in line with the fact that ‘the principle that personal data should be processed only in ways compatible with the specific purpose(s) for which they were collected is essential to respecting individuals’ legitimate expectations’ (European Data Protection Supervisor 2015, p. 10), thus confirming the idea that regulation should be ethically aware and informed, so that a human-centric use of data would be the only viable possibility.

6.3.2 *The Ethics of Providers of Cloud Computing Services*

The exploration of ethical and regulatory issues pertinent to data in cloud computing highlights how different stakeholders may have different vested interests in cloud computing and consequently encounter different kinds of ethical issues. Both cloud computing providers and cloud computing users are central to the discussion. Cloud computing providers may be regarded as those who offer cloud-based services and solutions to businesses and/or individuals. They provide virtual hardware, software, infrastructure and other related services. In turn, a cloud user may be regarded as someone who is available to (or who, lacking personal computing resources, necessarily needs to) surrender some control of the data he or she inputs in a system, on the basis that the user can trust the system itself.

For the cloud provider-user relationship to operate effectively, it is critical that cloud providers maintain the trust of users: when a user does not trust the system, he or she is less inclined to expose his or her vulnerability to the system and thereby less inclined to engage with it. The theme of

trust is therefore central to cloud computing, and this section begins by examining how ethics can promote the generation of trust, especially through the establishment of codes of ethics—which would need to be respected and enforced beyond the borders of country-based regulation (Sect. 6.3.2.1). The section then considers the perspective of providers regarding sustainability, and the extension of the discussion on “green” computing to cloud computing (Sect. 6.3.2.2). It also explores issues pertaining to the increasing concentration of power and the emergence of oligopolies in the cloud computing industry (Sect. 6.3.2.3).

6.3.2.1 *Codes of Ethics for Cloud Computing: Promoting Trust*

The accelerated velocity in cloud computing innovation makes it difficult for cloud computing regulators to keep pace with updating standards and guidance and for providers to ensure compliance while maintaining users’ trust. Indeed, while it may be debated that ‘certification, audits and a new generation of contractual clauses and binding corporate rules can help build a robust trust’ (EDPS 2015, p. 10), it may also be argued that ‘eliminating bureaucracy in data protection law, by minimising the requirements for unnecessary documentation to maximise room for more responsible initiative by businesses’ supported by additional broader guidance would be a more useful future initiative within the sector (EDPS 2015, p. 10).

In the wake of this call for a more responsible implementation of good practices—as opposed to a detailed menu of further regulations—it is interesting to consider the work of Whitehouse et al. (2016), who highlight that further major shifts in the cloud computing landscape are likely in the coming years and advocate heightened emphasis on ethics is necessary with respect to key stakeholders, namely providers and users. This, they suggest, is particularly important if certain behaviours on the part of these stakeholders are desirable into the future. They note that an ethics sufficiently robust to be able to withstand the intensity of the sector and capable of keeping pace with the inevitable developments in the sector is needed but has not yet been established. This, they assert, will help to generate increased trust on the part of users. The International Federation for Information Processing (IFIP) comprises more than 50 different Information and Communication Technology (ICT) global groups. One of their key foci is the societal and ethical challenges of cloud computing (Whitehouse et al. 2016). They assert that enhanced ethics offers many

further advantages for the cloud computing sector e.g. improved products and services, improved workplace behaviours, improved overall quality.

One of the potential key constituents for the promotion of a responsible way of building a culture of trust is the introduction of codes of ethics specific to cloud computing (Kouatli 2016). Whitehouse et al. (2016) describe how actors and organisations can make visible their ethical responsibilities and pledge to meet them in a transparent manner within codes. Codes may comprise both codes of conduct, which provide guidance in relation to personal conduct of individuals, and codes of ethics which go beyond the behaviour of individual actors, pertaining to organisations and wider sectoral behaviour. Both involve emphasis on moral guiding principles e.g. ‘Contribute to society and well-being’; ‘Be honest and trustworthy’; ‘Respect the privacy of others’; ‘Give proper credit for intellectual property’ (Association for Computing Machinery 1978 Code, cited in Whitehouse et al. 2016). Codes thereby are heavily influenced by Deontological Ethics, which focuses on particular imperatives that are typically constant over time. Codes normally also provide more contextual examples to explain how these imperatives might be applied and these examples might be updated periodically to illustrate the application of imperatives as pertinent issues change over time e.g. technological advances. However, codes also focus on balancing different stakeholders’ concerns, and, in so doing, incorporate key Utilitarianism components.

Codes have the capacity to support and affirm common standards that go beyond cultural differences of users. This is particularly important to the cloud computing sector, given its global context and the acknowledged difficulties in legislating and regulating in an international environment where different legal, cultural and operational norms may operate in the different jurisdictions and where trust considerations are dependent both on the sector and the country (Fujitsu Research Institute 2010).

Whitehouse et al. (2016) suggest that two-part codes of ethics might be considered, which distinguish between principles and guidance that are internationally acceptable and those that are locally feasible. It is likely that reporting of and monitoring of this guidance may be considered a local issue, given jurisdictional variations. Further, drafting of codes must be general enough to adapt to new and changing conditions without being so general that they cannot be of any practical use. They must also be specific enough to provide direction to relevant actors to the extent of being able to direct them and to also enable stakeholders to hold them to account.

Whitehouse et al. (2016) state that a further ‘conscientious, applied examination of key ethical and societal challenges ‘will continue to take place in the future both in practice and on practice’ (2016, p. 24) to ensure relevant codes can be maintained. However, it is also important to note that criticisms in relation to codes of ethics and their adoption (see e.g. Webley and Werner 2008) can be applied, *mutatis mutandis*, to cloud computing. It is also important to acknowledge that codes of ethics are often perceived as ineffective in changing organizational culture, being necessary but not sufficient measures to exert change in behaviours (Webley and Werner 2008).

6.3.2.2 *Green and Sustainable Cloud Computing*

Literature on cloud computing has developed notably with reference to “green” computing, which plays to a renewed societal interest in relation to protecting the environment. In some instances, the “green” issue is discussed to the extent that the relatively novel term, “greenwashing”, has been linked to this sector (Nanath in Moorthy et al. 2015). This refers to the marketing of cloud computing as more environmentally friendly than other tools, when in reality no substantial effort has been made to render it so. In a more extreme sense, “greenwashing” may even refer to an attempt to make something that is environmentally damaging appear to be environmentally friendly. This section reports different perspectives on cloud computing providers and their attention (or lack thereof) to environmentally sensitive issues.

Scott and Watson (2012) assert that new technologies such as cloud computing ‘provide unprecedented opportunities to improve the efficiency of business operations and represent a realistic opportunity to reduce energy costs and combat global warming’ (Scott and Watson 2012, p. 1). Di Salvo et al. (2017) go so far as to affirm that cloud computing is not only a green technology, but it is the “greenest.” They claim that the centralised aspects of cloud computing effectively facilitate the operation of a virtual machine system and storage of data in a manner that consumes less than half the energy and global resources required by traditional decentralised systems. Lin (2012) also examines “green” cloud computing and highlights that a well-considered scheduling strategy of the various information flows, combined with careful management of resource allocation, may further contribute to a more sustainable and green technology.

Buyya and Gill (2018) provide a more balanced discussion, arguing that while cloud computing reduces some discrete environmental

footprint, the wider data center industry may have a disproportionate negative environmental impact. In practice, hyperscale cloud data centers consume a disproportionate amount of energy—currently almost on a par with sectors such as the aviation sector—and are reaching technical limits. This negative impact of high carbon usage on global warming has been referred to as the “dark side” to cloud computing.

Bachour and Chasteen (2010, p. 1) refer to the ‘triple bottom line’ concept and the monitoring of ‘economic viability’, ‘social responsibility’ and ‘environmental impact,’ which they acknowledge may be difficult to define and measure. Scott and Watson (2012) urge caution in relation to monitoring and measuring green issues connected to cloud computing and other technologies. They assert that potential models for identifying and measuring such “green” components must consider a wide range of impacts, including direct financial impacts as well as broader societal impacts. They propose a framework which captures key stakeholders—societal, organizational, customer and supply-chain—and core value dimensions—economic, environmental, ethical and competitive position. Buyya and Gill (2018) advocate an alternative “green” model for holistic management of resources to ensure more energy-efficient and sustainable cloud operations in a bid to further decrease carbon footprints of cloud datacentres. Similarly, Di Salvo et al. (2017) note that the extent of “green” labelling has to date been based solely on energy consumption reduction and assert a more appropriate assessment of sustainable practices should also consider wider aspects such as eco-energy efficiency performance.

The duality of the cloud and its impact on the environment is thereby acknowledged: cloud computing has much potential to impact positively on discrete environmental matters; however, less positive ‘green’ computing considerations also need to be addressed. While most climate change activists are currently focused on limiting emissions from other sectors, such as the auto, aviation and energy sectors, the cloud computing industry may be on track to generate more carbon emissions than all of these sectors combined. It is therefore important that this “green” issue be even a more central component of the next generation of cloud (Garg et al. 2015; Lin 2012; Mohamed and Pillutla 2014; Murugesan 2008).

6.3.2.3 *Concentration of Power and Oligopolies in the Cloud Computing Industry*

As previously highlighted, the cloud overarches national and international borders and boundaries. Indeed, it may be observed that cloud computing has accelerated the pace of a truly global world (Mohamed and Pillutla 2014). While the cloud is offered to users all over the world, cloud computing as an industry is very much concentrated in the hands of a relatively small number of providers, akin to an oligopolistic market. These providers sustain the cost of the cloud infrastructure and decide on the cloud services provided. An issue commonly associated with oligopolies is the control that the small number of companies providing a specific good or service have on setting prices. This concern is also prevalent with regard to cloud computing: Feng et al. 2014 conduct an analysis of cloud providers' pricing strategy, addressing the cloud computer economic arena as an oligopoly market. Timmermans et al. (2010) assert that a significant amount of cloud computing innovation originates in the US. Synergy Research Group (Alley 2019) tracks such activity and reports that 38% of worldwide hyperdata centres are located in the US. It also reports that Amazon, Microsoft, Google, Alibaba and Oracle are the most active companies in this arena. These are effectively stockpiling information about consumers, presumably seeking to gain some competitive advantage in the process.

In these aforementioned contributions, there is no explicit mention of ethical issues associated with the concentration of power in a key industry such as cloud computing. Usually, ethical issues related to concentration of power regard the (un)fair treatment of the weak party in the economic agreement (Crane and Matten 2016) i.e. powerful oligopolies can establish terms and conditions that violate the rights of final users, who are effectively forced to accept them if they want to benefit from the service. Whatever the selected approach to ethics might be, a concentration of power is usually not in favour of the satisfaction of the greatest number of people (Utilitarianism), nor of the respect of established rules (Deontological Ethics).

Moreover, concentration of power which generates oligopolies is also responsible for spreading particular cultural influences. Timmermans et al. (2010) reflect on such trends within cloud computing and ponder if Western values may thereby dominate pertinent future applications, frameworks and regulations, and lead to 'increasing cultural homogenization' (2010, p. 5). This argument is discussed by Ess (2001) who posits that today's multicultural domains 'reflect an extensive diversity, if not

cacophony, of cultural identities, traditions, voices, views, and practices' (2001, p. 196) and asserts that it is critically important that cloud systems deal with such diversity in an ethical manner. However, if current trends continue, it is likely that Western perspectives will dominate into the future.

6.3.3 *The Ethics of Cloud Computing Users*

The ethical issues pertaining to users of cloud computing services predominantly relate to the way they use the services. Cloud users are the main stakeholders of cloud provider entities, being at the same time the most vulnerable element of the complex chain of interactions that cloud computing services entail. With reference to the ultimate technical capabilities and limitations imposed by the different cloud systems, users decide how to interact relative to the context in which they find themselves. One means of understanding the perspective of users of cloud computing services is to engage with the term "prosumers." The expression was coined in 1980 by Alvin Toffler (Toffler 1980), and refers to consumers who, simultaneously, are also producers. The European Data Protection Supervisor discusses this term in relation to the end users of new technologies, including cloud computing. The associated reference to prosumers relates to one of the pillars for a new digital ethics: the empowerment of individuals using technologies. Consumers are no longer passive receptors of the available good or service; rather, they co-create the product present in digital platforms. As a result, the empowerment of twenty-first century prosumers is meant to increase their technological and ethical awareness. This perspective of empowerment is a top-down approach, where regulators are attempting to provide tools to strengthen the role and responsibility of individual users of digital platforms.

An alternative perspective on users' awareness of their digital presence is to consider how individuals can empower themselves, without the support of a regulatory authority. Cloud users themselves can learn how to engage with the cloud environment by developing intellectual and practical habits that may be examined through the lens of the epistemic virtues. De Bruin and Floridi (2017) examine epistemic virtues, also referred to as informational or knowledge virtues, in light of the specific circumstances that cloud computing users encounter. They highlight that users must be able to make informed decisions in relation to their engagement with cloud services. To enable such informed decisions, there must be clarity of communication between the two parties i.e. between providers and users. De Bruin and Floridi (2017) note current barriers to communication

within the industry whereby terms of usage are written in lengthy and complex legal jargon which many people do not readily understand.

De Bruin and Floridi (2017), building on the work of Kawall (2002) and De Bruin (2015), ultimately characterize the virtue of “interlucency” as the other-regarding epistemic virtue that helps establish a common knowledge through providing the relevant information in a language that can be understood and shared by the interested users. More than the virtue of a single cloud user, the epistemic virtue of interlucency, according to De Bruin and Floridi, must be applied to the cloud computing industry as a whole. To ground their contribution, the authors make explicit reference to the concept of “comprehensibility” as formulated by Habermas (quoting Habermas 1981).

De Bruin and Floridi (2017) further discuss users’ attitudes. They suggest that users should be intellectually impartial, sober and courageous. Intellectual impartiality applies to users insofar as they are able to overcome personal prejudices towards the cloud computing industry and the possible risks connected to the circulation of their data. They may attempt to do so by listening to authoritative voices in the field of technology and by seeking information from independent experts. Intellectual sobriety helps users to ‘resist the overly enthusiastic adoption of beliefs about either the pros and the cons of cloud computing’ (2017, p. 29). Intellectual courage concerns the continuous active attitude to overcome ignorance and lack of information even when faced with obstacles. The authors assert that users must continue to ask questions when something is not clear, for example the terms and conditions of a specific service.

It is interesting to note how De Bruin and Floridi (2017) articulate in favour of “proscriptive pressure” on the side of users more than on the side of the providers of cloud services: in so doing, they are actually interpreting one of the main ethical issues associated with the relationship between technology and the use of technology. Indeed, the authors place emphasis on the freedom of the agent and on his/her responsibility to make the best use of technology without limiting the possibility of technology developers to advance their discoveries, highlighting that the ethical boundaries of technological advances should be determined in relation to the way they are used, not by what they can potentially do. For example, a terrorist organization can benefit from services available in the cloud, however the objective for which it uses this service is illegal and contrary to the good of society.

6.4 CONCLUSIONS

The chapter offers an overview of ethics and prominent ethical theories, which can help to chart existing literature in relation to ethics and cloud computing. One of the key findings of this analysis is that the contributions aimed at addressing ethical issues in cloud computing do not explicitly refer to a specific conception of ethics, nor explicitly declare a reference point for their analysis from an ethical perspective. It was therefore not possible to structure the chapter in line with the different schools of ethics, and required analyses to focus on recurring topics within selected cloud computing literature. Given the complex multi-stakeholder cloud computing environment, ethical issues particular to cloud computing were distinguished in relation to three categories: data, providers and users.

With reference to data, issues related to ownership, security and privacy were discussed. The cloud computing literature in this context is particularly technical and oriented to address the legal framework of pertinent data issues. Further research in relation to data ethics in cloud computing may be inspired by the seminal work conducted in the parallel field of data ethics and algorithm ethics. In addition, the methodology of social ethics could be useful to conduct research on the way the society of the future will store and manage data via cloud computing technology. This research could explore the different kinds of society that could result depending on the quality and quantity of individual and collective data available and how human beings could live in these kinds of societies. Another interesting direction that the research about data ethics in cloud computing might take is suggested by Koehn (2019). In the context of the new technologies of the twenty-first century, she argues that it is worth reflecting on Plato's Socratic notion of responsibility: this notion is essentially dialogic and goes beyond the concept of responsibility typical of the Anglo-American culture, which perceives responsibility as part of a role-based duty. This personalization of responsibility can help those who manage data on others' behalf, so that they do not limit themselves to what is prescribed by their role, but are able to see the relational component of their role towards the people on the cloud platform, considering them as people and not as a set of data.

With reference to the ethical issues related to cloud computing service providers, codes of ethics, green and sustainable cloud computing, and concentration of power were examined. Future research in sustainability and oligopolies in cloud computing may consider studies such as those conducted in mainstream literature regarding these topics, while ethics

and cloud computing literature might explore further possibilities for writing and implementing codes of ethics, and may seek to examine the experiences (and failures) of other sectors in this regard.

As regards ethical issues pertaining to cloud users, the perspectives of individual empowerment and epistemic virtues were explored. Very few authors have dedicated attention to these important areas. A possible pathway for future research may be an application of ancient Aristotelian ethics to the new technological environment: while the context may have profoundly changed, the fundamental attitudes and questions of human beings still remain and the ethics and cloud computing literature could benefit from the wisdom of one of the first ethical theories formulated.

It may be argued that the pace of academic publications, while slower than cloud computing innovation, is still relatively rapid. It must be acknowledged that the majority of contributions examined in this chapter report specific perspectives on focussed topics in the cloud computing domain, without delving further into the theoretical foundations of their ethical analysis. It is anticipated that the structure and articulation of this chapter will aid the reader to understand how a multi-stakeholder ethical analysis is needed in order to appropriately examine the multi-stakeholder context within the cloud computing domain. The aforementioned categories selected for this review are interrelated and overlapping, and highlight factual complexities. The cloud providers and users must be mindful that they shape the morality of the cloud computing context through their interactions with the other stakeholders and with the platform itself, and they must not abdicate their responsibilities to the possibilities offered by the technology. Providers must be accountable, not only to the final users of their platforms, but also to the environment, and to the cultural context within which the platforms operate. It must also be remembered that regulation, although continuously evolving, is unlikely to advance at the pace of cloud computing innovation and this review clearly illustrates that ethics is an integral component to orient cloud computing towards the good of society into the future.

REFERENCES

- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, 305, 357–383. <https://doi.org/10.1016/j.ins.2015.01.025>.
- Al-Khouri, A. M. (2012). Data Ownership: Who Owns “My Data”? *International Journal of Management Information Technology*, 2(1), 1–8. <https://doi.org/10.24297/ijmit.v2i1.1406>.

- Alley, A. (2019, October 18). *Synergy: There Are More Than 500 Hyperscale Data Centers in the World*. Retrieved from <https://www.datacenterdynamics.com/news/synergy-there-are-more-500-hyperscale-data-centers-world/>
- Annas, J. (1993). *The Morality of Happiness*. Oxford University Press. <https://doi.org/10.1093/0195096525.001.0001>.
- Aristotle. (2000). *Nicomachean Ethics*. Cambridge, UK and New York: Cambridge University Press.
- Bachour, N., & Chasteen, L. (2010). *Optimizing the Value of Green IT Projects within Organizations*. 2010 IEEE Green Technologies Conference, pp. 1–10. <https://doi.org/10.1109/GREEN.2010.5453804>
- Bartolini, C., Santos, C., & Ullrich, C. (2018). Property and the Cloud. *Computer Law & Security Review*, 34(2), 358–390. <https://doi.org/10.1016/j.clsr.2017.10.005>.
- Bowers, K. D., Juels, A., & Oprea, A. (2009). *HAIL: A High-Availability and Integrity Layer for Cloud Storage*. Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 187–198. <https://doi.org/10.1145/1653662.1653686>
- Buyya, R., & Gill, S. S. (2018). Sustainable Cloud Computing: Foundations and Future Directions. *Business Technology & Digital Transformation Strategies*, 21(6), 1–9.
- Cavoukian, A. (2008). Privacy in the Clouds. *Identity in the Information Society*, 1(1), 89–108. <https://doi.org/10.1007/s12394-008-0005-z>.
- Constantine, D. (2012). Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both. *Georgia State Law Review*, 49(4), 499–528.
- Crane, A., & Matten, D. (2016). *Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization* (4th ed.). Oxford: Oxford University Press.
- Crimmins, J. E. (2019). Jeremy Bentham. In E. N. Zalta (Ed.), *Stanford Encyclopedia of Philosophy*. Retrieved from <https://plato.stanford.edu/archives/sum2019/entries/bentham/>
- De Bruin, B. (2015). *Ethics and The Global Financial Crisis: Why Incompetence Is Worse Than Greed*. Cambridge: Cambridge University Press.
- de Bruin, B., & Floridi, L. (2017). The Ethics of Cloud Computing. *Science and Engineering Ethics*, 23(1), 21–39. <https://doi.org/10.1007/s11948-016-9759-0>.
- Di Salvo, A. L. A., Agostinho, F., Almeida, C. M. V. B., & Giannetti, B. F. (2017). Can Cloud Computing Be Labeled as “Green”? Insights Under an Environmental Accounting Perspective. *Renewable and Sustainable Energy Reviews*, 69, 514–526. <https://doi.org/10.1016/j.rser.2016.11.153>.
- Ess, C. (2001). Culture and Global Networks: Hope for a Global Ethics? In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy*

- (pp. 195–225). Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9780511498725.012>.
- European Commission. (2018). *General Data Protection Regulation*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:43:FIN>
- European Data Protection Supervisor. (2015, September 11). *Towards a New Digital Ethics*. Retrieved from https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf
- Feng, Y., Li, B., & Li, B. (2014). Price Competition in an Oligopoly Market with Multiple IaaS Cloud Providers. *IEEE Transactions on Computers*, 63(1), 59–73. <https://doi.org/10.1109/TC.2013.153>.
- 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. <https://doi.org/10.4038/ictcr.v4i2.4674>.
- Floridi, L., & Taddeo, M. (2016). What is Data Ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), 20160360. <https://doi.org/10.1098/rsta.2016.0360>.
- Fujitsu Research Institute. (2010). *Personal Data in the Cloud: A Global Survey of Consumer Attitudes*. Retrieved from https://www.fujitsu.com/uk/Images/fujitsu_personal-data-in-the-cloud.pdf
- Garg, S., Dwivedi, R. K., & Chauhan, H. (2015). *Efficient Utilization of Virtual Machines in Cloud Computing Using Synchronized Throttled Load Balancing*. 2015 1st International Conference on Next Generation Computing Technologies (NGCT), pp. 77–80. <https://doi.org/10.1109/NGCT.2015.7375086>
- Grimes, J. M., Jaeger, P. T., & Lin, J. (2009). *Weathering the Storm: The Policy Implications of Cloud Computing*. Illinois Digital Environment for Access to Learning and Scholarship Conference.
- Habermas, J. (1981). *Theorie des kommunikativen Handelns*. Frankfurt am Main: Suhrkamp.
- Herschel, R., & Miori, V. M. (2017). Ethics & Big Data. *Technology in Society*, 49, 31–36. <https://doi.org/10.1016/j.techsoc.2017.03.003>.
- 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.
- Izang, A. A., Adebayo, A. O., Okoro, O. J., & Taiwo, O. O. (2017). Security and Ethical Issues to Cloud Database. *The Journal of Computer Science and Its Applications*, 24(2), 65–75.
- Kawall, J. (2002). Other—Regarding Epistemic Virtues. *Ratio*, 15(3), 257–275. <https://doi.org/10.1111/1467-9329.00190>.
- Koehn, D. (2019). *Toward a New (Old) Theory of Responsibility: Moving beyond Accountability*. <https://doi.org/10.1007/978-3-030-16737-0>

- Kouatli, I. (2016). Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management. *Procedia Computer Science*, 91, 412–421. <https://doi.org/10.1016/j.procs.2016.07.110>.
- Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, 125, 691–697. <https://doi.org/10.1016/j.procs.2017.12.089>.
- Lin, C. (2012). A Novel Green Cloud Computing Framework for Improving System Efficiency. *Physics Procedia*, 24, 2326–2333. <https://doi.org/10.1016/j.phpro.2012.02.345>.
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, 3(2), 205395171667967. <https://doi.org/10.1177/2053951716679679>.
- Mohamed, M., & Pillutla, S. (2014). Cloud Computing: A Collaborative Green Platform for the Knowledge Society. *VINE*, 44(3), 357–374. <https://doi.org/10.1108/VINE-07-2013-0038>.
- Moorthy, J., Lahiri, R., Biswas, N., Sanyal, D., Ranjan, J., Nanath, K., & Ghosh, P. (2015). Big Data: Prospects and Challenges. *Vikalpa: The Journal for Decision Makers*, 40(1), 74–96. <https://doi.org/10.1177/0256090915575450>.
- Murugesan, S. (2008). Harnessing Green IT: Principles and Practices. *IT Professional*, 10(1), 24–33. <https://doi.org/10.1109/MITP.2008.10>.
- Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.
- Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, 140(4), 32–48.
- Pearson, S., Shen, Y., & Mowbray, M. (2009). A Privacy Manager for Cloud Computing. In M. G. Jaatun, G. Zhao, & C. Rong (Eds.), *Cloud Computing* (Vol. 5931, pp. 90–106). Heidelberg: Springer. https://doi.org/10.1007/978-3-642-10665-1_9.
- Reed, A., Rezek, C., & Simmonds, P. (Eds.). (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3. 0*. Retrieved from <https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf>
- Schiffman, J., Moyer, T., Vijayakumar, H., Jaeger, T., & McDaniel, P. (2010). *Seeding Clouds with Trust Anchors*. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop—CCSW'10, p. 43. <https://doi.org/10.1145/1866835.1866843>
- Scott, M., & Watson, R. (2012). *The Value of Green IT: A Theoretical Framework and Exploratory Assessment of Cloud Computing*. BLED 2012 Proceedings, p. 30.
- Stark, L., & Tierney, M. (2014). Lockbox: Mobility, Privacy and Values in Cloud Storage. *Ethics and Information Technology*, 16(1), 1–13. <https://doi.org/10.1007/s10676-013-9328-z>.

- Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, 34(1), 1–11. <https://doi.org/10.1016/j.jnca.2010.07.006>.
- Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, 10(7), 190903. <https://doi.org/10.1155/2014/190903>.
- Tanenbaum, A. S., & van Steen, M. (2016). *Distributed Systems: Principles and Paradigms* (2nd ed., adjusted for digital publishing). Leiden: Maarten van Steen.
- The Centre for Information Policy Leadership. (2018). *The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society*. Retrieved from https://www.informationpolicycentre.com/uploads/5/7/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf
- Timmermans, J., Stahl, B. C., Ikonen, V., & Bozdag, E. (2010). *The Ethics of Cloud Computing: A Conceptual Review*. 2010 IEEE Second International Conference on Cloud Computing Technology and Science, pp. 614–620. <https://doi.org/10.1109/CloudCom.2010.59>
- Toffler, A. (1980). *The Third Wave* (1st ed.). New York: Morrow.
- US Government. (1986). *Electronic Communications Privacy Act*. Retrieved from <https://www.justice.gov/jmd/electronic-communications-privacy-act-1986-pl-99-508>
- van den Hoven, J. (2008). Moral Methodology and Information Technology. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 49–67). Hoboken, NJ: Wiley. <https://doi.org/10.1002/9780470281819.ch3>.
- Webley, S., & Werner, A. (2008). Corporate Codes of Ethics: Necessary But Not Sufficient. *Business Ethics: A European Review*, 17(4), 405–415. <https://doi.org/10.1111/j.1467-8608.2008.00543.x>.
- 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. <https://doi.org/10.1145/2874239.2874242>.
- Whitworth, B., & De Moor, A. (2003). Legitimate by Design: Towards Trusted Socio-Technical Systems. *Behaviour & Information Technology*, 22(1), 31–51. <https://doi.org/10.1080/01449290301783>.
- Zissis, D., & Lekkas, D. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems*, 28(3), 583–592. <https://doi.org/10.1016/j.future.2010.12.006>.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.