Ethical Decision-Making Skills for Responsible Citizens of Cyberspace: Quo Vadis?

Laurette Pretorius
Andries Barnard

Abstract

Apart from being able to identify ethical problems, computing professionals need to be able to analyse ethical problems that arise in the computing context in general, and also in the development of software artefacts for solving real problems in particular. Furthermore, they should have the knowledge and skills to decide on ethical courses of action in resolving such problems. This paper focuses on such ethical decision making skills in the context of cyberspace.

1. Introduction

If we agree that computing ethics is that branch of applied philosophy that *"instructs computing specialists on how best to lead their professional lives"* (Lenarcic, 2003), then computing professionals should be equipped with the relevant and appropriate knowledge and skills for this purpose. If we further agree that the computing profession concerns, among others, the development of software artefacts for solving real problems, a mere ethical awareness is not sufficient. Computing professionals need to be able to not only identify ethical problems that arise, but also to analyse them and to decide on ethical courses of action in resolving such problems. This paper focuses on such ethical decision making skills in the context of cyberspace.

In section 2 we provide the context by elaborating on what we mean by *'cyberspace'* and other related terms, on whom the citizens of cyberspace are, and what we mean by the term *'responsible'*. Section 3 concerns a methodology for ethical analysis as well as a number of

Alternation 12.1a (2005) 171-195 *ISSN 1023-1757*

relevant and well-known ethical theories, while section 4 focuses on frameworks and procedures for practical ethical decision-making. This is followed by a discussion of two examples. A framework for ethical decision-making is applied to these two examples, one that deals with the analysis of human behaviour particular to the field of computing, while the other deals with an analysis of software agent behaviour. In section 5 we briefly consider possible challenges of the future, in particular the evolution of cyberspace as nanotechnology, ubiquitous computing and ambient intelligence develop, and what this may or would mean in terms of ethical decision-making.

2. The Context

In order to contextualise the subsequent discussion of ethical decision-making skills, the terms occurring in the title, as well as a number of other related concepts, are clarified.

2.1 What is Cyberspace?

The term "cyberspace" was coined by William Gibson in his novel Neuromancer. The "*word Cyberspace is currently used to describe the whole range of information resources available through computer networks*" (Web Hosting Directory, 2005). For the purposes of this paper we thus consider *cyberspace* to be the realm that owes its existence to the global connectivity of networks such as the Internet as well as those global networks constituted by ubiquitous computing technology and devices. Cyberspace is rapidly rendering itself as a central part of early 21st century life.

2.2 Who Are the Citizens of Cyberspace?

In order to explore the implications and consequences of this reality for us as human beings, and as computing professionals in particular, we need to reflect on the entities that populate cyberspace. We distinguish between two classes of citizens of cyberspace, namely *human users* and *software entities*, in particular *software agents*, present in Internet and ubiquitous computing applications. For the purposes of this discussion, we concur with the definition of Fou (2001) that a

software agent is *"a piece of software that has the capacity to autonomously conduct its work."* Such an agent may be autonomous, can act, its actions are specified beforehand, it operates within some environment (in this case cyberspace), and its position within the environment is not necessarily fixed. For a more detailed discussion on this topic, the reader is referred to the exposition of (Smith, Eloff, Venter, Barnard and Pretorius, 2003). Agents form an integral part of cyber society, and as such they interact with one another, as well as with the human citizens of cyberspace (Wagner, 2000). Indeed, we should take clear cognizance of the fact that humans share cyberspace with *software agents*, artificial beings *created by computing professionals*. This means that, apart for the traditional and often expected interaction of human-to-human in cyberspace, software agents deployed in cyberspace now expand the class of entities that can be involved in interactions and, therefore, moral situations (Floridi and Sanders, 2001).

2.3 What is a Responsible Citizen of Cyberspace?

The term *'responsible'* is defined by The Shorter Oxford English Dictionary (1955) as *"answerable or accountable to another for something; morally accountable for one's actions; capable of rational conduct; capable of fulfilling an obligation or trust; reliable or trustworthy"*. The term *'moral'* means *"of or pertaining to the distinction between right and wrong, or good and evil, in relation to actions, volitions or character"* while *'ethics'* is defined as *"the science of morals"*. So, ethics is the *discipline* relating to right and wrong, moral duty and obligation, moral principles and values, and to moral character. Ethics and morality are therefore not synonymous terms, although both refer to customs in their original Greek and Latin respectively (Beck, 2003). The Greek term *'ethics'* also implies character, whereas *'mores'* refers to social customs. We return to this in section 3.1.

In physical space the regulation of our complex society is achieved by various means including ethical, moral and legal systems. The proper functioning of these systems heavily relies on the responsible behaviour of the members of this society. Moreover, in a similar way

the regulation of the equally complex cyberspace society requires regulation, the success of which also relies on the responsible behaviour of its citizens, human and artificial alike.

Tavani (Gruba, 2004) broadens the concept of ethics as defined in The Shorter Oxford English Dictionary (se above) and describes *cyberethics* as the *"study of moral, legal and social issues involving cybertechnology"*, with cybertechnology including the Internet as well as those global networks constituted by ubiquitous computing technology. Moreover,

- privacy,
- property,
- liability,
- security, as well as
- freedom (of choice, speech and values)

constitute the *five ethical dimensions* of cybertechnology, and together characterise the *integrity* of cyberspace (Gruba, 2004; Spinello and Tavani, 2001).

So, in reflecting on what it means to be a responsible citizen of cyberspace, we ultimately need to consider the ethical, moral and legal principles that apply to *both* human *and* software agent activity in cyberspace. A detailed discussion of this falls outside the scope of this paper; see for example (Van der Merwe, Pretorius and Barnard, 2004). What is, however, relevant here, is the multi-faceted role that the computing professional plays in this regard. What exactly is this role and how does it impact on the regulation of cyberspace?

2.4 The Dual Role of the Computing Professional

We may describe the role of computing professionals in the context of cyberspace as that of informed and critical *users* of cybertechnology as it evolves, on the one hand, and as designers, *creators* and developers of this technology and the software agents and applications that populate cyberspace, on the other. This dual role clearly has sig-

nificant implications in terms of the responsibility of computing professionals as citizens of cyberspace. Floridi and Sanders (2003) who use the term *agent* for what we here refer to as the computing professional, furthermore state that *"ethics is not only a question of dealing morally well within a given world. It is also a question of constructing the world, improving its nature and shaping its development in the right way. This proactive approach treats the agent as a world owner, a game designer or referee, a producer of moral goods and evils, a provider, a host, or a creator. ... A mature moral agent is commonly expected to be both a morally good user and a morally good producer of the environment in which she operates."*

Indeed, Lenarcic (2003) goes so far as to say that *"[s]oftware developers in particular potentially wield immense virtual power and should be mindful of their artifacts' long-term consequences."* These important facets of the computing professional's professional life provide the impetus for this, and related research.

2.4.1 Regulating Cyberspace: Ethics, Morality and Law Perspective

Gleason and Friedman (2003) argue that *"the development of particular cyberspatial norms"* will benefit all of the actors involved in online collaboration. They furthermore state that *"efforts should be made to articulate a conceptual model of cyberspace that respects its unique attributes – one that is accessible to both the actors that will take lead organizing and regulating cyberspace, and, more importantly, the citizens of the world who will hold those actors accountable"*. We view the computing professional as playing a leading role in this sense. In this paper we specifically focus on norms for and the ethical behaviour of computing professionals as direct actors, but also indirectly as creators of software agents.

As intimated by Gleason and Friedman (2003), the **actions** performed by both human and software agents within their community, should be constrained in order not to jeopardise the integrity of cyber-

space community. It is thus important that both human and software agents respect these fundamental criteria, namely privacy, property, liability, security, and speech and values.

Successful regulation of cyberspace, as of any system, is largely based on the assumption of individual and collective responsibility and spans the conceptual continuum of personal ethics, public morality and external regulation by means of, among others legislation. One can argue that responsible citizens of cyberspace should act ethically, have high moral values and are law-abiding.

2.4.2 Regulating Cyberspace: Lessig's Perspective

A different, but not unrelated perspective on the regulation of cyberspace is Lessig's paradigm as discussed by Spinello (2003), which distinguishes the following four modalities of regulation of cyberspace, namely:

- law;
- norms;
- the market; and
- architecture (Lessig originally used the term code).

Lessig, as quoted in Spinello (2003), claims that *"the architectures of cyberspace are as important as the law in defining and defeating the liberties of the Net"*. Lessig (1999) is furthermore concerned about the regulative force of architecture (code) because, in his opinion *"while laws are transparent, code is obscure"*. This paradigm puts even more emphasis on the role of code, and therefore on the dual role and responsibility of the computing professional in cyberspace. This affords some priority to the formulation of software development standards for the ethical behaviour of software agents. We argue that, with respect to Lessig's concerns, the formulation of such standards to regulate software agent behaviour is of equal importance to the promulgation of laws to regulate human behaviour. In this respect we have

explored related concerns in (Smith, Eloff, Venter, Barnard and Pretorius, 2003) and proposed an architectural framework to be used by software developers in (Barnard, Cloete and Pretorius, 2004).

Legislation in itself is certainly not sufficient to guarantee acceptable normative behaviour in cyberspace. Lessig (1999) argues that human agents in cyberspace need to demonstrate ethical and moral principles and behaviour if they do not want to compromise their freedom of choice (one of the five ethical dimensions that constitute the integrity of cyberspace, section 2.3). In particular he is concerned that designers of software and hardware might increasingly resort to his modality of architecture for the purposes of regulation, because they do not consider any of the other modalities to be effective (Lessig, 1999).

Recently, Gleason and Friedman (2004) argued that *"[w]ithout a basic framework for understanding, the higher-order process of decision-making becomes difficult – virtue can be threatened by that which we do not understand"*. It is within this context that the computing instructor should not only equip the computing professional of the future with a commensurate level of technological knowledge and understanding of cyberspace, but also with the necessary skills of ethical and moral decision-making in order to ensure the *integrity of cyberspace*. In the following sections we explore some of these skills and frameworks for ethical and moral decision-making.

3. Ethical Decision-Making: Theory

3.1 Background

The discussion of morals is probably as old as language itself. We know that Socrates and Plato, among others, contemplated moral issues and questions at length, but Aristotle was the first to undertake a serious and systematic study of moral principles and employed the term *'ethics'* in his discourse (see, for example Beck, 2003). Aristotle viewed *"ethical theory as a field distinct from the theoretical sciences"*, with a methodology *"that must match its subject matter –*

good action" (Kraut, 2001). In other words, *"[b]ecause ethics is a practical rather than a theoretical science, Aristotle also gave consideration to the aspects of human nature involved in acting and accepting moral responsibility. Moral evaluation of an action presupposes the attribution of responsibility to a human agent"* (Kemerling, 2001).

Summarising, ethics is a practical science concerned with good actions and good actions can only result from good decisions, which, in turn, require systematic evaluation and responsible decision-making. In order to apply this line of reasoning to cyberspace and its citizens, we need to address the questions of:

1. what is *'good'* and
2. how a citizen of cyberspace could arrive at an appropriate *decision*.

3.2 What Is Good?

The first question is addressed by briefly discussing some of the better-known ethics theories that may be applied in the analysis of ethical behaviour. In this respect we review the basic principles of two deontological theories, viz. duty-based and rights-based ethics, the teleological theory of utilitarianism (Spinello, 1997), and the theory of just consequentialism (Moor, 2001). Note that these theories need to be discussed in the context of cyberspace.

3.2.1 Duty-Based Ethics Theory

The duty-based ethics of Kant may be summarized as *"the absolute principle of respect for other"* entities (i.e. the citizens of cyberspace) that *"deserve respect because of their rationality and freedom"* (Spinello, 1997: 34). Rananu, Davies and Rogerson (Maner, 2002b) suggest that answers to the following (relevant) questions should be considered with regards to the action of the citizen of cyberspace:

- Fidelity: Is there a promise that should be kept in contemplating or performing some action?

- Reparation: Is there a wrong that should be righted due to the contemplation or performance of said action?
- Justice: Should the outcome of the action be fair?
- Beneficence: Can the lot of others be improved as a result of the contemplation or performance of the action?
- Gratitude: Is an expression of gratitude due to the performance of an action appropriate?
- Non-injury: Can others be protected from injury or harm due to the contemplation or performance of said action?

3.2.2 Rights-Based Ethics Theory

This approach focuses on individual rights and respect for these rights which are equal. According to Spinello (1997: 39) everyone (i.e. all the citizens of cyberspace), *"for example, equally shares in the rights to life and liberty regardless of their nationality or status in society"*. Rananu, Davies and Rogerson (Maner, 2002b) suggest that answers to the following questions should be considered, i.e. is the right of the cybercitizen:

- to know respected?
- to privacy respected?
- to property respected?

3.2.3 Consequence-Based Ethics Theory

Utilitarianism is a widely used form of consequentialism (Spinello, 1997: 27). For the purposes of this paper, we concur with Spinello (1997: 28) that *"utilitarianism is the moral doctrine that an action is morally right if it produces the greatest happiness for the greatest number of"* entities (cybercitizens) *"affected by it"*. One thus needs to determine which cybercitizens would be affected by the contemplation or performance of an action, and to what degree.

3.2.4 Just Consequentialism

Moor (2001) summarises the theory of just consequentialism to imply that the ends, however good, *"do not justify using unjust means"*. Regarding the contemplation, and in particular the performance of some action, one would thus need to determine whether unjust means would be required to facilitate performance of the action by the cybercitizen in question. Therefore, if it is not possible to achieve the envisaged end (performance of the action) without utilizing unjust means, the requirement of just consequentialism is not satisfied.

3.3 How to Decide?

The second question concerns the process by which an agent may arrive at an ethical decision. We follow Spinello (2003, pp. 17-18) who proposes a general three-step approach based on human intuition, a critical normative evaluation and public policy implications. This methodology encompasses the two complementary practical approaches toward ethical decision making in developing information systems, discussed in (Wu, Rogerson and Fairweather, 2001). In particular Wu et al. (2001) first consider the methodological or procedural approach, founded on prescribed procedures, steps or stages, as the basis for ethical decision-making. Secondly, they discuss the approach of placing emphasis on the personal moral character and mature ethical judgement of individuals. Their conclusion is that the combination of these two approaches represents *"an effective and practical paradigm for examining or evaluating ICT workers' ethical activities or performance in developing information systems"* (Wu et al., 2001).

In this respect, we are of the opinion that Spinello's methodology also applies in the context of cyberspace. In particular, Spinello's methodology makes provision for all five positions regarding the foundations of computer ethics to be found in (Floridi and Sanders, 2003):

- no resolution approach (computer ethics has no foundation);

- professional approach (computer ethics is solely a professional ethics);
- radical approach (computer ethics deals with absolutely unique issues);
- conservative approach (computer ethics is only a particular applied ethic); and the
- innovative approach (computer ethics expands the meta-ethical discourse with a substantially new perspective).

We contend that ethical decision-making by (intelligent, autonomous) software agents is a relatively new and complex topic, and we illustrate this briefly with an example in a subsequent section.

3.3.1 Spinello's General Approach to Ethical Decision-Making

As a general methodology we focus on Spinello's (2003, pp. 17-18) general three-step approach based on:

- human intuition;
- a critical normative evaluation; and
- public policy implications.

The first step in this approach of Spinello relies on the informal ethical and moral disposition and sense of integrity of the decision-maker – representing the moral character and maturity of judgement, as referred to by (Wu et al., 2001). For the purposes of this paper we assume that the computing professional is responsible, i.e. ethically and morally sensitive, in the sense previously discussed, and has been sensitised to the importance of computing ethics, see for example (Barnard, De Ridder, Pretorius and Cohen, 2003).

Secondly, a critical normative evaluation is conducted within the context of a chosen ethical theory, a number of which are discussed below. Although responsible human beings are *assumed* to be capable of acceptable moral and ethical judgement, heuristics and procedural guidelines for making ethical decisions in complex situations are use-

ful and even suitable, particularly in the case of computing professionals adept to procedural thinking. Indeed, *"[t]he search for useful analytical heuristics has been a common theme in applied ethics for many years. ... Within computer ethics, heuristics have been of early and continuous interest."* (Maner, 2002a). We return to one such heuristic framework in subsequent sections.

Thirdly, public policy implications as embodied in legal and organisational rules of conduct, and codes of ethics are investigated and appropriately applied. A detailed discussion of such policies falls outside the scope of this paper. We do, however, contend that (future) computing professionals should acquaint themselves with the legislation and codes of ethics that apply in their specific circumstances. Of special significance in the South African context is the Electronic Communications and Transactions Act (Act 25 of 2002), see for example (Barnard, Pretorius and Venter, 2004)

4. Ethical Decision-Making: Practice

From a practical perspective, ethical decision-making may be described as a process of (Gruba, 2004):

- identifying a problem;
- generating alternatives; and
- choosing among them.

The alternatives selected above should maximize the most important ethical values while achieving an intended goal.

Wu et al. (2001) claim that *"more and more ethicists and computing professionals have focused their attention on the possibility and viability on applying ethics in the field of ICT through various methods or procedures."* In this respect Maner made a significant contribution in his paper entitled *Heuristic Methods for Computing Ethics* (Maner, 2002a) and supplemented this paper by a website that extensively covers procedures for ethical decision-making (Maner, 2002b). In our opinion these two contributions of Maner are of practical use to both

the computing instructors who want to systematically introduce their students to practical ethical decision-making, as well as to the responsible computing practitioner who requires procedural and practical decision-making assistance in complex real-life situations, particularly in cyberspace. Below we illustrate how one such procedure can be applied for ethical decision-making pertaining to human users and software agents as citizens of cyberspace.

4.1 A Framework for Ethical Decision-Making

Regarding an ethical analysis of cybercitizen behaviour we use the *Five-step Process of Ethical Analysis* of Rananu, Davies and Rogerson (Maner, 2002b) as basis. Other similar procedures for ethical analysis may be found in Maner (2002a and 2002b). The analysis procedure of Rananu, Davies and Rogerson, originally designed primarily for the analysis of human behaviour and ethical decision-making, was chosen because it can be readily applied to the ethical analysis of cybercitizen behaviour in general. For the purposes of this paper we *modify this process* to be *applicable in cyberspace* as outlined below:

4.1.1 Step 1: Analysis of the Scenario

In analysing the behaviour of a citizen of cyberspace, the following must be considered:

What are the facts?

Who are the stakeholders?

Identify relevant ethical and social issues.

4.1.2 Step 2: Application of Appropriate Formal Guidelines

In analysing the behaviour of a citizen of cyberspace, the following must be considered:

- Consider common themes for corporate or professional codes of conduct; see (Maner, 2002b) for more details.

- Does the behaviour of the citizen of cyberspace conform to or violate the Golden Rule that states, *"do unto others as you would have them do unto you"* (Spinello, 1997: 37)
- Who benefits from or is harmed by the actions of the cybercitizen?

4.1.3 Step 3: Application of Ethics Theories

We propose the use of the four ethics theories presented in sections 3.3 through 3.6 and refer the interested reader to (Maner, 2002b) for more details.

4.1.4 Step 4: Application of Relevant Laws

In analysing the behaviour of a citizen of cyberspace, the following must be considered:

Laws passed to regulate the information industry and cyberspace.

The rare law that enforces unethical behaviour.

4.1.5 Step 5: Application of Informal Guidelines

Rananu, Davies and Rogerson (Maner, 2002b) suggest that answers to the following appropriate informal questions should be considered where applicable:

- Recall your first impressions or reactions and what your moral intuition said about the action?
- Apply the mother test: Would you tell her? Would she be proud or ashamed?
- Apply the TV test: Would you inform the entire cyberspace community of your actions?
- Apply the Other Person's Shoe test: What if the roles were reversed?
- Apply the market test: Could you advertise the act to give you a marketing edge?

4.1.6 Step 6: Make a Defensible Decision

An ethical conclusion regarding the cybercitizen's actions and behaviour can be made based on the above five steps.

4.2 Example 1: Human Behaviour

In (Pretorius & Barnard, 2004) a detailed case study regarding the unethical use of e-mail facilities by computing professionals was presented. In particular, on September 11 2001, eight hours after the terrorist attacks on the World Trade Center and Pentagon, two South African brothers, Willem and Christiaan Conradie, allegedly fabricated and distributed the following e-mail message (Damon, 2001):

Title: CNN News flash 4255/11/09/200/23h15 (sic)

Verbatim extracts: *'The US Secretary of State, Colin Powell, revealed late last night that there is a strong possibility that South Africans and possibly the South African government might be involved ... Video footage from the airports revealed that at least three South Africans boarded each fatal plane. The subject is still under investigation, but sources believe that it has a strong link to the recent US boikot (sic) of the racism conference held in the South African city of Durban. CNN information sources disclose (sic) that some of the masterminds might be in hideaway in South Africa. Strong links has (sic) also been made between SA and Lybia (sic).'*

It was reported by the South African (SA) newspaper media that this e-mail had significant national, international, and financial repercussions and influenced relations between the United States (US) and the SA governments at a difficult time in the history of the US. It reportedly resulted in the decline of the SA currency and had a negative effect on the Johannesburg Stock Exchange ("Bolandse broers", 2001; Coetzee, 2001; Damon, 2001; Momberg, 2001). The Conradie brothers, allegedly responsible for the creation and dissemination of the e-

mail, were arrested and charged with sabotage and fraud, but eventually all charges against them were dropped.

Pretorius & Barnard (2004) analysed this incident from various perspectives, taking a closer look at the reported perceptions of the different stakeholders and considering various aspects of appropriate ethical analyses including the application of the framework of section 4.1. The purpose of this paper was firstly to demonstrate the application various approaches to ethical analysis and not to justify the seemingly obvious conclusion that the alleged creation and dissemination of the hoax e-mail was unethical and lead to the spreading of harmful misinformation (Pretorius and Barnard, 2004). Secondly, it was shown that the ethical and legal conclusions were not consistent. We maintain that real life ethical issues are usually more complex and would benefit from systematic analysis.

4.3 Example 2: Software Agent Behaviour

In this section we consider the Microsoft Office Assistant (Microsoft named it Clippy because of its paper clip persona) as a representative example of intelligent agent technology. Clippy is the little animated figure that appears on the user's screen and presents tips about using Microsoft programs. When first released, critics dismissed Clippy as the equivalent of training wheels for computer novices. Yet the friendliness of Clippy conceals a great deal of computing potential. *"In fact, it's essentially a back door for Microsoft to allow macros that can take control of a PC and help out users"* (Lemos, 2003).

We note that Clippy's settings are global for all programs in the Microsoft Office suite. When Clippy is set to provide a set of help options for one program in the suite, it will do the same for all the others within that suite. Furthermore, Clippy exhibits a number of salient features of an agent as described in section 2.2 and can therefore be classified as a citizen of cyberspace.

It is instructive to perform a systematic a posteriori ethical analysis of the actions of Clippy (excerpt from Smith, Eloff, Venter, Barnard and Pretorius, 2003).

Step 1: analysis of the scenario

In analysing Clippy's behaviour, we take note of the following:

Facts: The agent Clippy is a little animated figure that appears on the user's screen and provides tips about using Microsoft Office programs. It also opens a dialogue box that allows a user to bypass the Help menu and enter a simple question in natural language.

Stakeholders: The human user, the agent Clippy, and the host on which the Microsoft Office package is installed.

Ethical and social issue: Does Clippy exhibit any unacceptable or unethical behaviour by being present on the user's screen and employing continual intrusive animation in order to offer unsolicited assistance?

Step 2: application of appropriate formal guidelines

No corporate or professional codes of conduct available to Clippy.

Clippy's conformance/violation of the Golden Rule: One can argue that Clippy's continual intrusive animation in order to offer unsolicited assistance, can be viewed by the user as distracting him/her from the task at hand. More fundamentally, Clippy's continued presence and monitoring of the user's actions and keystrokes can be viewed as an invasion of the privacy of the user. The fact that Clippy sometimes also goes to sleep when a period of inaction on the part of the user is detected, can be viewed in a negative light, and even experienced as intimidating behaviour on the part of Clippy towards the user. On a certain level thus it may seem as if Clippy violates the golden rule. However, the user has the option to control or de-activate Clippy's presence and one can hence argue that if Clippy is in violation of the golden rule, it is with the consent of the user. As an independent agent thus Clippy does not violate the golden rule.

Who benefits from or is harmed by Clippy's actions? By design Clippy is intended to assist the user - a novice user may find the continued assistance helpful, whereas a more advanced user can customise

Clippy's level of assistance and presence (and in the extreme even de-activate Clippy). Therefore the user can benefit from Clippy.

One can thus conclude that Clippy does not intentionally violate these formal guidelines.

Step 3: application of ethics theories

Duty-based ethical theory

Fidelity: Clippy does offer the user relevant assistance, and thus lives up to the promise of user support.

Reparation: Not applicable.

Justice: Clippy's assistance is available to all Office users.

Beneficence: Clippy's design implies that assistance is freely available to all users irrespective of competency levels. Thus this agent may improve the lot of the user in general. The expert user may find Clippy's presence distracting but still has the option to either customise or de-activate Clippy.

Gratitude: Not applicable.

Non-injury: Not applicable.

In terms of the duty-based theory thus, Clippy's actions towards the user are not regarded as unethical.

Rights-based ethical theory

Clippy's visual presence or not is a true reflection of the agent's activity, and thus the user is always fully aware of its presence. Therefore the user's right to know is respected.

The default design of the agent is that it is always present and active. The deactivation ability is only an option. Thus we contend that the user's right to privacy is not respected.

Clippy has no autonomous intervention capabilities, and thus the user's right to property, i.e. his/her control and possession of electronic data and the concomitant integrity thereof, is respected.

Clippy poses a minor threat to the user's right to privacy (which can be counteracted by the user), while respecting the user's right to know and right to property. In terms of rights-based ethics thus, Clippy's actions towards the user are not regarded as unethical.

Consequence-based ethical theory

The user has final control regarding the agent's activities and existence and is thus subject to the user's discretion. In this respect the agent does not influence the user, whereas the user determines the lifespan of the agent. We can thus conclude that the impact of the agent on the (single) user is limited, and as the agent interacts only with the Office applications of the (single) user, general impact is also limited. Therefore Clippy's actions are not in conflict with utilitarian principles.

Just consequentialism

We are reminded that just consequentialism implies that the end, however good, "do not justify using unjust means" (Moor, 2001). We again note that the default design of the agent is that it is always present and active in an attempt to provide the user with assistance. This action of the agent compromises the user's right to privacy and is an instance of using unjust means towards a good end. Clippy's actions can thus be viewed as a violation of just consequentialism.

We conclude that the majority of ethical theories applied in this step, suggest that Clippy is a relatively benign agent that does not pose malicious (autonomous) intentions towards the user.

Step 4: application of relevant laws

Not applicable.

Step 5: application of informal guidelines

We only apply the Other Person's Shoe test for illustrative purposes.

The Other Person's Shoe test: Clippy's obtrusive and even intimidating character may be demonstrated by its continual intrusive

animation in order to offer unsolicited assistance, its continued presence and monitoring of the user's actions and keystrokes, and the fact that Clippy sometimes also goes to sleep when a period of inaction on the part of the user is detected. These inherent character flaws imply that Clippy would have difficulty in passing the Other Person's Shoe test.

Step 6: make a defensible decision

From the above it is apparent that the unethical aspects of Clippy's behaviour can be counteracted or managed by the (expert) user. Although some may view Clippy's actions as irritating or distracting, the above ethical analysis clearly demonstrates that on the whole, Clippy's actions towards the user cannot be regarded as unethical.

5. Quo Vadis?

As ubiquitous computing technology matures and as increasingly intelligent, often invisible computing devices make their way into the lives and bodies of human beings, the ethical, moral, social and technical issues become blurred. Are we as computing educators, scientists and professionals ready for the complexities and challenges of responsible decision-making in the cyberspace of the future?

We contend that it is the responsibility of present-day computing instructors to familiarize themselves with ethical issues and moral quandaries posed by cyberspace, and that they then impart this information to their students in a rigorous manner. This will ensure that the computing professional of the future, will not only be more aware of issues relating to cyberspace, but be able to proactively counteract unethical activities in order to ensure the continued integrity of cyberspace.

Moor (2001) warns that "*[w]ith policy vacuums and conceptual muddles galore, finding the right connections between computational practice and ethical categories and principles can be extraordinarily difficult.*" Regarding ubiquitous computing in particular, Langheinrich (2001) maintains that what "*lies at the intersection of privacy protec-*

tion and ubiquitous computing is easy to imagine: the frightening vision of an Orwellian nightmare-come-true, where countless "smart" devices with detailed sensing and far-reaching communication capabilities will observe every single moment of our lives, so unobtrusive and invisible that we won't even notice! Ron Revest calls this the "reversal of defaults": "What was once private is now public", "what was once hard to copy, is now trivial to duplicate" and "what was once easily forgotten, is now stored for ever." Clearly, "something" needs to be done, as nearly all work in ubiquitous computing points out, yet little has so far been accomplished."

Unless we as computer professionals take ownership of the domain in which we practice whilst affording a commensurate degree of sensitivity to social and ethical ramifications of the technology we develop, some of the bleak predictions of Moor and Langheinrich may become a reality. Indeed, in the words of Chuck Huff (2004): *"Software engineers should take responsibility where emerging methods allow them to, and should be humble about their ability to guarantee perfect functioning where they cannot measure or test performance in real conditions. By increasing knowledge about the social effects of software, and by adopting methods that allow us to anticipate these effects, we may be able to decrease sorrow ... But we will do so at the expense of our own simplistic approaches to software design."*

6. References

Act No. 25 2002. The South African Electronic Communications and Transactions Act.

Barnard, A, E Cloete, & L Pretorius 2004. A Framework for Performing Security and Ethical Analyses in Agent Computing. *Challenges for the Citizen of the Information Society: Proceedings of the Seventh International ETHICOMP Conference.* Syros, Greece. (eds.) T.W. Bynum, N. Pouloudi, S. Rogerson & T. Spyrou; 1:81 - 93.

Barnard, A, C De Ridder, L Pretorius & E Cohen 2003. Integrating Computer Ethics into the Computing Curriculum: A Framework for Implementation. *Proceedings of IS2003, Informing Science + Information Technology Education Joint Conference.* Pori, Finland; pp. 265 - 279.

Barnard, A, L Pretorius & L Venter 2004. The ECT act and Its Impact on a Typical Computing Curriculum; SACLA2004.

Beck, S 2003. History of Ethics Volume 1 - To 30 BC Ancient Wisdom And Folly, *Chapter on Ethics.* Accessed June 2004 http://www.san.beck.org/EC1-Ethics.html.

Bolandse Broers Voor na 'Opruiende' e-Pos 2001. *DieBurger*, September 17: 1.

Coetzee, H 2001. Broers in Hof oor VSA-e-Pos. *Beeld*, September 17: 4.

Damon, J 2001. Hoax e-Mail Suspects Due to Appear in Court Today. *Cape Times*, September 17: 3.

Floridi, L & JW Sanders 2001. On the Morality of Artificial Agents. Forthcoming in *Ethics of Virtualities - Essays on the Limits of the Bio-Power Technologies*, (eds). A. Marturano and L. Introna. To be published as part of the series *Culture Machine*, Athlone Press: London. Accessed July 2003 http://www.wolfson.ox.ac.uk/~floridi?pdf/maa.pdf.

Floridi, L & JW Sanders 2003. Internet Ethics: The Constructionist Values of Homo Poieticus. Invited chapter for *The Impact of the Internet on Our Moral Lives*; (ed.) R. Cavalier (SUNY: Fall 2003). Accessed June 2004 http://www.wolfson.ox.ac.uk/~floridi/.

Fou, J 2001. Web Services and Mobile Intelligent Agents: Combining Intelligence with Mobility. Accessed May 2003 http://www.webservicesarchitect.com.

Gleason, DH & L Friedman 2003. The Social Construction of Cyberspace. *Proceedings of the Fifth International Conference on Computer Ethics — Philosophical Enquiry.* Boston College: Chestnut Hill, MA, 41-51.

Gleason, D.H. & L Friedman 2004. Proposal for an Accessible Conception of Cyberpsace . *Challenges for the Citizen of the Information Society: Proceedings of the Seventh International ETHICOMP Conference.* Syros, Greece; (eds.) TW Bynum, N Pouloudi, S Rogerson & T Spyrou 1:318 - 329.

Gruba, P 2004. A Framework for Ethical Decision-Making. Accessed June 2004 http://www.cs.mu.oz.au/343/2004/ETweek02/ethics.pdf.

Huff, C 2004. Unintensional Power in the Design of Computing Systems. In *Readings in Cyberethics;* (eds.) R.A. Spinello and H.T. Tavani. Jones and Bartlett Publishers: Sudbury, MA.

Kemerling, G 2001. Aristotle: Ethics and the Virtues. Accessed June 2004 http://www.philosophypages.com/hy/2s.htm.

Kraut, R 2001. Aristotle's Ethics. *The Stanford Encyclopedia of Philosophy* (Summer 2001 Edition); (ed.) EN Zalta. Accessed June 2004 http://plato.stanford.edu/archives/sum2001/entries/aristotle-ethics/.

Langheinrich, M 2001. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. *Ubicomp 2001, LNCS 2201*; (eds.) GD Abowd, B Brumitt and SAN Shafer. Springer-Verlag: Berlin.

Lemos, R 2000. Microsoft's 'Clippy' a Security Nightmare? *ZDNet News*. Accessed May 2000 http://zdnet.com.com/2100-11-520809.html?legacy=zdnn.

Lenarcic, J 2003. The Dinosaur and the Butterfly: A Tale of Computer Ethics. *IEEE Security & Privacy*, September/October. Accessed June 2004 http://computer.org/security/.

Lessig, L 1999. *Code: And Other Laws of Cyberspace.* Basic Books: New York.

Maner, W 2002a. Heuristic Methods for Computer Ethics. *Metaphilosophy* 33(3):339-365.

Maner, W 2002b. Rananu, Davies and Rogerson: The Five-step Process of Ethical Analysis. *Procedural Ethics*. Accessed November 2002 http://csweb.cs.bgsu.edu/maner/heuristics/1996Rananu.htm.

Momberg, E 2001. Anti-SA Govt 'Flash' Was a Hoax. *Citizen*, September 14: 5.

Moor, JH 2001. Just Consequentialism and Computing. *Readings in cyberethics;* (eds.) RA Spinello & HT Tavani. Jones and Bartlett Publishers: Sudbury, MA.

Moor, JH 2001. The Future of Computer Ethics: You Ain't Seen Nothin' Yet! *Ethics and Information Technology*, 3:89-91.

Pretorius, L & A Barnard 2004. E-mail and Misinformation: A South African Case Study. *Proceedings of the Informing Science and Information Technology Education Joint Conference*; Rockhampton, Qld, Australia; 123-142.

Smith, E, MM Eloff, LM Venter, A Barnard & L Pretorius, 2003. Agents, Security and Ethics: A Framework for Analysis. *South African Computer Journal*, 31:18-24.

Spinello, R.A 1997. *Case Studies in Information and Computer Ethics.* Prentice Hall: Upper Saddle River, NJ.

Spinello, RA & HT Tavani, (eds) 2001. Preface, *Readings in Cyber-Ethics.* Jones and Bartlett: Boston, MA.

Spinello, RA 2003. *Case Studies in Information Technology Ethics*, second edition. Prentice Hall: Upper Saddle River, NJ.

The Shorter Oxford English Dictionary on Historical Principals, third edition. 1955. (ed.) C.T. Onions, Clarendon Press: Oxford, UK.

Van der Merwe, DP, L Pretorius & A Barnard 2004. Cyberethics and the South African Electronic Communications and Transactions Act. *Challenges for the Citizen of the Information Society:* Proceedings of the seventh International ETHICOMP conference. Syros, Greece; (eds.) TW Bynum, N Pouloudi, S Rogerson & T Spyrou; pp. 860 - 870.

Wagner, DN 2000. Software Agents Take the Internet as a Shortcut to Enter Society: A Survey of New Actors to Study for Social Theory. *First Monday*, 5(7). Accessed May 2003 http://firstmonday.org/issues/issue5_7/wagner/index.html.

Web Hosting Directory 2005. Accessed July 2005 http://www.webhostingrank.com/glossary/Cyberspace.html.

Wu, X, S Rogerson, & N Fairweather 2001. Being Ethical in Developing Information Systems: An Issue of Methodology or Maturity in Judgment? *Proceedings of the 34th Annual Hawaii International Conference on System Sciences* (HICSS-34)-Volume 8. Accessed June 2004 http://csdl.computer.org/comp/proceedings/hicss/2001/0981/08/0981toc.htm.

Authors' Contact Details

Laurette Pretorius (pretol@unisa.ac.za)
Andries Barnard (barnaa@unisa.ac.za)
School of Computing, University of South Africa
Pretoria, South Africa